An Ontology Based Authentication Framework for Healthcare Monitoring

Amira Henaien and Hadda BelHadj

1 Introduction

Nowadays, the widespread use of smart devices is producing a radical changes in our daily life activities. As one of the fields the most affected is healthcare attending more than 40% from the hole investments of the market of WoT [2, 4]. Several successful industrial or research works are developed with a very efficient design to track and monitor the health of a patient continuously and ubiquitously. The principle idea of WoT Healthcare Applications consists in involving a set of smart devices connected to daily life objects in the body of the patient or its environment. The main job of those devices is to collect the necessary data for an ubiquitous healthcare monitoring. And it may includes any sensing data about the user's health situation and the environment situation, the medical history of a patient, a device information and any health domain-specific data. It is very necessary and challenging to create new standardization and develop good practices to improve the usability, the maintainability, and the security of healthcare applications. As it is discussed in [3, 4], form this list, security is a priority. Any lost or fake information can leads to a dangerous situation and even to the death of human being. For a cardiology patient in a critical situation, any missing vital sign, as its heart beat, can delay an alert or completely loose it and deprive him from getting any aids. The wrong information or the missing data are not always technical bugs. It is absolutely possible that they are a willfully human being made errors spontaneously

A. Henaien (✉)
King Khalid University, Abha, Saudi Arabia
e-mail: aheniaen@kku.edu.sa

H. BelHadj
Laboratory of Technology and Smart Systems, Digital Research Center of Sfax, Sfax, Tunisia
e-mail: Hadda.lBnelhadj@esti.rnu.tn

L. Chaari (ed.), *Digital Health in Focus of Predictive, Preventive and Personalised Medicine*, Advances in Predictive, Preventive and Personalised Medicine 12,
https://doi.org/10.1007/978-3-030-49815-3_2

or deliberately. For this reasons, the system should be enhanced enough to protect its data. As the most first action that can be taken is a strong authentication system to limited the access using a powerful authentication methods.

Different authentication solutions are efficiently used and approved for information systems in general and medical systems in particular. However, new ubiquitous and continuous healthcare monitoring applications have a very particular type of users like: people with special needs, handicaps, old persons, new born babies. For this reason, common methods, viz, knowledge-based or possession-based methods are no more feasible. An old person with Alzaheimer probably is never able to remember the password. It is becoming necessary to create a standardized authentication technique supporting the variety of health situation of users and providing the highest guaranty of protection for the data. A technique taking on consideration the health and mental situation of a user should specify for each user his situations, specify the different possible means of authentication and associate a semantic interpretation to each one. Finally, this technique should be able to reason and interpret the best authentication technique for each user.

This paper presents a new ontology based authentication methodology for healthcare monitoring in a predictive, preventive and personalized medicine system. The main idea consists on allowing different and adapted methods of authentication depending in the health and mental situation of the user. The system allow for a caregiver or a doctor to define the different abilities and capabilities of a patient. Based on those information, the system is able to define the appropriate method to be used for the user to authenticate and is able to provide this method ubiquitously to be identified. This paper is organized as the following: Sect. 2 is a presentation of the background of this work. Section 3 is an overview of this framework. In Sect. 4 we present the main component of this framework, the knowledge management system. Finally, Sect. 5 is a conclusions and perspectives.

2 Related Work and Background

Context and Rules Based Authentication In a very general way, the process of the authentication is confirming that a specific attribute claimed by an entity in a system. This confirmation is in many cases an identification of an entity that claims using credentials. Usual identification methods are knowledge-based methods, i.e. a password, answer question, generated code, etc. Traditional authentication methods have been enhanced with different techniques, viz, location based authentication [1], bio-metric information based authentication [11], context-awareness based authentication [1, 5, 13, 14], shared authorization and authentication rules across network based authentication [17].

Security and Medicine Ontologies Ontologies are becoming a powerful tool in the development of interdisciplinary systems as e-healthcare systems since their are able to represent and interrelate many types of knowledge.

Based Context Modeling for Healthcare Applications During the last years, different medical ontologies have been proposed to summarize medicine terms and concepts, viz, Systematized Nomenclature of Medicine Clinical Terms (SNOMED CT) [15], International Classification of Diseases (ICD)-10 [9] and International Classification Nursing Practice ICNP [10]. The ontology ICNP is a formal structure containing terms and definitions providing a formal nursing terminology for the construction of nursing diagnoses, interventions, and results. Ontology is not only used for terminology, it is also involved in different healthcare applications, viz, [6] proposing a context-aware system for antihypertensive drug recommendations or [8] designing a diabetes diagnosis framework.

Ontology Based Security Approaches Besides to medicine ontologies, some security approaches have been proposed based on ontologies viz, [12] an ontology base authorization enabling semantically matching diverse authorization requests and semantic rule reasoning on requested access; [7] an ontology-based interoperation service translating security attributes from local security vocabularies into the attributes recognized by the central vocabulary. Souad et al. in [16] propose a classification into eight families of existing security ontologies for the different requirements definition.

3 Overview of the Proposed Ontology Based Authentication Framework

The proposed framework is designed to allow different types of identification. It express the abilities of a patient with a formal specification. For each user, the system determinate a personalized method of authentication. The data is collected from different devices like: body sensors worn by the user, ambient sensors surrounding the user or smart devices, as phone, tablet, etc. Body sensors are used to capture the health profile of the patient, viz, vital signs, motion, location, etc. Ambient sensor reflect an image of the patient's environment, viz, ambient temperature, lightness, existence of a caregiver, etc. Smart devices are basically used to allow the communication between the user and the system and between users, viz sending an alert to user about a patient's situation, monitoring a patient, etc. We suppose that a caregiver or doctor is authorized to enter the mental situation the abilities of the patient and edit it in case of any changes. Thus, the basis of the designed system is to provide the appropriate identification method for each user deduced from its role (Patient, Doctor, Caregiver, FamilyCaregiver, etc), the collected data of its current situation, the already described data of its mental situation and abilities and security-related knowledge. As described by Fig. 1, the general architecture of this framework is containing:

Sensing Component: a set of sensors and smart devices related directly to the user. Their role is to collect all the context data: health data, ambient data, location,

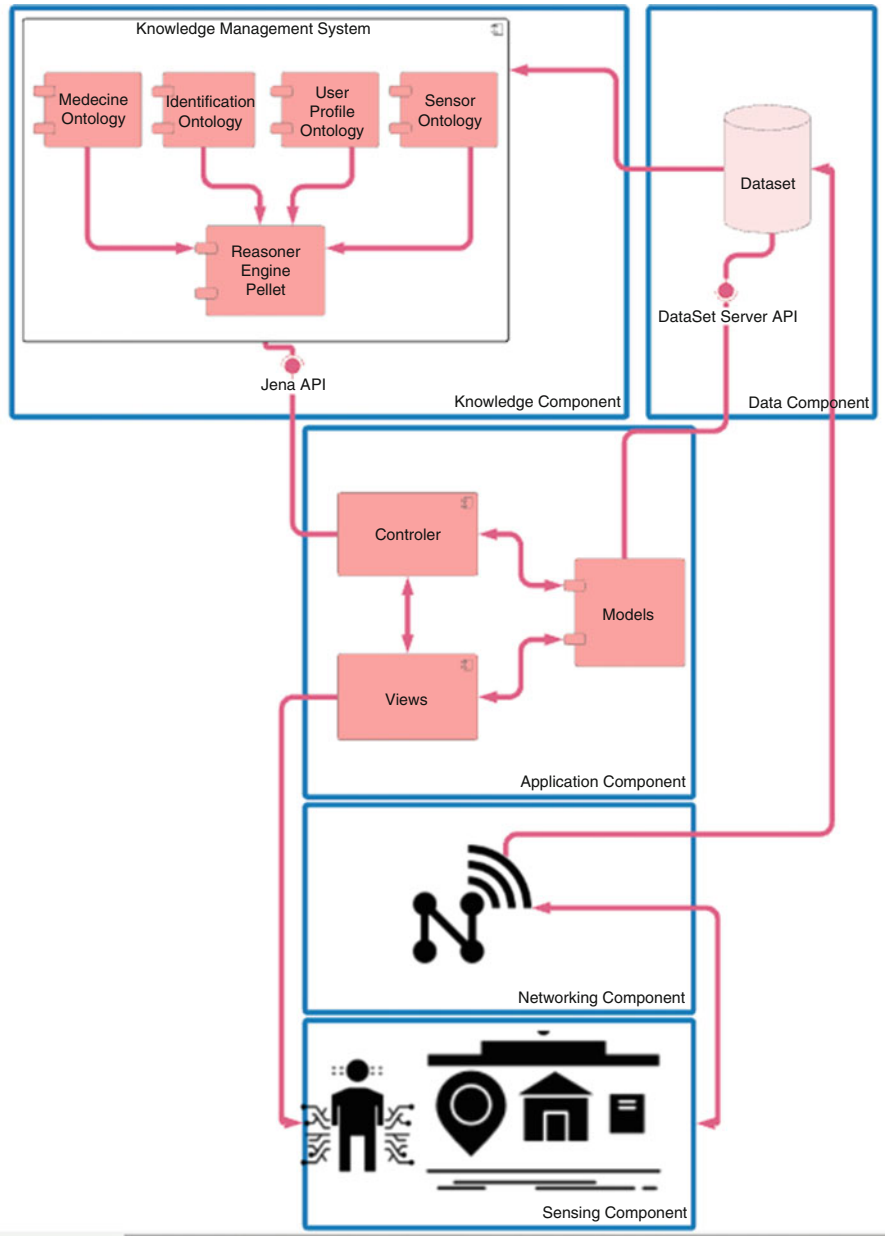

Fig. 1 General architecture of ontology based authentication framework

motion, personal information, etc. This set of sensors are related to one user and they are composing a smart platform.

Networking Component: a set of networking device allowing the communication between the different physical elements and the connection of those elements to the internet. Networking elements also allow the data exchange between the sensing layer and the knowledge component.

Data set Component: is a server hosting all the data: current data collected in real time and saved information about the user. It is providing instances enriching the ontologies from the knowledge component.

Application Component: is the implementation of all the features of the healthcare application providing all the services for ubiquitous and continuous medical monitoring. It is a MVC[1] application.

Knowledge Component: is playing a fundamental role in this architecture because it is the responsible for the knowledge base and the reasoning. It is composed of four ontologies and a reasoner engine (Pellet). This component is the responsible to provide the appropriate authentication method. The Fig. 2 explains the general process of authentication.

4 Ontology Based Knowledge Management System

The main part in the general architecture of the proposed framework, presented in Sect. 3, is the knowledge Management System. It decides the identification method associated to each user. It is composed basically from a set of ontologies: personal profile ontology, sensor ontology, medicine ontology, security ontology and a reasoner. Our ontologies are the extension of standard ontologies such as FOAF for personal profile, SSN and SOSA for sensors ontology and ICNP for medicine ontology. Those standard ontologies are merged with the security ontology containing basically a set of SWRL rules corresponding to the security rules. In the following, we present the different ontologies and the links between their entities.

Personal and health profile: we are using FOAF to present the personal profile of users. FOAF:person is representing all information related to the user, viz, account details, name, familyName, age, gender, etc. In the same time the ontology ICNP is providing an entity Individual presenting the health profile of a user as height, weight. We have specified FOAF:person equivalent to ICNP:Individual. ICNP is also describing an entity Role precising if the individual is Patient, Doctor, Caregiver, Nurse, etc. The property named hasLocation from ICNP associates a location to each patient.

Sensor ontology: The ontology SSN is providing an entity named Platform. It is a concept used to gather different entities as sensors, actuators, other platforms

[1] MVC: Model View Control

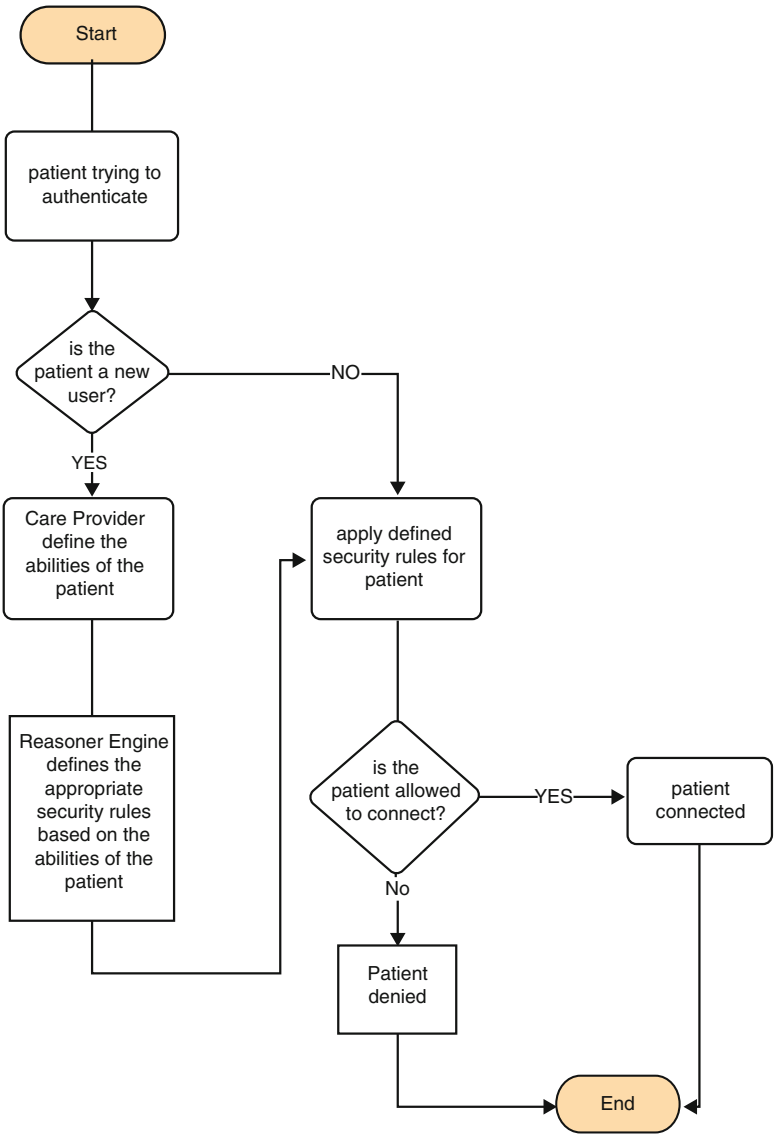

Fig. 2 Flow chart of authentication process

hosted in the same platform. SSN:Platform is associated to a user using the personalized property hasPlatform. The class SSN:Sensor is specified with two sub-classes BodySensors presenting sensors worn or attached to the body of the user and AmbientSensors presenting sensors existing in its environment. For each entity from the platform, we define its location using the same property hasLocation.

Medicine Ontology: ICNP provides an entity AbilityStatus with a set of sub-classes defining all the possible abilities of a person. Each ability contains two sub-classes an actual positive ability, in the case of safe ability, and actual negative ability, in the case of lost ability. For instance, ActualNegativeAbilityToSee is defining the disability of a patient to see. The property hasAbsoluteJudgeState is expressing the state of each ability for a user.

Security Ontology: the class IdentificationMethods contains a sub-classes for each identification methods. This list contains the different following entities: ByCareGiver, ByCornea, ByDoctor, ByEnteringPassword, ByFingerPrint, ByLocation, ByVoicePrint. The relation implementedBy related each method to its implementation. The property IdentifyBy is relating a user to his identification method.

SWRL Security Rules This ontology contains a set of SWRL rules used later by the reasoner to calculate the appropriate identification method and they are mainly authentication rules. For example, if all the abilities of a patient have ActualPositive for the hasAbsoluteJudgeState property, the authentication can be processed using classical authentication method using password, i.e. the property IdentifyBy for this patient is ByEnteringPassword. However, if a patient is blind, the property IdentifyBy for this patient is ByFingerPrint, ByCareGiver or ByDoctor.

5 Conclusions and Perspectives

This paper presents a new ontology based framework to personalize the authentication method to each user of a healthcare ubiquitous and continuous monitoring PPPM system. This new technique is very helpful for users with limited abilities or particular health situation. The identification method is defined depending on different parameters, viz, the user's personal information, his health situation, his mental situation, the possible identification methods, the available device to the user, etc. This work is based also on context and rules based authentication specified with SWRL. As a continuation of this work, we are aiming to develop the complete components constituting the system. We will also evaluate the performance of our system and compare it to other identification methods.

Acknowledgments The authors would like to express their gratitude to King Khalid University, Saudi Arabia for providing administrative and technical support.

References

1. Agadakos, I., Hallgren, P., Damopoulos, D., Sabelfeld, A., Portokalidis, G.: Location-enhanced authentication using the IoT: because you cannot be in two places at once. In: Proceedings of the 32nd Annual Conference on Computer Security Applications, pp. 251–264. ACSAC'16, ACM, New York (2016). https://doi.org/10.1145/2991079.2991090
2. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., Ayyash, M.: Internet of things: a survey on enabling technologies, protocols, and applications. IEEE Commun. Surv. Tutorials **17**(4), 2347–2376 (2015)
3. Alharam, A.K., El-madany, W.: Complexity of cyber security architecture for IoT healthcare industry: a comparative study. In: 2017 5th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), pp. 246–250. IEEE (2017)
4. Baker, S.B., Xiang, W., Atkinson, I.: Internet of things for smart healthcare: technologies, challenges, and opportunities. IEEE Access **5**, 26521–26544 (2017)
5. Bernal Bernabe, J., Hernandez-Ramos, J.L., Skarmeta Gomez, A.F.: Holistic privacy-preserving identity management system for the Internet of things. Mob. Inf. Syst. **2017**, 1–20 (2017)
6. Chen, D., Jin, D., Goh, T.T., Li, N., Wei, L.: Context-awareness based personalized recommendation of anti-hypertension drugs. J. Med. Syst. **40**(9), 202 (2016)
7. Ciuciu, I., Claerhout, B., Schilders, L., Meersman, R.: Ontology-based matching of security attributes for personal data access in e-health. In: OTM Confederated International Conferences on the Move to Meaningful Internet Systems, pp. 605–616. Springer (2011)
8. El-Sappagh, S., Ali, F.: Ddo: a diabetes mellitus diagnosis ontology. In: Applied Informatics, vol. 3, p. 5. SpringerOpen (2016)
9. ICD10: https://bioportal.bioontology.org/ontologies/ICD10
10. ICNP: https://bioportal.bioontology.org/ontologies/ICNP
11. Kumar, T., Braeken, A., Liyanage, M., Ylianttila, M.: Identity privacy preserving biometric based authentication scheme for naked healthcare environment. In: 2017 IEEE International Conference on Communications (ICC), pp. 1–7. IEEE (2017)
12. Poulymenopoulou, M., Malamateniou, F., Vassilacopoulos, G.: A virtual PHR authorization system. In: IEEE-EMBS International Conference on Biomedical and Health Informatics (BHI), pp. 73–76 (June 2014). https://doi.org/10.1109/BHI.2014.6864307
13. Shahzad, M., Singh, M.P.: Continuous authentication and authorization for the Internet of things. IEEE Internet Comput. **21**(2), 86–90 (2017)
14. Shone, N., Dobbins, C., Hurst, W., Shi, Q.: Digital memories based mobile user authentication for IoT. In: 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing, pp. 1796–1802. IEEE (2015)
15. SNOMED CT: https://bioportal.bioontology.org/ontologies/SNOMEDCT
16. Souag, A., Salinesi, C., Comyn-Wattiau, I.: Ontologies for security requirements: a literature survey and classification. In: International Conference on Advanced Information Systems Engineering, pp. 61–69. Springer (2012)
17. Trnka, M., Cerny, T.: Authentication and authorization rules sharing for Internet of things. Softw. Netw. **2018**(1), 35–52 (2018)