Intelligent Decision Technologies 15 (2021) 667–679
DOI 10.3233/IDT-210214
IOS Press

Accessing electronic health records in critical incidents using context-aware attribute-based access control

Evgenia Psarra[a,*], Yiannis Verginadis[b,c], Ioannis Patiniotakis[c], Dimitris Apostolou[a] and Gregoris Mentzas[c]
[a]*Department of Informatics, University of Piraeus, Piraeus, Greece*
[b]*School of Business, Department of Business Administration, Athens University of Economics and Business, Athens, Greece*
[c]*Institute of Communications and Computer Systems, Zografou, Greece*

Abstract. In emergency situations, different actors involved in first aid services should be authorized to retrieve information from the patient's Electronic Health Records (EHRs). The research objectives of this work involve the development and implementation of methods to characterise emergency situations requiring extraordinary access to healthcare data. The aim is to implement such methods based on contextual information pertaining to specific patients and emergency situations and also leveraging personalisation aspects which enable the efficient access control on sensitive data during emergencies. The Attribute Based Access Control paradigm is used in order to grant access to EHRs based on contextual information. We introduce an ABAC approach using personalized context handlers, in which raw contextual information can be uplifted in order to recognize critical situations and grant access to healthcare data. Results indicate that context-aware ABAC is a very effective method for detecting critical situations that require emergency access to personal health records. In comparison to RBAC implementations of emergency access control to EHRs, the proposed ABAC implementation leverages contextual information pertaining to the specific patient and emergency situations. Contextual information increases the capability of ABAC to recognize critical situations and grant access to healthcare data.

Keywords: Attribute-based access control, context-aware services, decision making, electronic health records, emergency services, fuzzy logic, health information management, medical diagnosis, medical information systems

1. Introduction

Controlling access to healthcare data is of great importance because the preservation of the privacy of the patient's information, such as his medical history, is a legal and societal requirement. Access control models deal with the rights a subject has upon performing some operations (such as read, write, etc.) on specific data objects. Prominent access control models that are based on the identity of a user include the Mandatory Access Control (MAC), the Discretionary Access Control (DAC) or the Role-Based Access Control (RBAC) [1]. Apart from these models which are static, a dynamic model has been introduced, the Attribute-Based Access Control (ABAC) [2]. In ABAC, there are no static lists of permissions that associate subjects with objects, but instead there are 'snapshots' of such associations that can be generated and dynamically change based on the current context.

In healthcare, contextual information, such as information indicating an emergency or criticality in patient's medical condition, should be taken into account when granting access to her medical data in order to ensure the best possible medical response. Hence, there

*Corresponding author: Evgenia Psarra, Department of Informatics, University of Piraeus, 18534 Piraeus, Greece. Tel.: +30 210 7723895; E-mail: jennypsarraemp@mail.ntua.gr.

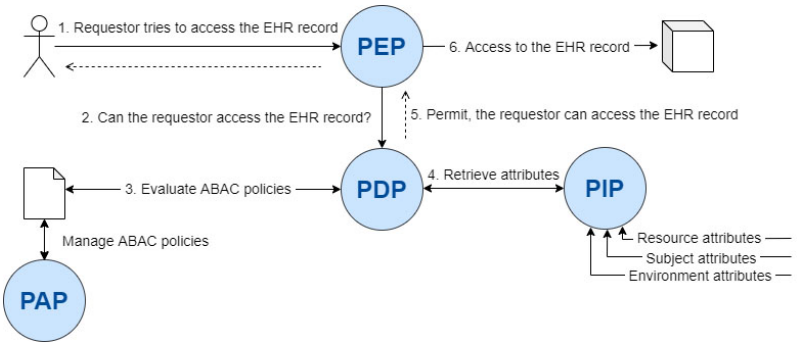

Fig. 1. ABAC architecture.

is a need to apply access control protocols with capabilities that incorporate the notion of context, i.e., the consideration of dynamically-changing contextual attributes that may characterize a situation. Context can be perceived as any information that can be used to characterize the situation of an entity (person, place, or object) that is considered relevant to the interaction between a user and an application, including the user and applications themselves [3]. In fact, the use of contextual information makes it possible to apply access control policies by considering the circumstances under which access requests should be evaluated. For example, in acute care cases, an emergency doctor wants to access parts of the patient's healthcare and medical information to cope best with an acute care situation. Contextual attributes values can be acquired for example from IoT sensors. Consider, for example, a smartwatch with blood pressure measurement capabilities. Still, contextual attributes are often too low-level and cannot be used to characterise a situation of used in isolation. Contrary, by processing contextual attributes, context can be uplifted: low-level contextual attributes can be used to detect higher-level context that characterises a situation.

We argue that context handlers can be valuable for enforcing dynamic authorization processes that take into the criticality of a certain health emergency before yielding an access control decision. This is quite important, since in emergency situations paramedics and first response teams should have immediate access to patients' health records although they could not have been considered in the defined policies at design time.

The research objectives of our work are threefold: First, to develop a method that can be used by medical experts to characterise critical, emergency situations requiring extraordinary access to healthcare data based on dynamically changing contextual attributes. Second, to apply the ABAC paradigm and its context-handling capabilities in order to implement the proposed context-uplifting method for characterising situations. Third, to enable personalisation in the way contextual attributes are used to characterise situations for different users.

2. Related works

2.1. Attribute-based access control

ABAC architecture (Fig. 1) comprises: (i) the Policy Enforcement Point (PEP), responsible for securing applications and data; It is responsible for intercepting requests and propagating authorization requests to the Policy Decision Point (PDP); (ii) the Policy Information Point (PIP), which bridges external sources of attributes e.g., LDAP databases; and (iii) the Policy Administration Point (PAP) which managed policies. Policies in ABAC are statements which combine attributes to define acceptable or not actions, therefore permitting or denying access to sensitive data. For example, if a requestor wants to access a specific health record, her request is intercepted by PDP, which evaluates relevant policies managed by PAP and using attribute values fetched from PIP. ABAC has been utilised to control access to Electronic Health Record Systems [4].

In XACML (eXtensible Access Control Markup Language) [5], a context handler is the system entity that converts decision requests in the native request format to the XACML canonical form and converts authorization decisions in the XACML canonical form to the native response format [6]. Independently of whether the XACML standard is used or not, context handlers are used in ABAC in order to convert the attribute representations into means that are relevant to the application environment. Low-level context is useful for inferring higher level context towards identifying critical situations, such as in the case of an emergency med-

ical dispatcher situation. This knowledge is pertinent in deciding whether access to personal healthcare data should be granted or not.

Alternatively to XACML architecture, the Open Policy Agent (OPA) [7] constitutes an open source, general-purpose policy engine which unifies policy enforcement. It provides a high-level declarative language for specifying policy as code and APIs to offload policy decision-making from software. When software needs to make policy decisions, it queries OPA and supplies structured data, e.g., JSON, as input. OPA policies are expressed in the Rego high-level declarative language which is purpose-built for expressing policies over complex hierarchical data structures. According to Siebach [8] OPA system uses its own policy grammar. The difficulty with this system is that it breaks domain boundaries in its approach to obtain attributes, or the policy language used is not simple enough to allow business owners to write the policies. For example with grammar difficulties, Rego, the language for writing policies in OPA is very expressive, but it requires significant technical development skills to develop policies with it.

For example, let us consider a defined access control policy that permits access to a patient's Electronic Health Records (EHRs) to doctors only if they are currently located in a specific hospital. A simple service that retrieves the latitude and the longitude of a doctor (e.g., based on a mobile device that transmits GPS data) is not sufficient for enabling the authorization system to yield a permit or deny decision. Additional functionality is required in order to consider the semantic level of the information that the access policy requires and then convert the raw data to indicate whether or not the registered GPS position refers to the specific hospital or not. Therefore, context handlers are dedicated software components that are used for processing raw contextual data relevant to an access control decision and semantically uplifting them as instances of a context model. Context handlers are responsible for fusing the context-aware policy enforcement mechanism with contextual information in a usable format that will enable the evaluation of access control policies. We note that the scope of context handlers can be quite broad and this is why their design and development should use as background knowledge an appropriate context model.

We first introduced the need for context handlers capable of processing raw contextual data and inferring knowledge which is useful for access control as part of our previous work [9] in the cloud platform-as-a-service security domain. Specifically, we have developed context handlers that are able: i) to provide real-time measurements with respect to certain contextual attributes and ii) to uplift the registered attribute value(s) to a semantic level that is appropriate for the application domain and the access control policy at hand. In this work, we further enhance our approach so that it can support context-aware access control in the healthcare domain.

Additionally, the Capability-based Access Control (CapBAC) mechanism exists, where the concept of capability was originally introduced in [10] as "token, ticket, or key that gives the possessor permission to access an entity or object in a computer system". In addition, according to Gusmeroli et al. [11] a capability is a communicable, unforgeable token of authority and it refers to a value that uniquely references an object along with an associated set of access rights. Similarly, in comparison of ABAC with CapBAC we view the following differences. On the one hand, ABAC mechanism has the following advantages over CapBAC: First of all, according to the work of Gusmeroli et al. [11] the ABAC approach, specifies access policies by directly using subject's properties (e.g.: age, location, position etc.), as well as resources and environmental properties, that results in more powerful (and complex) rules and more processing and data availability requirements. In addition, the authors [11], report that the main disadvantage of the capability-based authorization is that it requires issuing capabilities to all subjects, and the selection by the requesting subject of a specific capability when submitting a request. Although capability-based methods have been used as a feature in many access control solutions for the IoT-based applications, applying the original concept of capability-based access control model in IoT network has raised several issues, like capability propagation and revocation [12]. Finally, according to [11], as for other access control mechanisms that have to operate in open, cross domains or cross-enterprise contexts, it is worth mentioning that there is a need to standardize the structure of the capability tokens, the CapBAC supporting services and their access protocols. On the other hand, CapBAC has the following advantages over ABAC: Firstly, Gusmeroli et al. [11] state that a consistent definition of the attributes within a domain is perquisite for ABAC. Additionally, according to the authors [11] ABAC and RBAC systems do not provide flexible delegation rights features.

2.2. Emergency access control

Access to sensitive personal information is a very delicate subject and especially in the healthcare domain,

where there is a risk for the patient's private information to be exposed to malicious users. A comparison of diagnostic accuracy with and without access to medical data showed that accessing the EHRs led to an increase in the quality of the clinical decisions [13]. The study concluded that physicians accessing EHRs were more highly informed and thus made more accurate decisions than those who didn't have access to the medical data.

According to Joint NEMA/COCIR/JIRA Security and Privacy Committee [14], break-glass emergency-access is permitted so as to allow operators emergency access to private information in cases where the normal authentication cannot be successfully completed. Nazerian et al. [15] present an Emergency RBAC, which uses Break-the-Glass policy for managing the system in emergency situation with medical and drug-dispensation scenarios. Maw et al. [16] propose a Break-The-Glass Access Control model to address data availability issues and to detect the security policy violations of medical data in Wireless Sensor Networks. The work of Rabieh et al. [17] focuses on securing the patients' medical records to preserve their privacy in case of on-road emergencies while providing them with the appropriate medical service. Dumka and Sah [18] propose, in emergency cases, a smart ambulance equipped with information and communications technology to aid the ambulance staff to treat the patient in a more efficient and effective way. Aski et al. [19] proposed a lightweight access control framework that enables the users to access encrypted data and devices in two modes: attribute oriented access and emergency break-glass access.

Padhya and Jinwala [20] propose a mechanism which can handle emergency situations where no authorized user exists to perform or to delegate a time-critical task. Tasali and Vasserman [21] present how to handle Break-the-Glass natively within the ABAC model, maintaining full compatibility with existing access control frameworks, putting Break-the-Glass in the policy domain rather than requiring framework modifications. Rajput et al. [22] propose an emergency access control management system (EACMS) based on permissioned blockchain. This blockchain network provides access to the Personal Health Records data to authorized Emergency Team who has the granular access rights from the database, according the permissions derived from the patient's rules. According to Ghafghazi et al. [23] effective emergency response requires accurate, relevant, timely, and location-aware information (e.g., environmental information, health records). They propose a location-aware authorization scheme which protects access authorization and privacy, and filters irrelevant data by taking into consideration the time and location of the ongoing emergency.

2.3. Contextual attributes for emergency assessment

Context describes a specific situation by capturing the setting or circumstances in which an event occurs. A contextual attribute represents a measurable contextual primitive (e.g., a user's current location). It is the full set of contextual attributes that comprise the context of a situation (e.g., an access request that is initiated by a user from a specific location, to access a resource, at a particular time of day, on a specified day of the week). Our approach extends ABAC with healthcare-related context handlers that can uplift raw contextual information so as to consider the critically of a patient's health condition in the access control process.

Attributes in ABAC fall into four different categories [24]: (i) Subject attributes which define the user requesting the access e.g., age, department. (ii) Action attributes which define the requested action e.g., read, delete. (iii) Resource (or object) attributes which define the object of access e.g., the object type (medical record). (iv) Contextual (environment) attributes associated with dynamic aspects of the access control scenario, e.g. time.

To identify contextual attributes that can serve in the assessment of health emergencies, we reviewed several existing works. Yunda et al. [25] consider Age, Body Mass Index (BMI), Gender, Systolic Blood Pressure, and Medication intake as inputs, so as to estimate the Cardiovascular disease risk. Likewise, Kalaivani and Sivakumar [26] evaluate as inputs the Systolic Blood Pressure, Heart Rate, and Blood Sugar so as to estimate the patient's Risk Level. Guzman et al. [27] propose the attributes of Systolic and Diastolic Blood Pressure in their neuro-fuzzy hybrid model which is proposed as a new artificial intelligence method to classify blood pressure. A novel fuzzy expert system for detection of Coronary Artery Disease, using cuckoo search algorithm, is described by Moameri and Samadinai [28] by considering the attributes: Age, Chest pain type, Resting blood pressure, Electrocardiographic Results, Maximum Heart Rate, and Cholesterol level.

A number of researchers take into account personal characteristics of a user when evaluating access policies. For example, elevated heart rate can be considered critical for a certain patient only if the age, the current activity or even his medical conditions are considered. Leyla and MacCaull [29] focus on Personalized Access

Table 1
Access control policy example

Condition				Action
Requestor	Action	Resource	Context conditions	
Emergency doctor	Modify	Exam. results	Location IN Premises AND Curr. Day BETWEEN Mon.–Sat. AND Curr. Time BETWEEN 06:00–22:00 AND Systolic or Diastolic Blood Pressure = Low	Permit

Control where the patient decides who can access his health records. Zerkouk et al. [30] propose an access control model, based on the user capabilities and behavior, in order to assist automatically the dependent people according to the occurred situation.

3. Methods

3.1. A fuzzy-logic based approach for context handling

We propose and develop advanced context handlers that are able to cope with the inherent ambiguity that exists in interpreting contextual information for detecting potentially critical health-related situations. In such situations the ambiguity exists in the frame of personalisation aspects; e.g., elevated heart rate can be considered critical for a certain patient only if the age, the current activity or even his medical conditions are considered.

As healthcare information can be considered subjective or fuzzy, healthcare applications have been improved by leveraging fuzzy logic-based approaches. Computer-aided diagnosis in medicine is considered one of the most applicable sectors of fuzzy logic [31]. Fuzzy logic has been used in this context to support medical image or biomedical signal analysis, segmentation, and feature extraction/selection. Our approach utilizes fuzzy logic to realize inferencing in relation to context handlers.

Fuzzy logic is intended to model logical reasoning with vague or imprecise statements and emerged in the context of the theory of fuzzy sets, introduced by Zadeh [32,33]. It is based on the observation that people make decisions based on imprecise and non-numerical information. Fuzzy models or sets are mathematical means of representing vagueness and imprecise information. These models have the capability of making inferences by utilising information that is vague and lack certainty. In healthcare, it is often the case that there exists ambiguity in the definition as well as in the evaluation of attributes. Fuzzy logic provides the opportunity for modelling attributes and dependencies that are inherently imprecisely defined. Moreover, fuzzy logic models imprecise dependencies based on natural language. This simplifies the decision knowledge elicitation process since it is possible to interview medical experts in their own terms, i.e., they can take the rules that they already use in the decision process and model them as fuzzy rules to work within an inference system.

3.2. Criticality assessment using fuzzy context handlers

Contextual attributes are used for the definition of access control policy rules. We interviewed experts from the healthcare domain, including information technology officers and medical personnel from healthcare institutions (public agencies, hospitals, emergency services, etc.). Experts were asked to create access control policy rules in a structured way that allowed us to consolidate important contextual attributes that should be considered in our ABAC approach. Table 1 provides an example of an access policy provided by respondents.

The template uses the 'IF (Requestor Action Resource) AND (context conditions) THEN permit/deny' rule pattern. For instance, we can define the rule: 'If a doctor attempts to modify examination results, while his location is in premises (of the hospital), then access is permitted'. Context conditions can be Boolean expressions of simple conditions or other composite conditions. In several cases the simple conditions are constraints on context attributes (e.g., Location IN premises). Simple context conditions can be combined in order to form complex context conditions, using the standard AND, OR, NOT operators. A complete list of the contextual attributes, represented in a context model, is described in the work of Psarra et al. [34].

The criticality assessment of a patient's condition is made using a rule-based approach. Note, that since many of the contextual variables appearing in [34] are evaluated by experts using linguistic terms, such as 'if blood pressure is high', our approach adopts the following fuzzy inferencing process:

1. *Fuzzification of variables*. For each variable appearing in the policy rules which is evaluated by experts using linguistic terms, such as blood pressure and heart rate, the fuzzy sets are defined.

2. *Calculation of Implication function*. Each fuzzy 'if-then' rule is a fuzzy relation $R(x, y)$ which is called an implication relation. The implication relation is defined as follows:
$$R(x, y) \equiv \varphi(uA(x), uB(y)). \quad (1)$$
where φ is the implication operator. In our case, we use the implication operator of Larsen Product:
$$\varphi_p : u_A(x) \cdot u_B(y) \quad (2)$$
3. *Composition of fuzzy Relations*. The Generalised Modus Ponens (GMP) method ( ) is applied in every rule "if x is A then y is B", to obtain B' for a given A' using the relation Eq. (3):
$$B' = A' o R(x, y) \quad (3)$$
4. *Composition of Results*. Using the Sum method, the partial results obtained in step 3 are composed.
5. *Defuzzification of result*. Composite results obtained in step 4 are defuzzyfied using the Cendroid defuzzification method in order to produce a crisp value.

Note that alternative fuzzy operators may be used in the various steps of the fuzzy inferencing process. For example, the Mandani Min operator ($\varphi_c : u_A(x) \wedge u_B(y)$) may be used in step 2, the Max method in step 4, and the average-of-maxima in step 5.

3.3. Example

Let us consider an example in which our approach is applied to estimate the overall critical situation of a patient, so as to decide about granting emergency access to an EHR system. A fuzzy context handler was developed based on the following fuzzy rules which map the fuzzy variables Systolic Blood Pressure (m_1) and Diastolic Blood Pressure (m_2) with fuzzy values 'Low', 'Normal', 'Elevated', and 'High', and the fuzzy variable Heart Rate (m_3) with fuzzy values 'Low', 'Medium', and 'High', with the output fuzzy variable Criticality, with values 'Low', 'Medium', and 'High':

$K1_S$: If Systolic Blood Pressure is Low then Criticality is High
$K2_S$: If Systolic Blood Pressure is Normal then Criticality is Low
$K3_S$: If Systolic Blood Pressure is Elevated then Criticality is Medium
$K4_S$: If Systolic Blood Pressure is High then Criticality is High
$K1_D$: If Diastolic Blood Pressure is Low then Criticality is High
$K2_D$: If Diastolic Blood Pressure is Normal then Criticality is Low
$K3_D$: If Diastolic Blood Pressure is Elevated then Criticality is Medium
$K4_D$: If Diastolic Blood Pressure is High then Criticality is High
$K1_{HR}$: If Heart Rate is Low then Criticality is High
$K2_{HR}$: If Heart Rate is Medium then Criticality is Low
$K3_{HR}$: If Heart Rate is High then Criticality is High

Table 2
Systolic and diastolic blood pressure ranges

Blood pressure categories	Low	Normal	Elevated	High
SBP	60–95	85–125	115–145	135–200
DBP	50–63	57–83	77–93	87–130

Table 3
Heart rate ranges

	Low	Normal	High
HR	40–60	50–105	95–190

The corresponding fuzzy sets of each fuzzy variable appearing in the rules are defined according to the American Heart Association (AHA) for blood pressure [35] and for heart rate [36], see Tables 2 and 3.

We quantify criticality in the form of the fuzzy sets uC/C shown next:

$$C_{\text{LOW}} = \{1/0, 0, 8/20, 0.5/50, 0.2/80, 0/100\}$$
$$C_{\text{MEDIUM}} = \{0/0, 0.4/20, 1/50, 0.4/80, 0/100\}$$
$$C_{\text{HIGH}} = \{0/0, 0.2/20, 0.5/50, 0.8/80, 1/100\}$$

We calculate max (criticality (m_i)), which is the maximum value of criticality (m_i) of health metric mi and for all values of mi in the dataset. For systolic blood pressure for example, the distribution of criticality (m_1) is depicted in Fig. 2. Notice that max (criticality (m_1)) $= 67$. Similarly, we infer that max (criticality (m_2)) $=$ 67 and max (criticality (m_3)) $= 67$.

Let us assume that a particular patient has the following health status metrics, which are gauged by the emergency dispatch personnel: $SBP_1 = 110$ mmHg, $DBP_2 = 72$ mmHg, $\text{HR}_3 = 63$ bpm. Using the inference process described in section B, we calculate the corresponding criticalities, that are: *criticality*($SBP = 110$) $= 33$, *criticality*($DBP = 72$) $= 33$, and *criticality*($HR = 63$) $= 33$. If *criticality*(m_i) reaches $\max(\textit{criticality}(m_i))$ then the situation is critical, as far as metric m_i is concerned Eq. (4).

$$\begin{aligned} &\text{If } \textit{criticality}(m_i) = \max(\textit{criticality}(m_i)) \\ &\text{then}(\textit{SITUATION}_{m_i} \textit{ is CRITICAL}) \end{aligned} \quad (4)$$

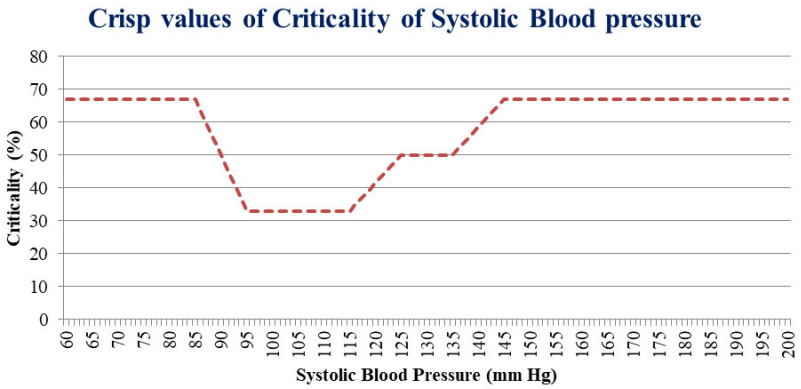

Fig. 2. Distribution of *criticality*(m_1), systolic blood pressure.

Table 4
Systolic blood pressure ranges

Age groups	Low SBP	Normal SBP	Elevated SBP	High SBP
19–40	60–100	90–140	130–160	150–200
41–60	60–115	105–150	140–170	160–200
60+	60–100	90–150	140–170	160–200

Table 5
Diastolic blood pressure ranges

Age groups	Low DBP	Normal DBP	Elevated DBP	High DBP
19–40	50–63	57–83	77–93	87–130
41–60	50–73	67–93	87–103	97–130
60+	50–73	67–93	87–103	97–130

Table 6
Heart rate ranges

Age groups	Low HR	Normal HR	High HR
19–40	40–60	50–105	95–190
41–60	40–60	50–95	85–170
60+	40–60	50–80	70–160

By having calculated the three individual patient's criticalities per health metric, the overall patient's criticality is derived according to Eq. (5).

$$\begin{aligned} &\text{If}((\mathit{SITUATION}_{SBP} \text{ is CRITICAL}) \\ &\text{OR}(\mathit{SITUATION}_{DBP} \text{ is CRITICAL}) \\ &\text{OR}(\mathit{SITUATION}_{HR} \text{ is CRITICAL})) \\ &\text{then}(\mathit{SITUATION}_{OVERALL} \text{ is CRITICAL}) \end{aligned} \tag{5}$$

So in our example, all individual criticalities give the output 'NON-CRITICAL'. According to the disjunctive relation Eq. (5), given that there isn't at least one partial result which provides the result 'CRITICAL', we conclude that the overall result about the patient's health condition is 'NON-CRITICAL'.

3.4. Personalization of context handling

We approach the challenge of personalization of context handling by adjusting the fuzzy sets of each fuzzy variable appearing in the rules based on the patient's profile, by taking into consideration for example her age. The fuzzy sets of each fuzzy variable appearing in the rules are now defined according to the respective ranges per age group of patients (Tables 4–6).

According to the AHA [35], the Systolic Blood Pressure ranges in the following categories: 1) Normal ($<$ 120 mmHg), 2) Elevated (120–129 mmHg), 3) High (hypertension) stage_1 (130–139 mmHg), 4) High (hypertension) stage_2 (140–180 mmHg), 5) Hypertensive crisis ($>$ 180 mmHg). In addition, the normal Systolic blood Pressure per adult age groups ranges in the following categories [37]: 1) 19–40 years (95–135 mmHg), 41–60 years (110–145 mmHg), 61 years or older (95–145 mmHg). The National Health Service (NHS) [38] defines blood pressure ranges of low blood pressure (hypotension) lower than 90 mmHg.

We consider the following ranges of Systolic Blood Pressure of people who belong in the respective age groups 1) 19–40 years, 2) 41–60 years, and 3) older than 60 years, given in the form u_S/S. The fuzzy sets of Systolic Blood Pressure for the age group 41–60 are the following: $S^{41-60}_{\text{LOW}} = \{1/60, 1/105, 0.5/110, 0/115, 0/200\}$, $S^{41-60}_{\text{NORMAL}} = \{0/60, 0/105, 0.5/110, 1/120, 1/130, 1/140, 0.5/145, 0/150, 0/200\}$, $S^{41-60}_{\text{ELEVATED}} = \{0/60, 0/140, 0.5/145, 1/150, 1/160, 0.5/165, 0/170, 0/200\}$, $S^{41-60}_{\text{HIGH}} = \{0/60, 0/160, 0.5/165, 1/170, 1/200\}$.

According to AHA [35], the Diastolic Blood Pressure ranges in the following categories: 1) Normal ($<$ 80 mmHg), 2) Elevated ($<$ 80 mmHg), 3) High Diastolic Blood Pressure (hypertension) stage_1 (80–89 mmHg), 4) High (hypertension) stage_2 (90–

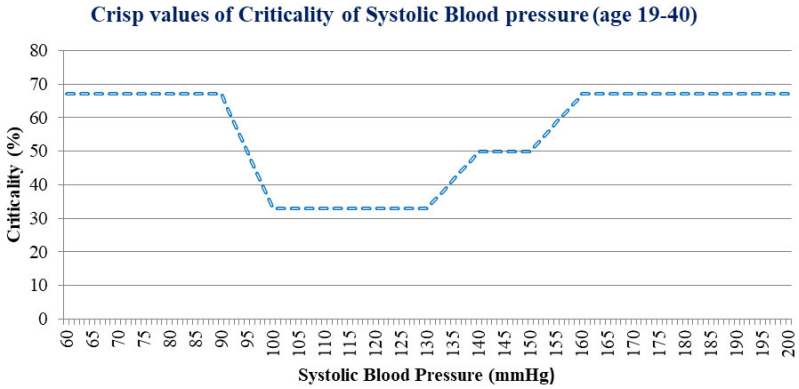

Fig. 3. Distribution of criticality (m_1, age), systolic blood pressure for the age group 19–40.

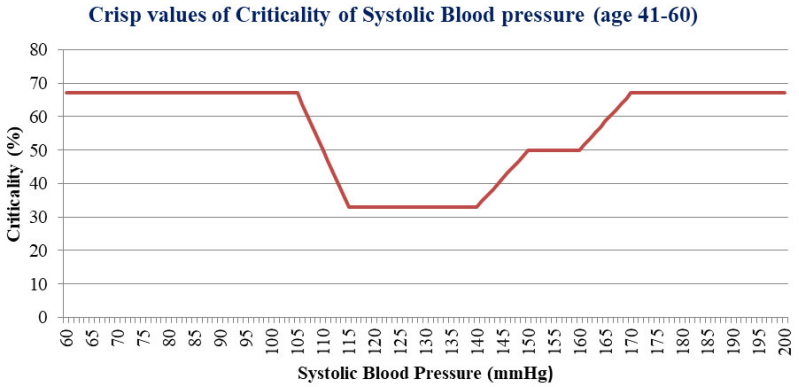

Fig. 4. Distribution of criticality (m_1, age), systolic blood pressure for the age group 41–60.

120 mmHg), 5) Hypertensive crisis (> 120 mmHg). In addition, the normal Diastolic Blood Pressure per age group is divided in the following categories [37]: 1) 19–40 years (95–135 mmHg), 41–60 years (110–145 mmHg), 61 years or older (95–145 mmHg). The NHS [38] defines the blood pressure ranges of low blood pressure (hypotension) as lower than 60 mmHg.

We consider the following ranges of diastolic blood pressure of people who belong in the respective age groups 1) 19–40 years, 2) 41–60 years, and 3) older than 60 years, given in the form u_D/D. The fuzzy sets of Diastolic Blood Pressure for the age group 41–60 are the following: D_{LOW}^{41-60} = {1/50, 1/63, 1/67, 0.5 /70, 0/73, 0/130}, $D_{\text{NORMAL}}^{41-60}$ = {0/50, 0/67, 0.5/70, 1/73, 1/ 87, 0.5/90, 0/93, 0 /130}, $D_{\text{ELEVATED}}^{41-60}$ = {0/50, 0/87, 0.5/90, 1/93, 1/97, 0.5/100, 0/103, 0/130}, D_{HIGH}^{41-60} = {0/50, 0/97, 0.5/100, 1 /103, 1/130}.

According to Abdullah et al. [39], the fuzzy variable Heart Rate ranges in the following categories: Low, Medium, and High. According to Al-Dmour et al. [40], the following "warning scores" categories are provided: 1) score_3 (> 130 bpm), 2) score_2 (< 40 bpm or 111–130 bpm), 3) score_1 (41–50 bpm or 101–110 bpm), score_0 (51–100 bpm). According to the Centers for Disease Control [41] the heart rate during exercise and the maximum heart rate per age are demonstrated. This particular source informs that the maximum heart rate per age is calculated by the mathematical formula: max heart rate = 220 – age. In our approach, we consider as upper-medium limit the range of 50–85% of heart rate usage [41].

We consider the following ranges of heart rate of people who belong in the respective age groups 1) 19–40 years, 2) 41–60 years, and 3) older than 60 years, given in the form uHR/HR. The fuzzy sets of Heart Rate for the age group 41–60 are the following: HR_{LOW}^{41-60} = {1/40, 1/50, 0.5/55, 0/60}, $HR_{\text{MEDIUM}}^{41-60}$ = {0/50, 0.5/55, 1/60, 1/85, 0.5/90, 0/95}, HR_{HIGH}^{41-60} = {0/85, 0.5/90, 1/95, 1/170}.

The distribution of criticality (mi, age) depends on the age group in which the patient belongs to. For systolic blood pressure for example, two distributions of different age groups are depicted in Figs 3 and 4.

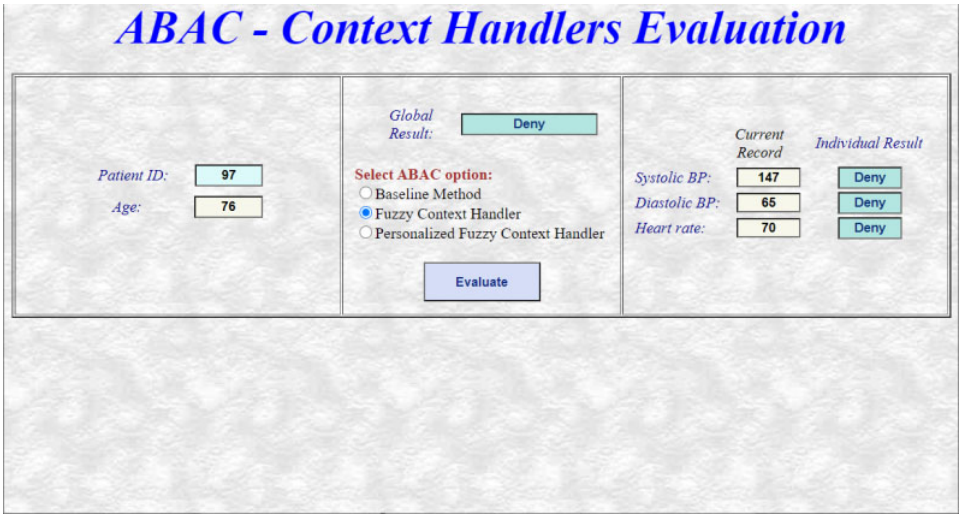

Fig. 5. ABAC integration within EHRServer.

The calculation of individual criticality in Eq. (4) is modified as follows:

$$\begin{aligned} &\text{If } \textit{criticality}(m_i, \textit{age}) \\ &= \max(\textit{criticality}(m_i, \textit{age})) \\ &\text{then}(\textit{SITUATION}_{m_i} \text{ is CRITICAL}) \end{aligned} \tag{6}$$

Then, by having calculated the three individual patient's criticalities per health metric by Eq. (6), the overall patient's criticality is derived according to Eq. (5).

To illustrate the effect of personalisation, consider another patient with the following health status metrics, which are gauged by the emergency dispatch personnel: $\textit{SBP}_1 = 160$ mmHg, $\textit{DBP}_2 = 85$ mmHg, $\textit{HR}_3 = 78$ bpm. If the patient's age group is 19–40, the criticalities are as follows: $\textit{criticality}(\textit{SBP} = 160, \textit{age} = 35) = 67$, $\textit{criticality}(\textit{DBP} = 85, \textit{age} = 35) = 50$, and $\textit{criticality}(\textit{HR} = 78, \textit{age} = 35) = 33$ and the assessment of the overall situation is 'CRITICAL'. If however, the patient belongs to the age group 41–60, the corresponding value of criticalities are: $\textit{criticality}(\textit{SBP} = 160, \textit{age} = 54) = 50$, $\textit{criticality}(\textit{DBP} = 85, \textit{age} = 54) = 33$, and $\textit{criticality}(\textit{HR} = 78, \textit{age} = 54) = 33$ and the assessment of the overall situation is 'NON-CRITICAL'. Hence, we derive two different assessment of the situation criticality depending on the patient's age group.

4. Implementation

We validated our approach by implementing it and integrating it within EHRServer. EHRServer [42] is an open source clinical information management and sharing platform based on the openEHR standard [43]. We used our approach to handle access control to data stored in EHRServer. We examined the following three test cases.

In the first case, we used the baseline ABAC method to control access. Specifically, if the data requestor is an ER (Emergency Room) doctor and the patients' metrics are in conjunction above the recommended limit, then the doctor has access to patient EHRs. The policy rule is shown next:

$$\begin{aligned} &\text{If}(\text{requestor} = \text{ER Doctor}) \\ &\text{AND contextual expression} \\ &(\text{SBP} > \text{SBP}_{\text{THRESHOLD}} \text{ OR} \\ &\text{DBP} > \text{DBP}_{\text{THRESHOLD}} \text{ OR} \\ &\text{HR} > \text{HR}_{\text{THRESHOLD}}) \\ &\text{then}(\text{permit access to patient EHRs}) \end{aligned} \tag{7}$$

In the second case, we used ABAC with non-personalized context handlers and the following rule:

$$\begin{aligned} &\text{If}((\text{requestor} = \text{ER Doctor}) \\ &\text{AND context expression} \\ &(\text{CRITICAL}_{\text{SITUATION}} = \text{true})) \\ &\text{then permit} \end{aligned} \tag{8}$$

In the third case, we used ABAC with personalized context handlers. We developed a web application (Fig. 5) so as to implement and validate the three types of ABAC methods.

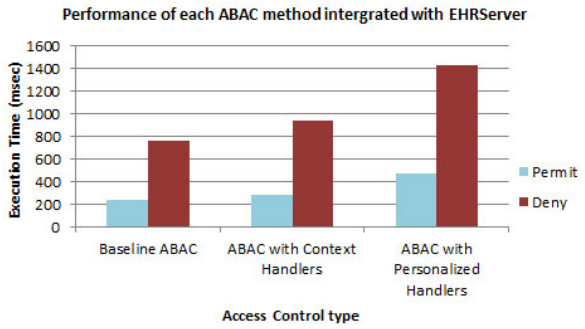

Fig. 6. Performance of each ABAC method integrated within EHRServer.

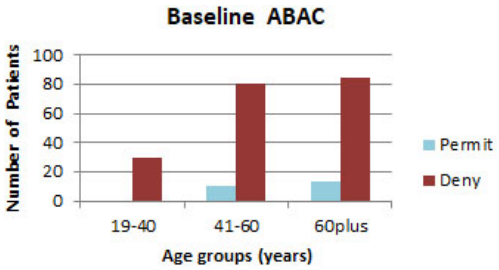

Fig. 7. Access control results, baseline ABAC.

Finally, we compared the performance of each ABAC method (baseline, non-personalised and personalised context handlers) for each one of the three test cases (Fig. 6). The ABAC method with personalised context handlers does have a performance penalty of approximately a factor of two. The performance penalty does not warrant its application in all but the most demanding applications in terms of performance.

5. Datasets and scenarios

To evaluate our approach, we used the PPG-BP (Photoplethysmograph – Blood Pressure) dataset [44], which contains 219 patient healthcare records. The patients' age varies from 20 to 89 years, with an average age of 58 years. The fields of each record are the following: ID, Gender, Age, Height, Weight, Systolic blood pressure, Diastolic blood pressure, Heart rate, BMI, Diseases (hypertension, diabetes, cerebral infarction, cerebrovascular disease). Three different emergency scenarios have been considered, based on the health metrics of systolic blood pressure, diastolic blood pressure, and heart rate. Comparisons between baseline ABAC, ABAC with context handlers and ABAC with personalized context handlers are shown.

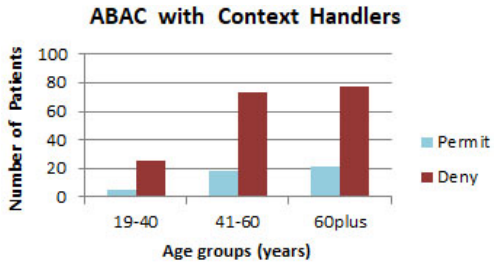

Fig. 8. Access control results, ABAC with context handlers.

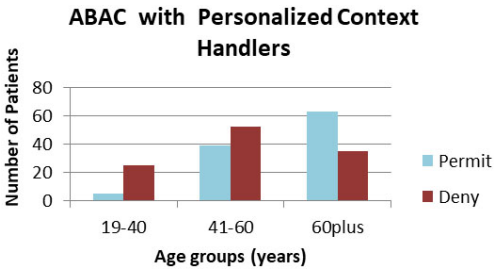

Fig. 9. Access control results, ABAC with personalized context handlers.

6. Access control results

To evaluate the capability of our approach to characterise critical situations and to permit or deny access to data using the ABAC paradigm, we assessed the distribution of permit and deny results as presented next.

6.1. *Permit and deny results for each ABAC method peerage group*

The distribution of Permit and Deny results of the access control mechanism using the baseline ABAC method per age group is presented in Fig. 7.

The distribution of Permit and Deny results of the access control mechanism using our non-personalized fuzzy context handler per age group, is presented in Fig. 8.

The distribution of Permit and Deny results of the access control mechanism using personalized context handlers per age group is presented as follows in Fig. 9.

Notice that ABAC with personalized context handlers achieves the highest number of permits in critical situations, especially on the two older age groups.

6.2. *False positives and negatives for each ABAC method per age group*

We also compared ABAC with personalised context handlers vs non-personalised as well as vs baseline

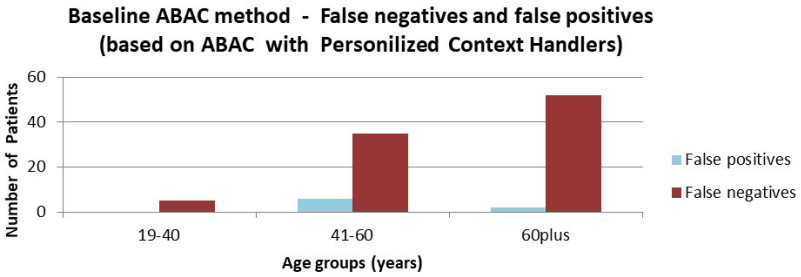

Fig. 10. False positives and negatives per age group, baseline ABAC.

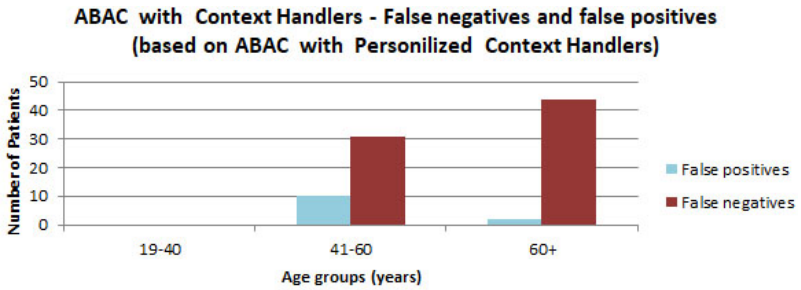

Fig. 11. False positives and negatives per age group, ABAC with context handlers.

ABAC in terms of false positives and false negatives. The former comparison is shown Fig. 11, while the latter is shown in Fig. 10.

Notice that baseline ABAC produces an increasing number of false negatives and positives as patients' age increases. False negative in particular are high and especially hazardous for the patient's life.

Similarly, we note that ABAC with non-personalised context handlers is not as capable as ABAC with personalized context handlers in detecting critical situations, especially in the oldest age group that is the most important.

7. Discussion

Employing personalized context handlers for emergency access control has the following advantages. First, access control is based on both objective patients' metrics and subjective expert knowledge. The latter in particular is easy to elicit and represent using a fuzzy logic approach, in which rules connect the fuzzy variables of each health metric with the criticality, which states the level of patient's health risk. Second, except from the patient's health metrics, additional personal information are taken under consideration such as the patient's age. Third, access control is evaluated based on a fuzzy rule-based inference process, which infer-ences the criticality risk of patients based on the fuzzy rules.

The limitations of our approach include the fact that only the age and a limited set of health metrics are taken into consideration in the fuzzy rules. The corresponding rules are reported as sound by medical experts; nevertheless, the incorporation of additional metrics would improve the completeness of the rules. Additional metrics include gender, BMI, education level, existence of chronic diseases, even lifestyle contextual information such as smoking or drinking habits.

In comparison to RBAC implementations of Break-the-Glass access control, in which the healthcare emergency medical team has predefined access in emergency situations because of their role, the proposed ABAC implementation leverages personalized context which takes into account patient's characteristics and current health metrics. It is worth highlighting that in our scenario, the break-the-glass access decision is made by ER medical personnel. Specifically, the personalized context handler's result (permit or deny) is sent to the ER team along with the patient's current health metrics and age. By having at their disposal both the system's access result and the patient's contextual information, the ER team can make an informed final decision.

Additionally, it is worth mentioning that the context handlers implemented in this work, where access policies are specified by directly using contextual informa-

tion (e.g. the patient's age), manage adequately the dynamic attribute values. On the contrary, CapBAC lacks dynamicity as the capability token is composed by the permissions that a subject has upon an object.

8. Conclusions

In an emergency situation, the criticality of a patient's medical condition should be taken into account when granting access to her EHR. Such emergency access controls are necessary so that healthcare professionals make informed decisions in life threatening situations. In this work, we introduced contextual attributes that serve in the criticality assessment of situations where access to patients' data is requested. We extended ABAC with healthcare-related context handlers, capable of inferring access policies by dynamically evaluating contextual attributes when granting access to healthcare data. We also created personalized context handlers so as to take into account the specificities of each patient when inferring access policies. ABAC with personalized context handlers is more capable than baseline ABAC and ABAC with non-personalised context handlers in detecting critical situations, especially in the oldest age group that is the most important.

Acknowledgments

This research has received funding from the EU, project H2020 826093, Asclepios (https://www.asclepios-project.eu/).

References

[1] Ferrari E. Access control in data management systems. Synth Lect Data Manag. 2010; 2(1): 1-117.
[2] Hu VC, Ferraiolo D, Kuhn R, Schnitzer A, Sandlin K, Miller R, et al. Guide to attribute based access control (abac) definition and considerations. 2014.
[3] Dey AK. Understanding and using context. Pers Ubiquitous Comput. 2001; 5(1): 4-7.
[4] Seol K, Kim Y-G, Lee E, Seo Y-D, Baik D-K. Privacy-preserving attribute-based access control model for XML-based electronic health record system. IEEE Access. 2018; 6: 9114-28.
[5] Oasis-open.org. [cited 2021 Sep 16]. Available from: http://docs.oasis-open.org/xacml.
[6] Quirolgico S, Hu V, Karygiannis T. Access control for sar systems. 2011.
[7] Open Policy Agent [Internet]. Openpolicyagent.org. [cited 2021 Sep 27]. Available from: https://www.openpolicyagent.org/.
[8] Siebach JAJ. The Abacus: A New Approach to Authorization. Brigham Young University; 2021.
[9] Verginadis Y, Patiniotakis I, Gouvas P, Mantzouratos S, Veloudis S, Schork ST, et al. Context-aware policy enforcement for PaaS-enabled access control. IEEE trans cloud comput. 2019; 1-1.
[10] Dennis JB, Van Horn EC. Programming semantics for multiprogrammed computations. Commun ACM. 1966; 9(3): 143-55.
[11] Gusmeroli S, Piccione S, Rotondi D. A capability-based security approach to manage access control in the Internet of Things. Mathematical and Computer Modelling. 2013; 58(5-6): 1189-1205.
[12] Gong L. A secure identity-based capability system. In: Proceedings 1989 IEEE Symposium on Security and Privacy. IEEE Comput. Soc. Press; 2003.
[13] Ben-Assuli O, Sagi D, Leshno M, Ironi A, Ziv A. Improving diagnostic accuracy using EHR in emergency departments: A simulation-based study. J Biomed Inform. 2015; 55: 31-40.
[14] Medicalimaging.org. [cited 2021 Sep 16]. Available from: https://www.medicalimaging.org/wp-content/uploads/2011/02/Break-Glass_-_Emergency_Access_to_Healthcare_Systems.pdf.
[15] Nazerian F, Motameni H, Nematzadeh H. Emergency role-based access control (E-RBAC) and analysis of model specifications with alloy. J Inf Secur Appl. 2019; 45: 131-142.
[16] Maw HA, Hannan Xiao, Christianson B, Malcolm JA. BTG-AC: Break-the-glass access control model for medical data in wireless sensor networks. IEEE J Biomed Health Inform. 2016; 20(3): 763-74.
[17] Rabieh K, Akkaya K, Karabiyik U, Qamruddin J. A secure and cloud-based medical records access scheme for on-road emergencies. In: 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC). IEEE; 2018. pp. 1-8.
[18] Dumka A, Sah A. Smart ambulance system using concept of big data and internet of things. In: Healthcare Data Analytics and Management. Elsevier; 2019. pp. 155-176.
[19] Aski V, Dhaka VS, Parashar A. An attribute-based break-glass access control framework for medical emergencies. In: Advances in Intelligent Systems and Computing. 2020. pp. 587-595.
[20] Padhya M, Jinwala D. BTG-RKASE: Privacy preserving revocable key aggregate searchable encryption with fine-grained multi-delegation & break-the-glass access control. In: Proceedings of the 16th International Joint Conference on e-Business and Telecommunications. SCITEPRESS – Science and Technology Publications; 2019.
[21] Tasali Q, Sublett C, Vasserman E. Controlled BTG: Toward flexible emergency override in interoperable medical systems. ICST Trans Secur Saf. 2020; 6(22).
[22] Rajput A, Li Q, Taleby Ahvanooey M, Masood I. EACMS: Emergency access control management system for personal health record based on blockchain. IEEE Access. 2019; 7: 84304-84317.
[23] Ghafghazi H, Elmougy A, Mouftah H, Adams C. Location-aware authorization scheme for emergency response. IEEE Access. 2016; 4: 4590-4608.
[24] Covington MJ, Sastry MR. A contextual attribute-based access control model. In: On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops. Berlin, Heidelberg: Springer Berlin Heidelberg; 2006. pp. 1996-2006.
[25] Yunda L, Pacheco D, Millan J. A Web-based fuzzy inference

system based tool for cardiovascular disease risk assessment. Nova. 2015; 13(24): 7.
[26] Kalaivani K, Sivakumar R. A novel fuzzy based bio-key management scheme for medical data security. J Electr Eng Technol. 2016; 11(5): 1509-18.
[27] Guzman JC, Melin P, Prado-Arechiga G. Design of an optimized fuzzy classifier for the diagnosis of blood pressure with a new computational method for expert rule optimization. Algorithms. 2017; 10(3): 79.
[28] Moameri S, Samadinai N. Diagnosis of coronary artery disease via a Novel Fuzzy expert system optimized by CUCKOO SEARCH. International Journal of Engineering. 2018; 31(12): 2028-2036.
[29] Leyla N, MacCaull W. A personalized access control framework for workflow-based health care information. In: Business Process Management Workshops. Berlin, Heidelberg: Springer Berlin Heidelberg; 2012. pp. 273-284.
[30] Zerkouk M, Cavalcante P, Mhamed A, Boudy J, Messabih B. Behavior and capability based access control model for personalized TeleHealthCare assistance. Mob Netw Appl. 2014; 19(3): 392-403.
[31] Yanase J, Triantaphyllou E. A systematic survey of computer-aided diagnosis in medicine: Past and present developments. Expert Systems with Applications. 2019; 138: 112821.
[32] Zadeh L. Fuzzy sets. Information and Control. 1965; 8(3): 338-353.
[33] Zadeh L. The concept of a linguistic variable and its application to approximate reasoning – II. Information Sciences. 1975; 8(4): 301-357.
[34] Psarra E, Verginadis Y, Patiniotakis I, Apostolou D, Mentzas G. A context-aware security model for a combination of attribute-based access control and attribute-based encryption in the healthcare domain. In: Advances in Intelligent Systems and Computing. Cham: Springer International Publishing; 2020. pp. 1133-1142.
[35] American Heart Association [Internet]. Heart.org. [cited 2021 Sep 17]. Available from: https://www.heart.org/.
[36] Mahmood U, Al-Jumaily A, Al-Jaafreh M. Type-2 fuzzy classification of blood pressure parameters. In: 2007 3rd International Conference on Intelligent Sensors, Sensor Networks and Information. IEEE; 2007. pp. 595-600.
[37] Lapum JL, Verkuyl M, Garcia W, St-Amant O, Tan A. Vital Sign Measurement Across the Lifespan-1st Canadian Edition. 2018.
[38] Low blood pressure (hypotension) [Internet]. Nhs.uk. [cited 2021 Sep 17]. Available from: https://www.nhs.uk/conditions/low-blood-pressure-hypotension/.
[39] Abdullah AA, Fadil NS, Khairunizam W. Development of fuzzy expert system for diagnosis of diabetes. In: 2018 International Conference on Computational Approach in Smart Systems Design and Applications (ICASSDA). IEEE; 2018. pp. 1-8.
[40] Al-Dmour JA, Sagahyroon A, Al-Ali AR, Abusnana S. A fuzzy logic-based warning system for patients classification. Health Informatics J. 2019; 25(3): 1004-1024.
[41] Target heart rate and estimated maximum heart rate [Internet]. Cdc.gov. 2020 [cited 2021 Sep 18]. Available from: https://www.cdc.gov/physicalactivity/basics/measuring/heartrate.htm.
[42] Gutierrez PP. CloudEHRServer by CaboLabs [Internet]. Cloudehrserver.com. [cited 2021 Sep 18]. Available from: https://cloudehrserver.com/.
[43] Sam Heard TB. openEHR Home [Internet]. Openehr.org. [cited 2021 Sep 18]. Available from: https://www.openehr.org/.
[44] Liang Y, Liu G, Chen Z, Elgendi M. PPG-BP Database [Internet]. figshare. 2021 [cited 18 September 2021]. Available from: https://figshare.com/articles/dataset/PPG-BP_Database_zip/5459299.