Access Control Model Based on Dynamic Delegations and Privacy in a Health System of Connected Objects

Jeanne Roux Ngo Bilong(✉), Kéba Gueye, Gervais Mendy,
and Samuel Ouya

LIRT Laboratory, Higher Polytechnic School,
University of Dakar, Dakar, Senegal
{jeanneroux.ngobilong, gervais.mendy}@ucad.edu.sn,
keba.gueye@esp.sn, samuel.ouya@gmail.com

Abstract. The Internet of Things (IoT) promotes the development of new platforms, services and applications that connect the physical world to the virtual world. Defining access control policies for these platforms remains a challenge for researchers, as security gaps are still observed in several domains, including health. There are much scientific work on systems for remote patient monitoring and most of them have technological limits in access control of patients' personal and confidential information. Moreover, these systems do not allow collaborative work because the doctor, in case of unavailability or in case of need of collegial decision, cannot delegate his role to another doctor having the same skills and the same attributes as him. In this paper, we propose a model based on dynamic role delegation, emphasizing on collaborative work and the protection of patients' privacy. This model is a redefinition of the ORBAC model taking into account the notion of user attributes. We use first order logic and non-monotonic logic T-JCLASSIC$\delta\varepsilon$ to perform an axiomatic interpretation of the model. We implement the model with WebRTC, Node.js and Kurento Media Server technologies to facilitate real-time communication between users, and raspberry pi for collecting biometric information received from sensors.

Keywords: Access control · Delegation · IoT · E-health

1 Introduction

Access controls are still relevant for the management of intelligent structures involving several domains, in this case that of telemedicine [1–3]. In addition, the environments integrate more and more different miniaturized devices as well as mobile communication technology. This allows you to deploy services anywhere, anytime and for anyone. This evolution imposes new security requirements and challenges in these dynamic, context-aware, intelligent environments [1]. Access control models such as Mandatory Access Control (MAC), Discretionary Access Control (DAC) and Role Based Access Control (RBAC) proposed so far do not take into account the dynamic side of access controls [4], neither the management of obligations or recommendations, nor the rules specific to the organization. These are static access control models.

G. Mendy et al. (Eds.): AFRICOMM 2018, LNICST 275, pp. 108–119, 2019.
https://doi.org/10.1007/978-3-030-16042-5_11

In order to improve access control policies, researchers have been working on dynamic access control models such as OrBAC, GeoRBAC (Geographic Role Based Access Control), Context Role Based Access Control (CRBAC), Multi-OrBAC, Poly OrBAC [1]. These models each represent an extension of RBAC, but are not entirely satisfactory because they do not make it possible to manage the delegation of roles, especially in a context of telemedicine that requires the availability of staff dealing in real time. In our work, we have implemented the DORBAC model which is an extension of the OrBAC model, taking into account the role delegation issue and the administration issue for the assignment of license and role. The rest of our work is organized as follows: Sect. 2 presents the state of the art of access control models. Section 3 deals with the description of the proposed model. In Sect. 4, we implement the model. Section 5 concludes our paper with an opening for future work.

2 State of the Art of Access Control Models

2.1 Discretionary Access Control (DAC)

Discretionary Access Control policies are based on the concepts of subjects, objects and access rights. Access rights to each piece of information are manipulated by the information owner. This access control model is flexible because a subject with access rights can grant access rights to any other user. The granting or revocation of privileges is regularized by a decentralized administrative policy [5].

Limits: difficulty of administration and limitation of the access to the objects according to the identity of the user.

2.2 Mandatory Access Control (MAC)

The MAC model has a security policy which is set and managed by an authority, and cannot be modified by users. This excludes problems related to information leaks (using Trojans) observed in the DAC model. This is mainly due to not allowing users to interfere with the access control policy [5]. Unlike discretionary access control policies, subjects of a mandatory access control policy do not own the information which they have access to. Moreover, the operation allowing the delegation of rights is controlled by the rules of the policy. Subjects no longer have control over the information they handle. The subject has access to information only if authorized by the system [1].

Limits: Vulnerable to hidden channels, does not taking into account the administration component in role management, does not take into account delegation issues and level of trust

2.3 Role-Base Access Control (RBAC)

The role-based access control model, or RBAC, is seen as an alternative approach to mandatory access control (MAC) and discretionary access control (DAC). Its security policy does not apply directly to users [2, 8, 11]. The RBAC model is centered on the role [9, 10, 12]. The latter represents in an abstract way a function or a profession within an organization, which associates the authority and responsibility entrusted to a person who plays this role (for example, Professor, Director, Engineer, Technician …). Each role is assigned permissions (or privileges), which are a set of rights corresponding to the tasks that can be performed by that role. A role can have multiple permissions, and a permission can be associated with multiple roles. Just as a subject can have several roles, a role can be performed by several subjects [5].

Limits:

- No role delegation [7].
- Preserving Privacy not taken into account.
- Doesn't express prohibitions, recommendations or obligations.

2.4 Organization Based Access Control (OrBAC)

In any organization, the administrator is responsible for managing each user's access to a resource, applying security rules. But managing access rights becomes complex as the number of users, resources and activities increases. In this context, the OrBAC model solves this problem by creating abstract entities (Role, View, activity) separated into concrete entities (Subject, Object, Action). The objective of this separation is to apply the security rules to abstract entities, and to each such entity, a concrete entity is associated. OrBAC defines four types of safety rules: Permission, obligation, prohibition and recommendation [6, 10].

Limitations: No delegation nor preserving privacy.

Figure 1 below shows the OrBAC model.

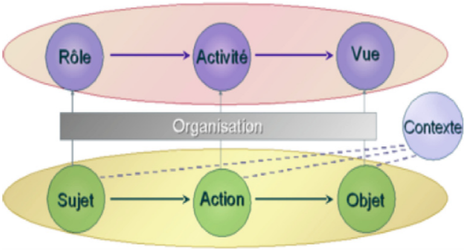


Fig. 1. Structure of OrBAC model

2.5 Synthesis of the Literature Review

We made a study of the most famous access control models. Each of them presents benefits and limits. The static access control models, the most advanced of which is RBAC, have a large limit due to its none-dynamicity. Several models, such as TrustBAC, TRBAC, have been proposed with the aim of partially improving it, but none of them to our knowledge integrates the parameters concerning the delegation and preserving privacy. We introduced too Dynamic access control models, the most advanced of which is OrBAC. Unfortunately, the latter, despite its dynamic side and its ability to manage permissions, prohibitions, obligations, recommendations, doesn't take into account some important parameters already existing in the RBAC model extensions and also like RBAC, delegation and data privacy. The limitations observed in this synthesis justify our choice to propose a dynamic model that will take into account delegation and data privacy.

3 Proposed Model (DORBAC)

3.1 Description of Non-monotonic Logic T-JClassic$\delta\varepsilon$

The non-monotonic logic T-JClassic$\delta\varepsilon$ was developed to permit a better management of the time aspect in a variety of domains such as reasoning about actions and plans, enhancing natural languages comprehension and also allowing the improvement of access control. T-JClassic$\delta\varepsilon$ allows representing temporal concepts while having default knowledge. It's Differing from the existing temporal description logics where temporal components are added to classical description logics. T-JClassic$\delta\varepsilon$ consists of: a set of atomic concepts P and atomic roles R, the two constants $\top$ (Top) and $\perp$ (Bottom) that represent respectively the universal and the bottom concept, a set of individuals called 'classic individuals', the concepts C and D, the unary connectives δ(Default) and ε(Exception), the binary conjunction π , the quantifier that enables universal quantification on role values, and the temporal qualifier @ to represent the interval 'X' at which a concept C applies, u is a real number, n is an integer, "Ii" are 'classic individuals' [3].

3.2 Description of Proposed Model

The Delegation and Organization Based Access Control Model (DORBAC) is an extension of the OrBAC model. The central element of this model is delegation, while taking into account confidentiality. We describe our model in an environment of e-health in which several nurses and doctors are involve. Whereas the nurse is a key player in the manipulation of patient data, here the role of the latter is limited to the material level. He will then be responsible for connecting the sensors to the patients and thus the collected information will be stored directly in a database. The doctors, licensing by the delegation, will then be able to delegate the roles. We define the doctor as follows:

$$\begin{aligned}&\text{Doctor} \equiv \text{Staff\_Member} \sqcap \text{Attribute\_Member} \sqcap \text{Licence\_assigment} \sqcap \\ &\text{Role\_Assigment} \sqcap \delta\text{Permission}\end{aligned} \tag{1}$$

The definition of the user Doctor gives to him the right of access to the services of the environment of the connected objects. Each doctor receives a license that will allow him to delegate his role to another doctor with the same attributes and/or additional attributes.

Role assignment can be considered as the first step of authorization. The assignment of license is considered as the second step. This gives the right to a user, to delegate his role to his colleague, who has the same attributes as him. The definition of a role and a permission translates into the following axioms:

- Role: given U_P the universe of all permissions, role R is the finite permission set. In other words,

$$R = \Sigma P_i / \ Pi \in U_P \tag{2}$$

- Permission: given U_{OIoT} the universe of all the objects of the Internet of Things, U_s the universe of services offered by the connected objects and U_{OPS} the universe of all operations allowed to a subject, a permission P is represented by the triplet (O_i, S_i, OPS_i) where $O_i \in U_{OIoT,}$ $S_i \in U_s$ and $OPS_i \in U_{OPS}$.

$$P = \Sigma O_i + \Sigma S_i + \Sigma OPS_i \tag{3}$$

$$\begin{aligned} \delta\text{Permission} = {} & \text{ObjectConntedP.permission} \sqcap \text{ServiceP.permission} \sqcap \\ & \text{OperationP.permission} \end{aligned} \tag{4}$$

3.2.1 Assignment of Role and License

- Role assignment for the doctor:

$$\begin{aligned} & \delta\text{Role\_Assigment} \sqsubseteq \text{OrgR.Assignee} \sqcap \text{AssigneeR.assigment} \sqcap \text{RoleR.assigment} \sqcap \\ & \delta\text{PrivilegesR.Service} \sqcap \delta\text{PrivilegesR.ObjectConnected} \end{aligned} \tag{5}$$

- Licensing of the doctor

$$\begin{aligned} & \delta\text{Licence\_Assigment} \sqsubseteq \text{OrgL} \sqcap \text{AssigneeL.assigment} \sqcap \text{LicenceL.assigment} \sqcap \\ & \delta\text{PrivilegesL.Action} \sqcap \text{CibleL.Objet} \sqcap \text{ContextL} \end{aligned} \tag{6}$$

3.2.2 Role Delegation

In our work, we consider the total delegation of role in which physicians with the same attributes can delegate themselves roles. Attributes represent the set of characteristics to determine a subject, a service or an object. A doctor may also delegate his role to another doctor with more attributes than him. Role delegation is represented by the following axiom:

$$\begin{aligned} & \text{Empower} \sqsubseteq \text{UserRD.Role\_Delegation} \sqcap \text{AttributeRD.Role\_Delegation} \sqcap \\ & \text{AssignmentRD.Role} \sqcap \text{ServiceRD.Service} \sqcap \text{Object\_ConnectedRD.Object} \sqcap \\ & \text{AssigneeRD.Grantor} \sqcap \text{Working\_HourRD.hour} \end{aligned} \tag{7}$$

The revocation of delegation can be represented as follows:

$$\begin{aligned}&\delta\text{Permission } \sqsubseteq \text{UseL.License\_Delegation} \sqcap \text{AssigneeL\_Assignee} \sqcap \\ &\text{AttributeRD.Role\_Delegation} \sqcap \text{DurationEndL.Licence\_Delegation} \sqcap \\ &\text{PermisionD.GD\_Revoke}\end{aligned} \tag{8}$$

3.2.3 Privacy

Privacy is another important issue [18] to considering domains such as crisis management. In the context of the management of data collected via connected objects (sensors), the protection of privacy in access control takes into account two dimensions, namely, the privacy of the connected object and the privacy of the subject (patient).

Preserving the privacy of the connected object is close to trust issue. Thus, a record stored in a database via the sensors is protected by a user if the user requests access to the information for a purpose other than that associated with him. The protection of the privacy of the object states that the access of a subject will affect the attributes assigned to him. The privacy of the patient is preserved in that the information is received at the sensor and stored directly in the database without the intervention of a data entry agent.

Purpose assignment function:

$$\begin{aligned}&\text{Purp\_assign}(\text{subject.ATTR}, O_{\text{IOT}}.\text{ATTR},\ \text{Ops.ATTR},\ \text{service.ATTR}) = \text{purp\_attr} \\ &(\text{subject.ATTR}) \subseteq \text{purp\_attr }(\text{service.ATTR}) \subseteq \text{purp\_attr }(O_{\text{IOT}}.\text{ATTR}) \subseteq \text{purp\_attr} \\ &(\text{service.ATTR}) \in \{0, 1\}\end{aligned} \tag{9}$$

Purp_attr is a function that returns the attribute of the set of goals of a subject, a connected object, a service, or an operation.

3.3 Comparison Between DORBAC and State-of-the-Art Models

Table 1 shows that compared to the models presented in the state of the art, our model is more comprehensive and reliable in terms of flexibility and privacy. Moreover, it is easy to implement.

Table 1. Comparison between DPORBAC and other models

Criteria of comparison	DAC	MAC	RBAC	ORBAC	DORBAC
Contrôle d'accès	✓	✓	✓	✓	✓
Contextual rules	x	x	x	✓	✓
Centralized administration	x	✓	x	x	✓
Privacy	x	x	x	x	✓
Dynamic	x	x	x	✓	✓
Delegation/revocation	x	x	x	x	✓
Permission, recommendation, prohibition, obligation	x	x	x	✓	✓
Collaboration	x	x	x	x	✓

Concerning the flexibility of our model, consultations and decisions are not the responsibility of only a single physician. Collaborative work between physicians is taken into account and role delegation is done dynamically. Confidentiality is also taken into account. We can deduce that our model has additional advantages compared to the models presented above in the state of the art.

4 Implementation of Our Model

4.1 Description of the Proposed Architecture

The architecture above allows to set up a platform using Node.js, Kamailio-IMS and KMS. This platform makes it possible, on the one hand, to establish a multimedia communication between two users simply by using their browser or their SIP account and, on the other hand, it allows the users to access the data of the predefined connected objects. The proposed architecture consists of three distinct entities: Web of Things (WoT), Application Programming Interface (API) and Web Application (Fig. 2).

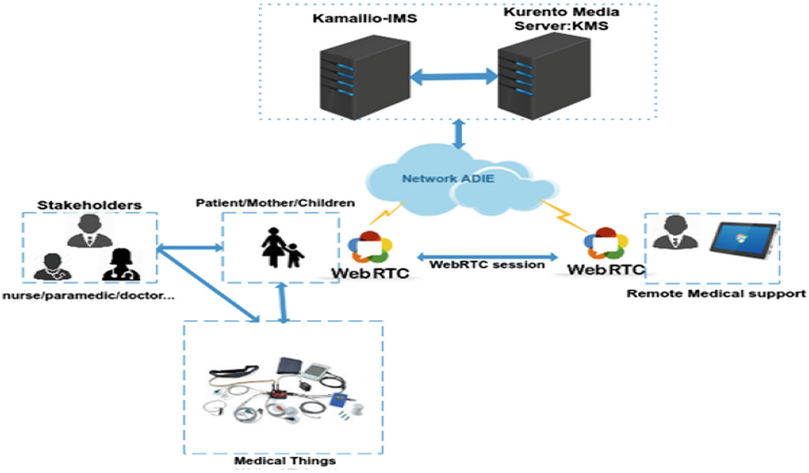


Fig. 2. Architecture of the proposed solution

4.2 Entities of the Proposed Architecture

WoT: represents the first part. Each endpoint is considered a gateway to its set of smart objects. In addition, each user has control over these objects. The NODEMCU ESP8266 aggregation node (Raspberry) is not responsible for reading the sensors. It simply provides a gateway between the user and the sensor network, and then performs data analysis. The sensor node is the lowest level of a sensor network. It is responsible for gathering information from sensors, performing user actions, and using communication mechanisms to send data to the aggregation node.

The ESP8266 gateway can then communicate with the sensors using one of the well-known communication protocols (Lora, Zigbee, Bluetooth, WIFI …). In the platform we put in place, a DHT11 humidity and temperature sensor is used. The latter is connected to the NODE MCU gateway (ESP8266) which sends the sensor data using WIFI.

In the case of e-health scenarios, we just need portable medical sensors. They can communicate via any protocol, since the WoT summarizes the complexity of the connectivity of objects.

Using the current architecture, an implementation of the remote clinical examination is possible. The doctor can then communicate with a patient using Kurento Media Server. The specialist or generalist doctor has access to a set of sensors. It can process the information collected by these sensors in real time, using the K-2I-E-health platform. Finally, these data can be analyzed and commented by the actors.

Figure 3 below shows the wiring of the Node MCU Gateway with the DHT11 temperature and humidity sensor.

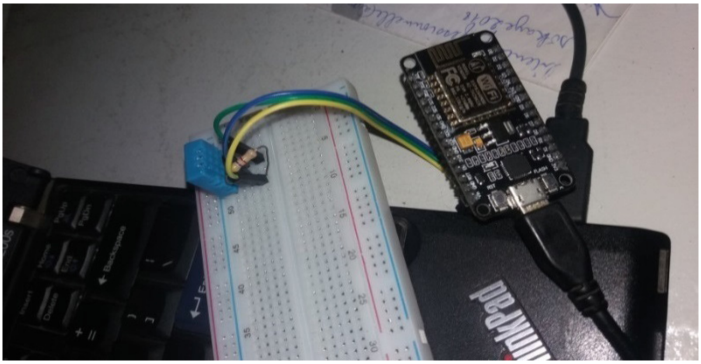


Fig. 3. Wiring the ESP8266 with the DHT11

4.3 API

We have developed a REST API capable of retrieving information collected by a connected medical device and storing it in a MongoDB database. MongoDB belongs to the NoSQL family Document-store, developed in C++. It is based on the concept of a key-value pair. The document is read or written using the key. MongoDB supports dynamic queries on documents. Since this is a document-oriented database, the data is stored as JSON, BSON style [13].

According to recent work [14–16], NoSQL database systems are non-relational databases designed to provide great accessibility, reliability and scalability to huge data. NoSQL databases can store unstructured data such as e-mails and multimedia documents. MongoDB has many security risks that can be overcome by a good, secure cryptographic system [17].

4.4 Web Application

To set up the web application, we use the NodeJs and Kurento Media Server technologies. This platform allows doctors and patients to register and authenticate themselves to access Kurento Media Server features. Once connected, the specialist physician (pediatrician) can view the sensor data and the patient's media flow (Figs. 4, 5 and 6).

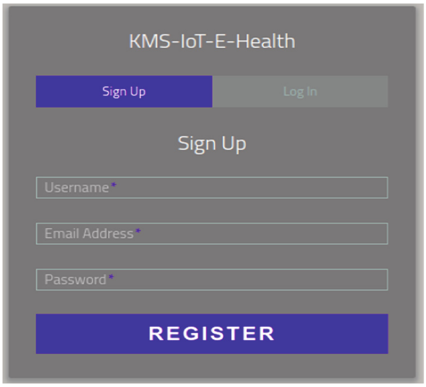


Fig. 4. Authentication on the K-2I-E-health

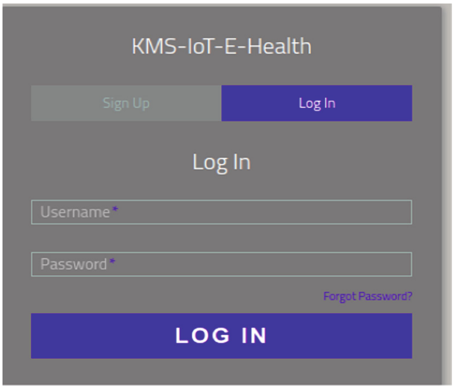


Fig. 5. Login on the K-2I-E-health

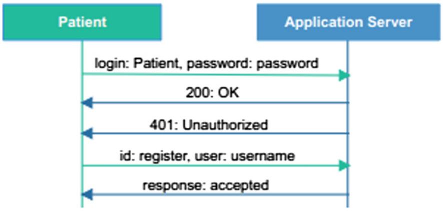
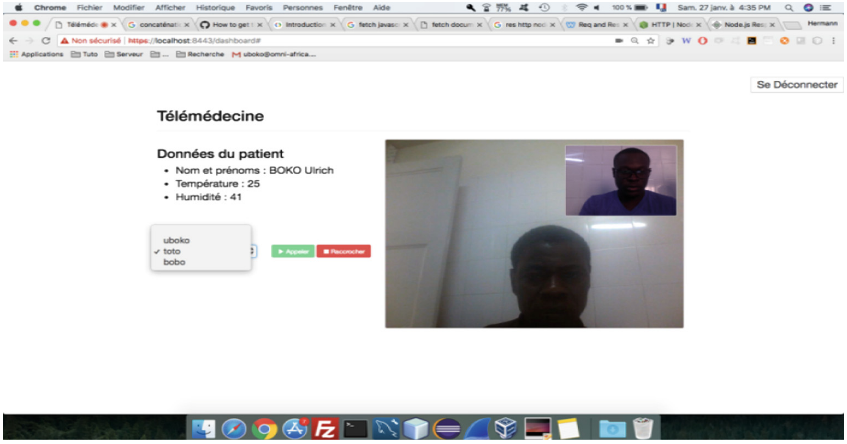


Fig. 6. Patient Authentication on the E-health Platform

The web application can also collect information from the database and display it. Connected users can then view sensor data. Figure 7 shows that actors can access the temperature and humidity sensor information. The same mechanism is applicable to any other sensor (Fig. 8).



Télémédecine

Données du patient

- Nom et prénoms : BOKO Ulrich
- Température : 25
- Humidité : 41

uboko
✓ toto
bobo

Fig. 7. Communication between Doctor toto and patient Boko Ulrich

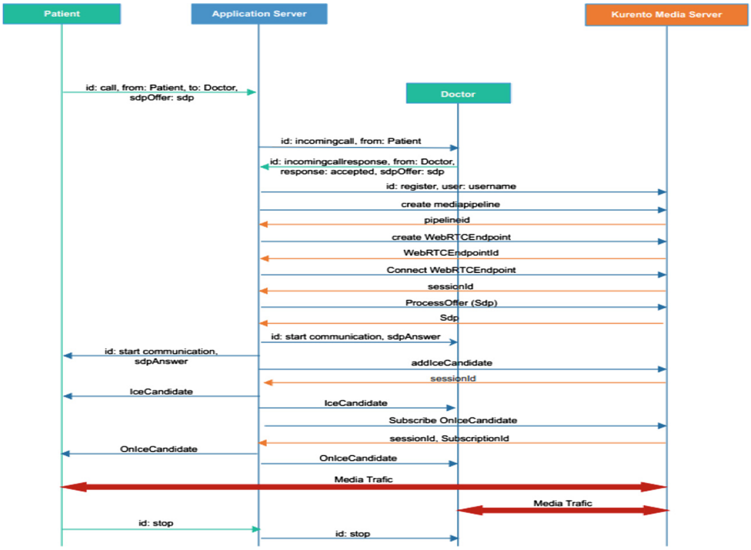


Fig. 8. Diagram of communication between Patient and Doctor

5 Conclusion

In this paper, we have proposed the DORBAC model, which is an extension of the OrBAC model. Our model makes it possible to take in to account the delegation of roles while ensuring the protection of the privacy of the patient. Thus, the proposed model allows for delegation only between physicians. The application of our model does not allow patient data capture by a health worker or assistant. The risk of seizure error is thus eliminated and the confidentiality of the patient preserved. Once the patient is connected to the sensors, its data are analyzed by the sensor network using the ESP8266 gateway, collected by the sensor node before being stored in the database. The patient or doctor with the required permissions can view the stored data via the application interface. The doctor can follow the patient and make a decision based on information received from the sensors. A videoconferencing session is then possible between the patient and the doctor.

References

1. Zerkouk, M.: Modèles de contrôle d'accès dynamiques (Doctoral dissertation, University of sciences and Technology in Oran) (2015)
2. El Kalam, A.A., et al.: Or-BAC: un modèle de contrôle d'accès basé sur les organisations. Cahiers francophones de la recherche en sécurité de l'information **1**, 30–43 (2003)
3. Bettaz, O., Boustia, N., Mokhtari, A.: Dynamic delegation based on temporal context. Procedia Comput. Sci. **96**, 245–254 (2016)
4. Abakar, M.A.: Etude et mise en oeuvre d'une architecture pour l'authentification et la gestion de documents numériques certifiés: application dans le contexte des services en ligne pour le grand public (Doctoral dissertation, Saint Etienne) (2012)
5. Ennahbaoui, M.: Contributions aux contrôles d'accès dans la sécurité des systèmes d'information (2016)
6. Ghorbel-Talbi, M.B., Cuppens, F., Cuppens-Boulahia, N., Bouhoula, A.: Managing delegation in access control models. In: International Conference on Advanced Computing and Communications. ADCOM 2007, pp. 744–751. IEEE, December 2007
7. Ray, I., Mulamba, D., Ray, I., Han, K.J.: A model for trust-based access control and delegation in mobile clouds. In: Wang, L., Shafiq, B. (eds.) DBSec 2013. LNCS, vol. 7964, pp. 242–257. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-39256-6_16
8. Zhang, L., Ahn, G.J., Chu, B.T.: A rule-based framework for role-based delegation and revocation. ACM Trans. Inf. Syst. Secur. (TISSEC) **6**(3), 404–441 (2003)
9. Chakraborty, S., Ray, I.: TrustBAC: integrating trust relationships into the RBAC model for access control in open systems. In: Proceedings of the Eleventh ACM Symposium on Access Control Models and Technologies, pp. 49–58. ACM, June 2006
10. Miege, A.: Definition of a formal framework for specifying security policies. The Or-BAC model and extensions (Doctoral dissertation, Télécom ParisTech) (2005)
11. El Kalam, A.A., Deswarte, Y.: Security model for health care computing and communication systems. In: Gritzalis, D., De Capitani di Vimercati, S., Samarati, P., Katsikas, S. (eds.) SEC 2003. ITIFIP, vol. 122, pp. 277–288. Springer, Boston, MA (2003). https://doi.org/10.1007/978-0-387-35691-4_24
12. Barka, E., Sandhu, R.: A role-based delegation model and some extensions. In: Proceedings of the 23rd National Information Systems Security Conference, vol. 4, pp. 49–58, December 2000
13. Truică, C.O., Boicea, A., Trifan, I.: CRUD Operations in Mon-goDB. In: International Conference on Advanced Computer Science and Electronics Information, pp. 347–348 (2013)
14. Chopade, M.R.M., Dhavase, N.S.: Mongodb, couchbase: performance comparison for image dataset. In: 2017 2nd International Conference for Convergence in Technology (I2CT), Mumbai, pp. 255–258 (2017)

15. Jose, B., Abraham, S.: Exploring the merits of NoSQL: a study based on mongodb. In: 2017 International Conference on Networks & Advances in Computational Technologies (NetACT), Thiruvanthapuram, pp. 266–271 (2017)
16. Patil, M.M., Hanni, A., Tejeshwar, C.H., Patil, P.: A qualitative analysis of the perfor-mance of MongoDB vs MySQL database based on insertion and retriewal operations using a web/android application to explore load balancing—Sharding in MongoDB and its advantages. In: 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, 2017, pp. 325–330 (2017)
17. Kumar, J., Garg, V.: Security analysis of unstructured data in NOSQL MongoDB data-base. In: 2017 International Conference on Computing and Communication Technologies for Smart Nation (IC3TSN), Gurgaon, India, 2017, pp. 300–305 (2017)
18. Smari, W.W., Clemente, P., Lalande, J.F.: An extended attribute based access control model with trust and privacy: application to a collaborative crisis management system. Future Gener. Comput. Syst. **31**, 147–168 (2014)