IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 4 February 2024, accepted 11 March 2024, date of publication 19 March 2024, date of current version 26 March 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3379300

RESEARCH ARTICLE

Blockchain-Based Authorization Mechanism for Educational Social Internet of Things

OLFA DALLEL, (Member, IEEE), SOUHEIL BEN AYED, AND JAMEL BEL HADJ TAHAR
NOCCS Laboratory, National Engineering School of Sousse, University of Sousse, Sousse 4002, Tunisia
Corresponding author: Olfa Dallel (olfa.dallel.noccs@gmail.com)

ABSTRACT The Social Internet of Things (SIoT) paradigm has been integrated in the education domain to enable educational IoT devices to establish social relationships and exchange academic services. Nonetheless, the social relationships are not adapted to the educational context where devices must be socially linked based on their academic roles and activities. Furthermore, the exchange of services raises the requirement to implement an access control mechanism. In SIoT, social constraints such as the social relationship type and contact frequency are critical requirements to make an access decision. However, these constraints cannot be specified using the eXtensible Access Control Markup Language (XACML) standard as device attributes nor as contextual conditions. In this paper, we propose an Educational Social Internet of Things (EducationalSIoT) platform implemented as an application-specific blockchain where we define new social relationships for educational devices. To control the access to the academic services, we suggest extending the XACML policy model by considering the social requirements, and accordingly, we adjust the policy evaluation process and suggest priority-based combining algorithms. Additionally, our platform ensures the delegation of access permission by defining delegation policies and controlling the delegation operation with consideration of the social features. The simulation results show that by integrating social features, an access request is evaluated in 0.22 ms and a delegation request is evaluated in 0.32 ms. Finally, we guarantee that our platform is protected against the man-in-the-middle and replay attacks.

INDEX TERMS Access control, application-specific blockchain, authorization, delegation, educational social Internet of Things.

I. INTRODUCTION

Education without technology becomes worthless. With the new advances in Information and Communication Technology (ICT) and its impact in transforming domains, several educational institutions (e.g. schools, universities) invest to incorporate the Internet of Things (IoT) technology [1]. The IoT transforms the traditional education to smart education [2] in order to provide smart services such as smart pedagogy, smart classrooms [3] and smart administration [4]. To extend its capabilities with cooperative services such as service discovery, the IoT is combined with the social network concept [5] leading to an emerging paradigm known as the Social Internet of Things (SIoT) [6]. SIoT applies the social networking principles to the IoT [7]. It allows smart devices to become social by autonomously forming social connections with the respect of socialization rules set by their owners. In order to face the scalability of IoT devices and provide a decentralized architecture, the blockchain technology, known as Distributed Applications (DApps), has been integrated with the SIoT (e.g. BlockSIoT [8]). Nevertheless, the applicability of blockchains combined with the SIoT to the educational context faces three main challenges among others: the limitations of the DApps blockchain technology, the inadaptability of social relationships to the educational context, and the requirement to secure access to the academic services.

On the one hand, DApps such as Ethereum are widely employed for distributed architecture, no central authority, transaction logging and transparency purposes [9]. The

The associate editor coordinating the review of this manuscript and approving it for publication was Pietro Savazzi.

DApps business logic can be customized only by deploying smart contracts. However, smart contracts represent barriers to developing more complex applications due to the immature ecosystem of the solidity language. For instance, they cannot incorporate the machine learning or deep learning models [10], [11] to build smart blockchains [12] which trains data, generates models and makes smart decisions. In addition, they must be re-deployed with any new changes.

On the other hand, IoT devices deployed inside an academic institution (e.g. smart whiteboards) and handheld and wearable objects (e.g. smart glasses) leveraged in the learning process form a new sub-category of IoT known as the Internet of Educational Things (IoET) [13]. The social relationships such as the co-location and co-work relationships [6] are used for the general SIoT purposes. For instance, the instructors allow their tablets to establish co-work social relationships with the smart whiteboard during their class. However, the social relationships formed between IoET devices need to be customized for the educational context. For example, to explain a medical procedure, the instructor can share a video from his laptop to smart glasses worn by medical students and trainees [14]. The instructor laptop must establish social connections only with smart glasses that belong to students of the same class. Therefore, in addition to the social relationships proposed for SIoT, we need to define new types of social relationships that can be established between IoET devices depending on their academic roles and activities.

Moreover, the exchange of data and services between the social devices raises the requirement to control the access to these resources (i.e. data and services) [15]. To provide an effective protection and prevent unauthorized access, the eXtensible Access Control Markup Language (XACML) [16] is leveraged to implement an authorization component such as the case of the SocIoTal [17]. XACML is a fine-grained and attribute-based authorization policy specification language [18] standardised by the OASIS standards consortium. It proposes a policy model where a policy set is composed of policy sets and/or policies, and a policy contains a set of rules.

In the context of a social network of IoET devices, a social device needs to allow only devices with specific social relationship type, social similarity, trustworthiness degree, social activeness, social contact frequency and social contact duration to access their data and services. Therefore, there is an imperative requirement to express these social constraints as access requirements in XACML. The similarity, the trustworthiness and the social activeness are social device features. Thus, they can be expressed in XACML as attributes of the access requester device (i.e. subject) or attributes of the requested device (i.e. resource). However, the social relationship type, the social contact frequency and the social contact duration cannot be expressed as device attributes nor as contextual conditions. They are social features that describe the social relationship between two social devices. In addition, the XACML standard does not support the specification of the social relationship constraints as access control requirements. To settle this matter, it is interesting to answer the following question: How to incorporate the social relationship features into the XACML policies?

Furthermore, to provide an interactive course, an instructor needs to allow the student devices to interact with the devices deployed in the classroom. For instance, to enable a student to participate in the lesson and write on the whiteboard, the teacher must temporarily grant his ''write'' permission to the tablet of the selected student. The selected tablet uses the granted permission to write answers on the smart whiteboard. In this case, the access permission is obtained by a delegation operation. The delegation is the operation performed by a delegator who, if having the right to delegate, temporarily or permanently grants or transfers all or a part of his own access permissions to a delegatee. A delegation policy model [19] defines the contextual conditions as well as the delegation conditions to control the delegation operation. Similarly to access control, the social features associated with the delegator, the delegatee and their social relationship must be incorporated as social requirements in order to define the delegation policies that control the delegation operation. Therefore, we need to leverage a delegation policy model which supports the specification of these social requirements.

A. OUR CONTRIBUTIONS

To overcome the aforementioned challenges, we propose the following main contributions:

- We review the social features and we present their existing classifications. Then, we propose new classifications based on the nature, the dynamicity and the type of the feature.
- We propose an Educational Social Internet of Things (EducationalSIoT) platform implemented as an application-specific blockchain [20]. To the best of our knowledge, no existing work comes up with a proposition for an educational platform based on the social network of IoET devices and the application-specific blockchain technology.
- In order to adapt social relationships to roles and activities of IoET devices in an academic institution, we define two new types of social relationships that can be formed in an academic environment: Class Object Relationship (ClsOR) and Institution Object Relationship (InsOR).
- We extend the XACML policy model and propose a delegation policy model to specify the social constraints required for making an access decision or a delegation decision, respectively. Based on the proposed policy models, we perform the required adjustments on the data flow models and modifications on the policy evaluation processes.
- To allow access and perform delegation operations in emergency situations, we propose to assign a priority

to rules and policies and we suggest new priority-based combining algorithms to derive the access or delegation decision of the highest-priority rule or the highest-priority policy.

The rest of this paper is organized as follows. The related work, in section II, covers the access control mechanisms proposed in the literature for IoT and the solutions proposed to control the delegation of access permissions. In addition, we review the XACML extensions suggested in recent research works. In section III, we present the social features of IoT devices and their classifications. Then, we propose a nature-based, topological-based and a social feature type-based classifications. We present our blockchain based EducationalSIoT platform for smart institutions in section IV. We give details about the authorization and delegation mechanisms with the consideration of social features. We present a simulation use case and performance evaluation results in section V. In section VI, we provide the security countermeasures that guarantee a secure EducationalSIoT platform. The last section outlines the main conclusions along with the future work.

II. RELATED WORKS

In this related works section, we start by reviewing access control mechanisms proposed for SIoT and access control mechanisms leveraging the blockchain technology. Then, we review the recent research works that tend to extend and adopt the XACML standard for a specific context.

A. ACCESS CONTROL MECHANISMS

Access control mechanisms are critical to secure service and data sharing. SocIoTal [17] implements an authorization mechanism based on the XACML standard for SIoT systems. However, the XACML standard does not consider the social constraints in the access control policy specification. To integrate the social requirements in the authorization mechanism, the adaptive fine-grained access control [21] leverages the similarity of the social relationships and employs a game theory method to compute the interest similarity to grant access. However, this mechanism integrates only the social relationship type and interest similarity as social attributes to make an access decision and does not consider the features such as the trustworthiness, the contact frequency and the contact duration that can impact the access decision. In addition, it does not integrate the contextual conditions to evaluate the access request.

For multi-domain SIoT-based systems, the smart devices belong to different authority domains. In order to determine the device role in a foreign domain and get access to the required resource, the role mapping concept is leveraged between the hierarchical access control structures to map the access requester security level in its target domain [22]. However, the social conditions such as the type of the social relationship between the access requester device and the resource device are not considered in the role mapping.

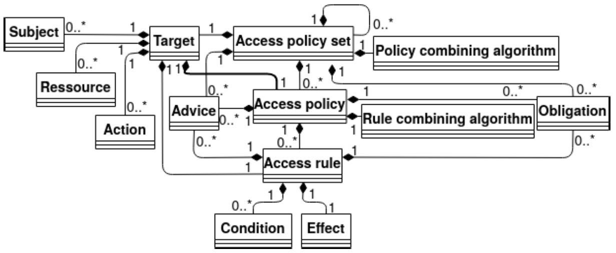


FIGURE 1. XACML-based access policy model (source [16]).

Blockchain-based access control mechanisms have been implemented to secure the access shared resources. The public key infrastructure is widely used for authentication where a user public key can be leveraged to authorize the access if this public key is specified in the authorized policy list [23]. To secure access to healthcare data in emergency situations, the smart contracts are leveraged to implement the Role-Based Access Control (RBAC) model [24]. Additionally, smart contracts play an important role in automatically executing the evaluation of the access permissions [25].

Besides, authorization can be extended by access permission delegation operation. In order to control the delegation operation, a delegation policy [19] defines the contextual conditions as well as the delegation conditions. The contextual conditions are the delegation requirements which depend on the context such as the time and the location. The delegation conditions are the delegation requirements that express the validity, the depth and the cost of the delegation operation. The validity represents the period of time during which the delegation operation can be performed. The depth is the number of times successor delegators can further perform the delegation operations. The cost is the fee paid by the delegatee once obtaining the required permission. The blockchain technology has been incorporated to secure the delegation operation. xDBAuth [26] consists of an authentication and authorization framework for Internet of Things based on the blockchain technology. It implements the authorization and delegation by leveraging the Access Control List (ACL) to specify the access requirements. However, the delegation policy model proposed in [19] and ACL-based delegation policies [26] cannot consider the social requirements to control the delegation operation.

B. XACML EXTENSIONS

The eXtensible Access Control Markup Language (XACML) [16] is a standard proposed by the OASIS consortium. It is leveraged to define the access policies and implement the authorization mechanism. It involves two main parts: (1) the policy language model as depicted in Fig. 1, and (2) the data flow model as illustrated in Fig. 2.

As depicted in Fig. 2, the XACML-based authorization mechanism, proposed in the XACML specification [16], consists of 5 entities. The Policy Enforcement Point (PEP) intercepts the access request and enforces the authorization decision. The Context Handler (CH) coordinates the

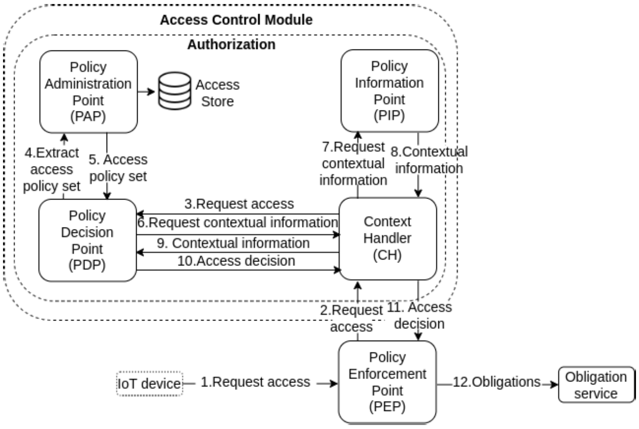


FIGURE 2. **XACML-based authorization mechanism data flow (source [16]).**

exchange of messages between different entities. The Policy Administration Point (PAP) manages and stores the access policy set. The Policy Information Point (PIP) represents the source of the contextual information. The Policy Decision Point (PDP) evaluates the access request against the access policy set and contextual information, and returns an authorization decision to the PEP.

Fig. 2 shows the data flow model which illustrates the sequence of messages exchanged between different entities of the authorization mechanism [27]. According to the XACML mechanism [16], an access requester sends a request to the PEP. The access request involves the subject (i.e. access requester), the requested resource to access and the action to perform. The PEP forwards the request to the CH. The CH first sends the access request to the PDP to check whether the access requester holds the required permission. The PDP inquires the PAP to extract the access policy set associated with the requester from the policy database. If the access policy set is found, the PDP inquires the PIP (via the CH) for the contextual information, then evaluates the access request against the access policy set and the contextual information, and returns the access decision to the CH. The CH forwards the authorization decision to the PEP.

Thanks to its simplicity, expressiveness and extensibility, XACML is extended and adapted for various specific applications and scenarios such as geospatial services [27], graph-structured data [18] and mobility [28].

GeoXACML [27] is an authorization policy specification language standardised by the Open Geospatial Consortium to secure the access to the geospatial information services such as the map visualization, conversion of coordinate systems and geospatial analysis [29]. The extensibility of the XACML standard allows the addition of new data types. GeoXACML standard adds new definitions of geometry data types (e.g. Point, LineString, LienarRing and Polygon), extends the policy model and adjusts the data flow. To evaluate policies, GeoXACML proposes new test functions (i.e. disjoint, touches, crosses, within, contains, overlaps, intersects and equals) to evaluate the topological relations expressed as condition predicates using its specific data types.

XACML for Graph (XACML4G) [18] is proposed to specify the access policies for the graph-structured data with the consideration of the patterns in terms of constraints on vertices and edges. To match the access control requirements, the policy model is adjusted by adding new elements. For instance, a pattern element is added to the XACML policy model in order to specify nodes, their connections, and characteristics on the attributes level.

XACML for Mobility (XACML4M) [28] is proposed to incorporate the mobility parameters such as the signal, the time, the frequency and the location requirements into the XACML standard. The extension of the data flow model consists of adding new entities or integrating new interactions with external entities. XACML4M incorporates the Polling Frequency Provider, Time Extensions, GeoLocation Provider entities to collect the required data for the access control.

XACML-based access control framework for security risks [30] adds a Risk Point (RP) to retrieve the risk policies and evaluate the risk attributes. Additionally, it involves a new rule evaluation algorithm which incorporates the risk threshold provided by the risk strategy to permit or deny the access. The evaluation of the rule list or the policy list produces, respectively, multiple rule decisions or policy decisions, leading to the requirement for choosing the appropriate decision. The rule-based and policy-based combining algorithms are employed to resolve the conflicts between multiple rule and policy decisions, respectively. The XACML specification proposes several combining algorithms such as permit-overrides, deny-overrides and first-applicable. To adopt the XACML-based access control for security risks, the license priority-based combining algorithm is proposed. This combining algorithm returns a license if any assessment returns a license even if other reviews have returned a denial [30].

Table 1 represents the XACML extension propositions for specific scenarios and applications in addition to different contributions (i.e. extensions) for each proposition. The extension of the XACML specification can be applied in different sub-parts: data type, policy model and data flow model. In addition, it can be extended by adjusting the decision making process as well as by proposing new rule-based and policy-based combining algorithms.

C. PROBLEM STATEMENT

Although the aforementioned related works propose solutions for access control, we aim in this work to propose an application-specific blockchain-based access control mechanism for SIoT by incorporating the social features in the access decision making. Therefore, we propose to extend the policy model of the XACML standard and adjust the policy evaluation data flow for authorization and delegation operations.

III. SOCIAL FEATURES FOR IOT DEVICES

By establishing social relationships, an IoT object becomes a social smart object and has its own social properties.

TABLE 1. XACML extension solutions.

Solution	Use case	Data type	Policy model	Data flow model	Decision making	Combining algorithm
GeoXACML [27]	Geospatial	✓	-	-	✓	-
[30]	Vehicular network big data	-	-	✓	✓	✓
XACML4G [18]	Graph-structured data	-	✓	✓	✓	-
XACML4M [28]	Connected vehicles	-	✓	✓	✓	-
Social XACML	Educational Social Internet of Things	-	✓	✓	✓	✓

These properties represent the SIoT fundamentals to consider in proposing services, trust management systems, routing protocols and security mechanisms in the social network of IoT objects. In this section, we review the social features associated with the IoT devices by giving the definition and the role of each social characteristic. Then, we discuss the classifications of the social features proposed in the literature and suggest new classifications based on the nature, the dynamicity and the type.

A. SOCIAL FEATURES

The social features refer to the metrics that describe the IoT devices in its social network [31]. They can reflect the behavior of the device in its environment [32].

1) TYPE OF SOCIAL RELATIONSHIPS

We present the social relationships according to the context of their establishment. When two objects are manufactured in the same period of time by the same company and belong to the same production batch, they form a Parental Object Relationship (POR) [6]. Therefore, they can exchange the firmware updates. Two objects fabricated by an industry maintain their social connections by establishing an Industrial Object Relationship (IOR) [33].

Based on the type of relationships between device owners, the social relationships between IoT devices can be: an Ownership Object Relationship (OOR) [6] which is established among two devices possessed by the same proprietor such as the smartphone, the tablet, the laptop, and the smartwatch, a Sibling Object Relationship (SIOR) / (SIBOR) [34] which is established among two objects which belong to two family members or two friends, a Guest Object Relationship (GUOR) / (GSTOR) [34] which is formed between devices possessed by guests, and a Stranger Object Relation (STOR) / (STGOR) [34] which is a relationship formed between objects which occasionally coexisted.

According to the provided services, the social relationships can be: a Basic Object Relationship (BOR) [33] which denotes the relationship between devices having the same primary task and belonging to the same proprietor, a Co-Work Object Relationship (CWOR) which is a relationship established between two devices which collaborate to perform the same task or provide the same service in the IoT application, and a Service Object Relationship (SEOR) / (SVOR) [34] which is established between two objects to coordinate the same service composition.

Moreover, according to the interaction between social devices, more relationships are defined. If they are geo-locally neighbors, two devices deployed in the same location can build a Co-Location Object Relationship (CLOR) [6]. Occasionally coexisted devices can establish Social Object Relationship (SOR) [6]. When two objects can establish OOR, CLOR and SOR relationships at the same time, a Mixed Object Relationship (MOR) [35] is created.

Since the object socialization is applied in various environments such as the Social Internet of Vehicles (SIoV), the Mobile Social Internet of Things (MSIoT) and the Social Internet of Industrial Things (SIoIT), the environment context can impact the type of the social relationship to establish between two objects.

In SIoV, the Guardian Object Relationship (GROR) [36] designates a hierarchical relationship that can be established between parent-child devices. For instance, the social connection between the On Board Unit (OBU) and the Road Side Unit (RSU) is a GROR social relationship where the OBU is considered as a child and the RSU as a super node. Furthermore, according to the vehicle drivers, social relationships can be [37]: a Content-oriented Driver Relationship (CDR) which denotes a social relationship between vehicles where the drivers have the same interest, a Relationship Driver Ties (RDT) which refers to a social relationship between vehicle drivers and passengers, and a Position-based Driver Relationship (PDR) which is created when the vehicles are geo-locally neighbors.

For the Internet of Mobile Things, mobility is a main property that characterizes the moving objects. These mobile devices can establish [38]: a Service Provider Object Relationship (SPOR) which is formed between devices which provide same services, a Service Requester Object Relationship (SROR) which is established between devices that request the same services in order to obtain the service from a friend which gets the service instead of getting the service from the service provider, an Explorer Object Relationship (EOR) which denotes a social connection created to search and discover services and clients and a Mobile Object Relationship (MOR) which is a social relationship created between two moving objects.

In order to provide a preventive maintenance in an industrial environment [39], the industrial assets and actors interacts with each others and can establish: Coercion Object Relationship (COR) to alert about fatigue limit, Torrid object relationship (TOR) to notify about a temperature overshoot, Corrosion Object Relationship (CROR) to alert about corrosive fluids or corrosive atmosphere, False Brinell Object Relationship (FBOR) to avoid false brinelling when external vibration occurs, True Brinell Object Relationship (TBOR) to notify about the overshoot in the elastic limit of the ring material, Spalling Object Relationship (SOR) to

TABLE 2. Classification of social relationship types.

Reference	Social Relationship	Context	Nature	Dynamicity	Diversity
Atzori *et al.* [6]	Parental Object Relationship (POR)	General	Parental	Static	Homogeneous
Arjunasamy *et al.* [33]	Industrial Object Relationship (IOR)		Parental	Static	Heterogeneous
Atzori *et al.* [6]	Owner Object Relationship (OOR)		Ownership	Static	
Roopa *et al.* [34]	Sibling Object Relationship (SIOR / SIBOR)		Friendship	Dynamic	
	Guest Object Relationship (GUOR / GSTOR)		Temporal	Dynamic	
	Stranger Object Relation (STOR / STGOR)		Temporal	Dynamic	
Arjunasamy *et al.* [33]	Basic Object Relationship (BOR)		Ownership	Static	
Atzori *et al.* [6]	Co-Work Object Relationship (CWOR)		Functionnal	Dynamic	
Roopa *et al.* [34]	Service Object Relationship (SEOR / SVOR)		Functionnal	Dynamic	
Atzori *et al.* [6]	Co-Location Object Relationship (CLOR)		Spatial	Static	
Atzori *et al.* [6]	Social Object Relationship (SOR)		Temporal	Dynamic	
Bentian *et al.* [35]	Mixed Object Relationships (MixOR)		Multi-relationship	Dynamic	
Alam *et al.* [36]	Guardian Object Relationship (GROR)	SIoV	Hierarchical	Dynamic	
Loscri *et al.* [37]	Content-oriented driver relationship (CDR)		Functionnal	Dynamic	
	Relationship driver ties (RDT)		Friendship	Dynamic	
	Position-based driver relationship (PDR)		Spatial	Dynamic	
Esfahani *et al.* [38]	Service Requester Object Relationship (SROR)	MSIoT	Functionnal	Dynamic	
	Service Provider Object Relationship (SPOR)		Functionnal	Dynamic	
	Explorer Object Relationship (EOR)		Functionnal	Dynamic	
	Mobile Object Relationship (MOR)		Temporal	Dynamic	
Roopa *et al.* [39]	Coercion Object Relationship (COR)	SIoIT	Functionnal	Static	
	Torrid Object Relationship (TOR)		Functionnal	Static	
	Corrosion Object Relationship (CROR)		Functionnal	Static	
	False Brinell Object Relationship (FBOR)		Functionnal	Static	
	True Brinell Object Relationship (TBOR)		Functionnal	Static	
	Spalling Object Relationship (SOR)		Functionnal	Static	
	Back Freight Object Relationship (BFOR)		Functionnal	Static	
	Withered Object Relationship (WOR)		Functionnal	Static	
	Defile Object Relationship (DOR)		Functionnal	Static	

alert about a marked increase in the vibrations generated by the machine elements, Back Freight Object Relationship (BFOR) to inform about an early failure of machine elements, Withered Object Relationship (WOR) to alert about a deficiency in the lubrication of the machine elements, and Defile Object Relationship (DOR) to notify about a contamination in the operating area.

Table 2 provides the main characteristics of each social relationship. For each relationship, we indicate the context of usage as well as the nature, the dynamicity and the diversity of the social relationship. The diversity refers to the ability of establishing social relationships with heterogeneous IoT devices.

2) CENTRALITY

The centrality refers to the interconnectedness of an object in the social network [40]. It reflects the importance of the device in the social network. A device with a high centrality represents a central node in the social network. It can communicate and interact with many devices. It plays an important role in the data transmission and participates in the network navigability, service discovery, network traffic and routing [31], [41], [42].

Multiple measures of centrality have been proposed in literature [40], [43]. The degree centrality represents the number of friend objects connected to an object. For mobile devices, since the objects are continuously in a moving situation, there would be frequent change in the friend relationships. Therefore, the mobility produced a dynamic social friendship network / topology. This can affect the centrality degree of a social object. The betweenness centrality represents the participation frequency of a device to be a node of the shortest paths between any two nodes in the social network. The closeness centrality is a centrality based on the distance. The less the distance between devices is, the higher closeness centrality is. The eigenvector centrality means that a device connected to devices with high centrality can impact the centrality of the node itself.

3) SOCIAL ACTIVENESS

The social activeness represents the degree of contribution of a device to a community [44], [45], [46]. The higher social activeness the device is, the more popular the device is.

4) SIMILARITY

The similarity is a social feature that characterizes a group of devices which share the same common characteristics such as the interests, geographical locations, needs [47] and preferences [44]. The similarity metrics can be [48]: the community-of-interest similarity which is calculated based on the interest similarity. The social communities are created based on the type of social relationships [49] such as a co-location-based community which groups the devices deployed in the same location or ownership-based community which involves the devices which belong to the same owner. The friendship similarity is leveraged to describe devices which share the same friend devices. The co-work similarity refers to devices which collaborate to accomplish a common task in an IoT application. The content similarity

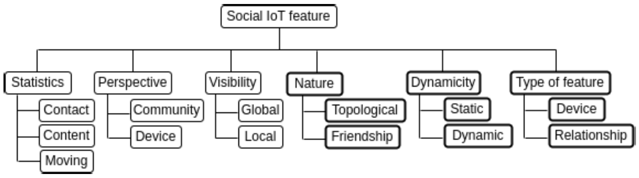


FIGURE 3. Social feature classification catagories.

is associated with two objects which share a common interest in the content during a period [50].

5) TRUSTWORTHINESS AND REPUTATION

The trustworthiness refers to the reliability of an object or the services provided by an object [51]. The evaluation of the trustworthiness is performed by a trustor which provides a qualitative or quantitative property of a trustee [52] such as a trust score. A trust score can be computed in a subjective or objective manner based on single or multiple and various metrics such as the behavior, the honesty, the cooperativeness and the community interests, the feedback, the object credibility and the centrality, as well as the social contact and the community of interest [53]. The indirect trust refers to the reputation. The reputation score is computed based on the evaluation performed by friend objects.

6) CONTACT FREQUENCY

The social contact represents the contact intensity or the number of times the friend devices establish communication to exchange data and services. It represents an indicator of closer [53] or irregular social relationship [54].

7) CONTACT DURATION

The contact duration refers to the amount of time spent during the communication. The friend device having the longest contact duration represents a permanent social friend.

B. CLASSIFICATIONS OF SOCIAL FEATURES

There have been research works [41], [55] that proposed various classifications of the social features. Fig. 3 depicts the social feature classification categories for SIoT and Table 3 represents a classification of the social features in different categories.

1) STATISTICS-BASED CLASSIFICATION

The social features can be classified based on the statistics nature of the features including the contact statistics and the content statistics [41]. The contact statistics, such as the centrality, the contact frequency and the contact duration, ensures robust connections between devices. The content statistics are related to the exchanged data or common interests such the similarity of the content interests.

2) PERSPECTIVE-BASED CLASSIFICATION

The perspective classification categorizes a social feature based on its belonging to the device or the community of devices. The individual social feature is specific to a single IoT device, whereas the common social feature characterizes a set or a community of the social devices. The centrality, the trustworthiness, the activity, the contact frequency and the contact duration are social features that describe a device, whereas the similarity is considered as a common social feature and is leveraged for the community detection and recommendation task [44].

3) VISIBILITY-BASED CLASSIFICATION

The social features can be classified based on its visibility as local (private) and global (public) social metrics [41], [55]. For instance, the interest similarity of the nodes is a global feature. The trustworthiness degree is considered as a local metric whereas the reputation is considered as a global metric.

In addition to the aforementioned classifications, we propose new classifications based on the nature, the dynamicity and the type of the social features.

4) NATURE-BASED CLASSIFCATION

The social network of IoT objects has a graph structure. The graph structure has specific properties such as the centrality. We can classify the social features based on their nature: topological and friendliness features. The topological features refer to those features that represent the structure properties of the social network whereas the friendliness features are the social characteristics that describe the friendship relations between devices. In SIoT, the topological properties are leveraged for the friendship establishment and managing [56].

5) DYNAMICITY-BASED CLASSIFCATION

The social features can be classified as static and / or dynamic. The static features are unchangeable whereas the dynamic social features can change their values over the time, the device location or according to the social situation.

6) FEATURE TYPE-BASED CLASSIFCATION

The social feature can be characteristic of the social device or a feature of the social relationship. The device's social attributes characterize the social device, and the relationship's social attributes describe the social relationship that connects two social devices.

IV. BLOCKCHAIN-BASED EDUCATIONAL SOCIAL INTERNET OF THINGS PLATFORM

We propose a Social Internet of Things platform for educational institutions called EducationalSIoT platform. Our EducationalSIoT platform is built upon an application-specific blockchain. Application-specific blockchains are decentralized applications built based on the cosmos-sdk [20]. We adopt the application-specific blockchain in order to benefit from the blockchain technology features and to be able to customize its business logic to provide academic services based on the social network of IoET devices.

TABLE 3. Social feature classification.

	Statistics		Perspective		Visibility		Nature		Dynamicity		Type	
Feature	**Contact**	**Content**	**Community**	**Device**	**Global**	**Local**	**Friendship**	**Topological**	**Static**	**Dynamic**	**Device**	**Social relationship**
Centrality	✓	-	-	✓	-	✓	-	✓	-	✓	✓	-
Social activeness	-	✓	-	✓	-	✓	✓	-	✓	-	✓	-
Similarity	-	✓	✓	-	✓	-	✓	-	✓	-	✓	-
Trustworthiness & reputation	✓	-	✓	✓	✓	✓	✓	-	-	✓	✓	-
Relationship type	✓	-	-	✓	-	✓	✓	-	✓	-	-	✓
Contact frequency	✓	-	-	✓	-	✓	✓	-	-	✓	-	✓
Contact duration	✓	-	-	✓	-	✓	✓	-	-	✓	-	✓

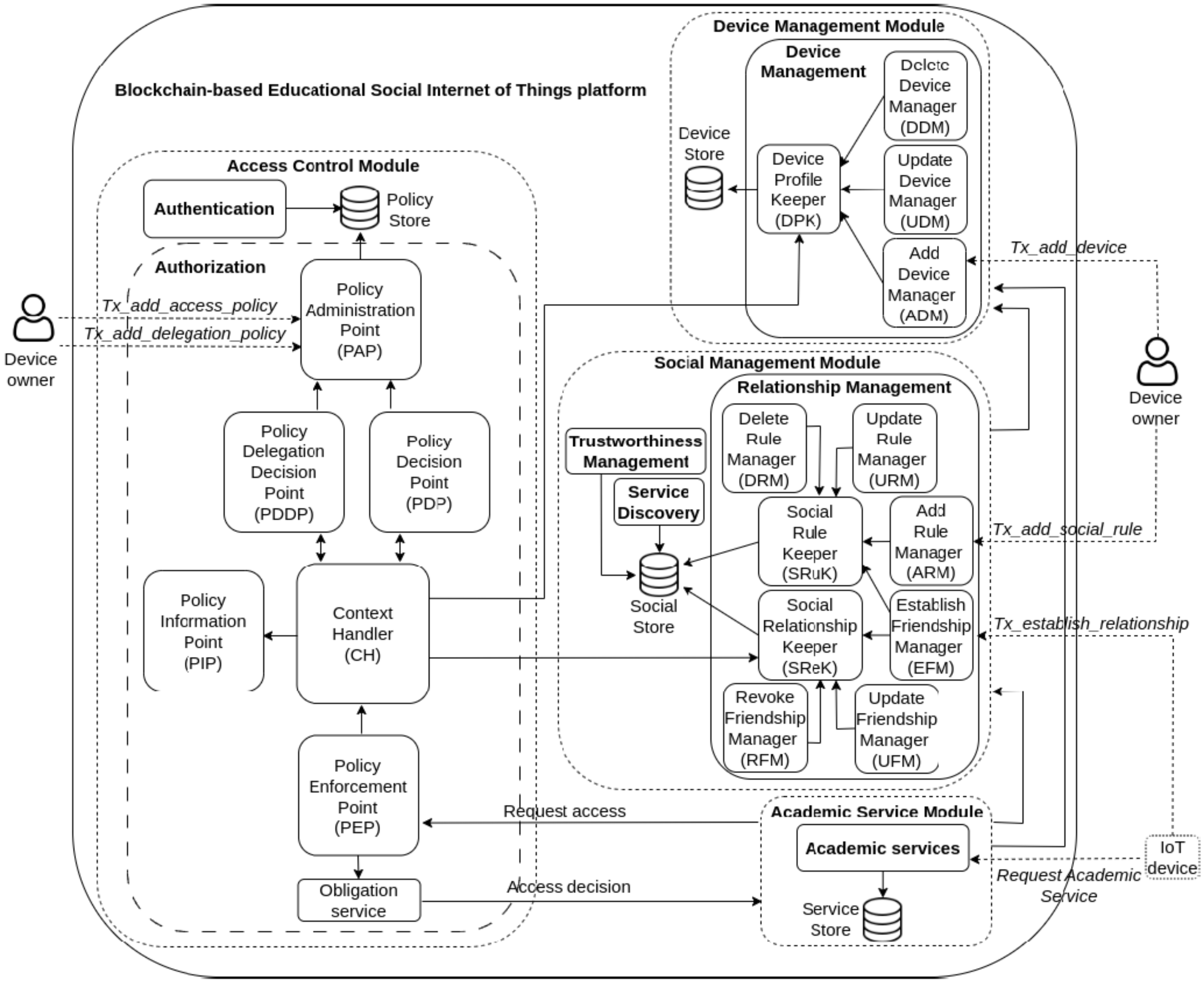

Blockchain-based Educational Social Internet of Things platform
Device Management Module
Device Management
Delete Device Manager (DDM)
Update Device Manager (UDM)
Add Device Manager (ADM)
Device Profile Keeper (DPK)
Device Store
Access Control Module
Authentication
Policy Store
Authorization
Tx_add_access_policy
Tx_add_delegation_policy
Device owner
Policy Administration Point (PAP)
Policy Delegation Decision Point (PDDP)
Policy Decision Point (PDP)
Policy Information Point (PIP)
Context Handler (CH)
Policy Enforcement Point (PEP)
Obligation service
Social Management Module
Relationship Management
Trustworthiness Management
Service Discovery
Social Store
Delete Rule Manager (DRM)
Update Rule Manager (URM)
Social Rule Keeper (SRuK)
Add Rule Manager (ARM)
Social Relationship Keeper (SReK)
Establish Friendship Manager (EFM)
Revoke Friendship Manager (RFM)
Update Friendship Manager (UFM)
Tx_add_device
Device owner
Tx_add_social_rule
Tx_establish_relationship
Request access
Access decision
Academic Service Module
Academic services
Service Store
IoT device
Request Academic Service

FIGURE 4. Blockchain-based Educational Social Internet of Things Platform.

Our EducationalSIoT platform provides IoT device management services, social relationship management services, academic services and access control. As depicted in Fig. 4, it includes following modules:

A. DEVICE MANAGEMENT MODULE

The Device Management Module (DMM) allows the management of the IoET devices. To add a device, the device owner sends a Tx_add_device transaction with the device information such as the identifier, the type, the brand, the organization and the owner. The institution administrators have the responsibilities of adding the IoET devices deployed in the institution building such as the cameras, the RFID readers, the smart timetables and the smart whiteboards. The academic institution members (e.g. teachers, students and the administration staff) are responsible for adding their personal devices such as the smartphones, the smartwatches and the laptops. As depicted in Fig. 4, the Add Device Manager (ADM) is responsible of verifying the Tx_add_device transaction, creating a device profile and storing the device via the Device Profile Keeper (DPK) in the Device Store (DS). A digital certificate is generated for the new added device. The device owner can update or remove the device profile by sending Tx_update_device transaction or Tx_remove_device transaction, respectively. The Update Device Manager (UDM) and Delete Device Manager (DDM) are responsible for the execution of the Tx_update_device transaction and Tx_remove_device transaction respectively. For simplicity, we add only the required interactions between different entities in Fig. 4.

B. SOCIAL MANAGEMENT MODULE

The Social Management Module (SMM) includes the social services provided based on the social network of IoET devices. It involves relationship management, service discovery and trustworthiness management.

To socialize their devices, the device owners must define the device socialization rules by sending a Tx_add_social_rule. The socialization rules allow or deny a device to autonomously establish social relationships with other devices. These rules are stored in the Social Store (SS) of the SMM. Additionally, the device owners can update or remove the socialization rules by executing a Tx_update_social_rule transaction or a Tx_remove_social_rule transaction, respectively. The execution of the socialization rule management transactions are handled by the Add Rule Manager (ARM), the Update Rule Manager (URM), and the Delete Rule Manager (DRM). The Social Rule Keeper (SRuK) is the entity which manages the socialization rules in the Social Store (SS).

In an SIoT environment, the IoET devices can establish the following social relationships. (1) The POR relationship denotes a relationship formed between two devices produced by the same manufacturer, since the academic institutions tend to buy their devices of the same batch and version from the same manufacturer or subcontractor. (2) The OOR relationship links two devices that belong to the same educational institution. (3) The CLOR relationship is established between two devices deployed in the same space. (4) The CWOR relationship identifies a social relationship formed by two devices which collaborate to provide the same academic service. (5) The Social Object Relationship (SOR) is formed when a device of an interim visitor establishes a social relationship with a device of an institution member or with a device that belongs to the academic institution.

The academic context requires specific social relationships. Therefore, we propose the Class Object Relationship (ClsOR) and the Institution Object Relationship (InsOR). (6) The Class Object Relationship (ClsOR) denotes a social relationship that links two devices belonging to two members of the same class. (7) The Institution Object Relationship (InsOR) denotes a social relationship that links two devices belonging to the academic members or that is formed between a member device and a device deployed in the same academic institution. We will provide examples to illustrate the applicability of these social relationships in the next section (i.e. section IV-C).

To establish a social relationship, an IoET object sends a Tx_establish_relationship transaction to form a social connection with a target device. The relationship management service checks the socialization rules specified by the device owners. If the rules are satisfied, the social relationship is created and stored in the SS. The Tx_update_relationship transaction and the Tx_remove_relationship transaction are available to update or remove the social relationship, respectively. The execution of the friendship management transactions are handled by the Establish Manager (EFM), the Update Friendship Manager (UFM), and the Revoke Friendship Manager (RFM). The Social Relationship Keeper (SReK) is the entity which manages the social relationships in the Social Store. The service discovery provides the required functionalities to find available services on the social network of IoET devices. The trustworthiness management is leveraged to compute the trustworthiness of IoET devices based on their behavior, their feedback and their credibility. The service discovery and the trustworthiness management are out of the scope of this paper.

C. ACADEMIC SERVICE MODULE

The Academic Service Module (ASM) provides academic services such as smart administration, smart pedagogy and safety in the academic institution. Examples of services include:

1) Attendance service: Every classroom door is equipped with an RFID reader. In addition, a camera is installed at the entrance of every classroom. The RFID reader and the camera establish a CWOR relationship to detect the student attendance. Once the RFID reader detects an RFID card, the camera takes a photo of the person for face-recognition. This service collects the identifier detected by the RFID reader and identifier determined by the face-recognition technique. If there is a matching, the attendance is automatically recorded.
2) Scheduling service: This service is ensured by smart timetables which provide course scheduling details and actualities. For instance, a smart timetable can establish CWOR relationships with the smart speakers spread across the academic institution in order to inform students about the beginning of information sessions or to remind them about important events. The smart

devices of students, in particular visually impaired ones, can establish InsOR relationships with the smart timetables to get the published content and read it.

3) Classroom service: A classroom includes but is not limited to a smart whiteboard, a smart light, in addition to the laptops, tablets, smartphones, smartwatches and smart glasses of teachers and students. The classroom service provides functionalities to ensure the course delivery. In order to provide an interactive course, the laptops and tablets of teachers and students can establish ClsOR relationships to write and copy notes. The smart light can establish a CWOR relationship with the instructor laptop in order to automatically adjust the brightness when the instructor starts a slideshow to ensure a comfortable environment. Students with impaired or physical disabilities can use their tablets to record the answer, then these tablets convert the recorded speech to a text and write the textual answers to the smart whiteboard.
4) Locate free places: To find free places in the amphitheater or the institution library, a student smartphone can establish an InsOR relationship with a camera deployed inside the amphitheater or the institution library. Therefore, the student can access the camera and check the availability of the free places.
5) Safety and security: this service is leveraged to control the access at the entrance of the institution. For instance, a camera and an RFID reader, deployed at the entrance of a university, provide a service of monitoring and tracking of the institution visitors. Therefore, they establish a Co-Work relationship.
6) Emergency service: In emergency situations, the smartphones of the institution members having InsOR relationships with the cameras can access these cameras to find the safe and nearby exits.

To offer academic services, the exchange of data between IoET devices is performed by executing two transactions: the Tx_publish transaction to publish data on the blockchain on a topic associated with a specific device, and the Tx_retrieve transaction to retrieve the latest published data. The publish or retrieve operations can be performed only if the publisher or the retriever devices have the required access permissions. As illustrated in Fig. 4, ASM sends an access request to the Access Control Module (ACM) to obtain an access decision. Depending on the access decision, it either allows or denies access to the requested service (i.e. publish or retrieve data).

D. ACCESS CONTROL MODULE

The Access Control Module (ACM) involves the authentication and the authorization. The authentication mechanism leverages the digital certificates. In the following subsections, we focus on the authorization which involves the access and delegation policy management, the authorization mechanism and the delegation mechanism.

1) REQUIREMENTS FOR ACCESS CONTROL

The social features are essential factors to consider while making the access and delegation decisions in the SIoT. Thus, it is imperative to select the most suitable social characteristics that can impact the decision making. Moreover, the access control mechanism is involved during the social interactions to control the access to the requested resources. Therefore, the social interaction indicators must be involved in making this decision. On the other hand, according to the XACML specification, the authorization decision is based on the attributes that describe the access requester (i.e. subject), the attributes that describe the requested resource and the access conditions. The aforementioned type-based classification distinguishes the features associated with the social devices and the features associated with the social relationship interactions. Thus, we propose to express the social device features as the device attributes and the social interaction features as the access conditions in the policy model.

In addition to the device attributes, the social attributes to consider for the IoT devices are as follows. The centrality is considered since a central device (i.e. having a large number of friends or high centrality degree) has less chance to perform malicious operations compared to new devices joining the social network. The trustworthiness degree reflects the behavior of a device in the social network and is specified to avoid the untrusty devices. It helps in detecting the malicious devices and isolating them. The interest similarity degree enables the device owner to select the device access requester that belongs to the same social communities or can be a possible candidate to join the same social communities. The social activeness represents the degree of collaboration with other devices and the contribution of a device to a community.

Along with the contextual conditions (i.e. location, time), the social relationship constraints require to be specified as conditions. The type of the social relationship guarantees that the subject device has a specific intention of establishing a social relationship such as co-location, co-work, or ephemeral contact. The social contact frequency represents the contact intensity and it guarantees a certain number of social communications. The social contact duration refers to the amount of time spent during communication and it represents an indicator that the social contact is permanent. The date of the friendship establishment is leveraged to select specific friend devices based on their friendship periods.

2) ACCESS POLICY MODEL

As shown in Fig. 5, we propose a Social XACML-based access policy model which extends the XACML policy model [16]. The Social XACML policy model enables the device owner to specify the social attributes for the access requester device (i.e. subject), the social attributes for the object device (i.e. that provides the requested service) and the social conditions as access control requirements.

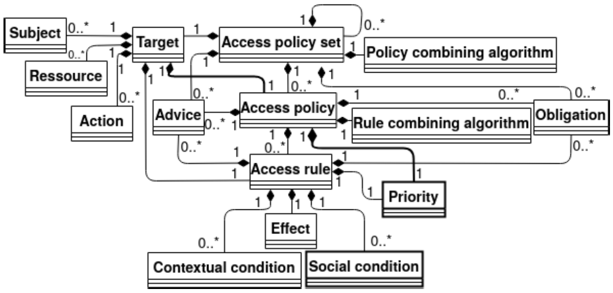


FIGURE 5. Social XACML-based access policy model.

An access policy set involves (''optionally'') a policy set, a target, a set of policies, a policy-based combining algorithm, (''optionally'') a set of obligations and (''optionally'') a set of advice. The target is used to specify the attributes of the subject that requests the access, the attributes of the resource to access (i.e object device and provided service) and the action to perform.

An access policy consists of a target, a set of rules, a rule-based combining algorithm, (''optionally'') a set of obligations and (''optionally'') a set of advice. Additionally, we propose to add a priority element in order to promote the policy which has the highest priority. We suppose that the highest priority is determined by the highest priority value.

An access rule incorporates a target, an effect, a priority, a set of contextual conditions, (''optionally'') a set of obligations and (''optionally'') a set of advice. To define the social conditions, we suggest adding the social condition element in the rule structure. The social condition is a boolean expression used to specify the type of the social relationship, the minimum or maximum value of the contact frequency, the minimum or maximum value of the contact duration and the date of social relationship establishment. The social relationship type guarantees to pick the device based on the intention of the social interaction such as co-location, co-work, or ephemeral contact. The social contact frequency guarantees a certain number of social communications and is leveraged to promote the device with which there are frequent social communications. The social contact duration represents an indicator showing that the social contact is permanent. Date of friendship establishment is leveraged to choose specific friend devices based on their friendship periods. The values associated with these social conditions are extracted from the social relationship (that links the subject to the object) stored in SS of the SMM. The new added elements (i.e. priority and social condition) are represented as a bold box Fig. 5.

In order to protect the access to its device, the device owner specifies the access policy set by sending a Tx_add_access_policy_set transaction. Once the Tx_add_access_policy_set transaction is successfully executed, the access policy set is stored in the Access Store (AS) by the PAP as illustrated in Fig. 4. The device owner also can update or remove his defined access policies by executing a Tx_update_access_policy_set transaction or a Tx_delete_access_policy_set transaction, respectively.

TABLE 4. Notation table.

Notation	Description
a	Action to perform
AT	Evaluation function of an access target
b	Brand feature of a device
CC	Evaluation function of contextual conditions
cd	Contact duration
ce	Centrality feature of a device
cf	Contact frequency
DA_d	Evaluation function of attributes of device d
Dee	Delegatee
DC	Evaluation function of delegation conditions
dc	Delegation cost
dd	Depth of delegation operation
Dor	Delegator
DT	Evaluation function of a delegation target
dty	Type feature of a device
dv	Delegation validity period
ef_x	Evaluation function of an attribute or a condition or an item x
F	False
fp	friendship period
I	Indeterminate
l_d	Location of a device d
M	Match
mo	Model feature of device
NM	Not match
o	Device object
p	Permission to delegate
rd	Number of redelegation operations
s	Device subject
SC	Evaluation function of social conditions
si	Similarity feature of a device
srt	Social relationship type
srvc	Requested service
T	True
t	Request time
tr	Trust degree feature of a device

3) SOCIAL XACML-BASED AUTHORIZATION MECHANISM

To publish or retrieve data from the blockchain, the ASM inquires an authorization decision by sending an access request to the PEP which transmits the request to the CH. Fig. 6 depicts the data flow model of the authorization mechanism. The CH (1) forwards the access request to the PDP. The PDP (2) extracts the access policy set for the specified target via the PAP from AS. Via the CH, the PDP (4) inquires the PIP to extract the required contextual attributes, (8) inquires the Device Profile Keeper (DPK) of the DMM module to extract the subject and resource profiles from the DS, and (12) inquires the Social Relationship Keeper (SReK) of the SMM module to extract the subject-resource social relationship data from the SS. Then, the PDP starts by the evaluation of the access rules. We define five evaluation functions according to the nature of the attribute, the condition or the item to evaluate. Table 4 represents the notation used in this paper.

- A score evaluation function evaluates an attribute value or a condition value based on a predefined score value. The device attributes such as the similarity, the centrality and the trust degree as well as the social conditions associated to a social relationship such as the contact

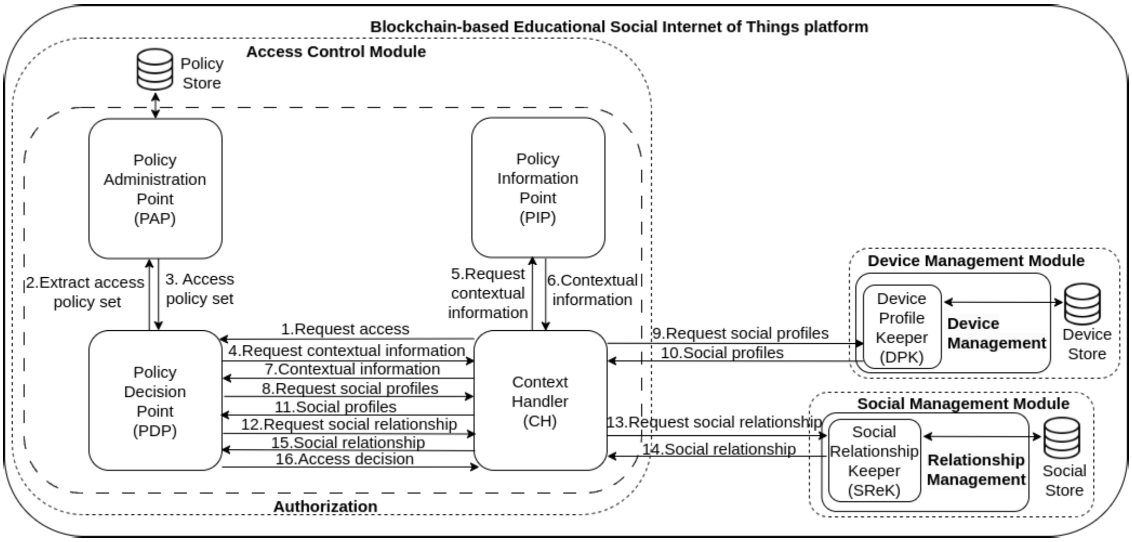

Blockchain-based Educational Social Internet of Things platform
Access Control Module
Policy Store
Policy Administration Point (PAP)
Policy Information Point (PIP)
2.Extract access policy set
3. Access policy set
5.Request contextual information
6.Contextual information
Policy Decision Point (PDP)
Context Handler (CH)
1.Request access
4.Request contextual information
7.Contextual information
8.Request social profiles
11.Social profiles
12.Request social relationship
15.Social relationship
16.Access decision
9.Request social profiles
10.Social profiles
13.Request social relationship
14.Social relationship
Device Management Module
Device Profile Keeper (DPK)
Device Management
Device Store
Social Management Module
Social Relationship Keeper (SReK)
Relationship Management
Social Store
Authorization

FIGURE 6. Authorization mechanism.

frequency, the contact duration are evaluated based on score values. The score evaluation function of x based on its score x_{score} is defined as follows:

$$score(x, x_{score}) = \begin{cases} T, & \text{if } x \diamondsuit x_{score}, \\ F, & \text{if } x \,!\diamondsuit\, x_{score}, \\ I, & \text{otherwise.} \end{cases} \quad (1)$$

where $\diamondsuit$ is a relational operator that can be $<$, $\leq$, $=$, $\neq$, $>$ or $\geq$.

- An inclusion evaluation function checks if an attribute value or a condition value belongs to a predefined set of values. The type, the brand, the model and the organization of a device as well as the type of a social relationship are evaluated based on their inclusions in predefined sets of items. The inclusion evaluation function of x based on a predefined set of items x_{set} is defined as follows:

$$inclusion(x, x_{set}) = \begin{cases} T, & \text{if } x \in x_{set}, \\ F, & \text{if } x \notin x_{set}, \\ I, & \text{otherwise.} \end{cases} \quad (2)$$

- A period evaluation function verifies if a condition value, such as the access request timing or the relationship establishment date, is in a specific interval of time. The period evaluation function of x based on $x_{notBefore}$ date and $x_{notAfter}$ date is defined as follows:

$$period(x, x_{notBefore}, x_{notAfter}) = \begin{cases} T, & \text{if } x \in [x_{notBefore}, x_{notAfter}], \\ F, & \text{if } x \notin [x_{notBefore}, x_{notAfter}], \\ I, & \text{otherwise.} \end{cases} \quad (3)$$

- A matching evaluation function which verifies if an item specified in the access request, denoted as x, matches an item predefined in the access policy set, denoted as x_{pre}. For example, the requested action and the requested service specified in the access request must match the action and the service predefined in the target of the access policy set, respectively. The matching function is defined as follows:

$$matching(x, x_{pre}) = \begin{cases} T, & \text{if } x = x_{pre}, \\ F, & \text{otherwise.} \end{cases} \quad (4)$$

The ‘‘otherwise’’ refers to a situation where x cannot be evaluated due to its absence. For the sake of simplicity, we denote an evaluation function of an attribute or a condition or an item x as ef_x.

The result of the evaluation of the access target AT is determined based on the evaluation of the subject device attributes DA_s, the matching of the action a to perform and the matching of the requested service srvc and the evaluation of the object device attributes DA_o as follows:

$$AT(s, a, srvc, o) = \begin{cases} M, \text{if } \forall x \in \{a, srvc\}/ef_x = T \\ and\ DA_s = T\ and\ DA_o = T \\ I, \text{if } \exists x \in \{a, srvc\}/ef_x = I \\ or\ DA_s = I\ or\ DA_o = I \\ NM, \text{otherwise.} \end{cases} \quad (5)$$

where DA_d is the evaluation result of the attributes of the device d and is evaluated based on the brand b, device type dty, model mo, centrality ce, similarity si, and trust degree tr as following:

$$DA_d(b, dty, mo, ce, si, tr) = \begin{cases} T, & \text{if } \forall x \in \{b, dty, mo, \\ & ce, si, tr\}/ef_x = T, \\ I, & \text{if } \exists x \in \{b, dty, mo, \\ & ce, si, tr\}/ef_x = I, \\ F, & \text{otherwise.} \end{cases} \quad (6)$$

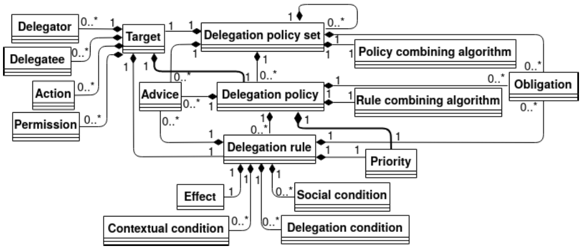


FIGURE 7. Delegation policy model.

The evaluation of the contextual conditions CC is determined based on the request timing t and the location of the subject device l_s and the location of the object device l_o as follows:

$$CC(t, l_s, l_o) = \begin{cases} T, & \text{if } \forall x \in \{t, l_s, l_o\}/ef_x = T, \\ I, & \text{if } \exists x \in \{t, l_s, l_o\}/ef_x = I, \\ F, & \text{otherwise.} \end{cases} \tag{7}$$

The result of the evaluation of the social conditions SC is determined based on the social relationship type srt, the contact frequency cf, the contact duration cd and the friendship period fp as follows:

$$SC(srt, cf, cd, fp) = \begin{cases} T, & \text{if } \forall x \in \{srt, cf, cd, fp\} \\ & /ef_x = T, \\ I, & \text{if } \exists\ x \in \{srt, cf, cd, fp\} \\ & /ef_x = I, \\ F, & \text{otherwise.} \end{cases} \tag{8}$$

The access decision is determined based on the effect that can be "Permit" or "Deny", the target evaluation result, the contextual condition evaluation result and the social condition evaluation result. Table 5 is the truth table of the access decision. The "Indeterminate{P}" and "Indeterminate{D}" refer to situations where some attributes or some conditions cannot be evaluated while the effect is "Permit" or "Deny", respectively.

Once all rules of a policy are evaluated, a rule-combining algorithm is applied to derive a single decision. In addition to the permit-overrides, deny-overrides, first-applicable combining algorithms proposed by the XACML standard, we suggest a new combining algorithm based on the priority of the rules called the highest-priority rule-based combining algorithm. The highest-priority rule-based combining algorithm sorts all the rules based on their priorities and promotes a "Permit" decision over a "Deny" decision. Thus, if multiple rules have the same priority, the first rule that returns a "Permit" decision will be applied. The authorization decision is the result of combining the set of policy decisions based on the policy-based combining algorithm. Finally, the PDP (16) returns the authorization decision.

4) DELEGATION POLICY MODEL

To define a delegation policy, we propose a new delegation policy model inspired from the XACML policy model as shown in Fig. 7.

A delegation policy set involves the following elements: ("optionally") a policy set, a target, a set of policies, a policy-based combining algorithm, ("optionally") a set of obligations and ("optionally") a set of advice. The target is used to specify the attributes of the delegator that grants or transfers his permissions, the attributes of the delegatee and the action to perform (i.e. grant or transfer) and the permission to delegate. Similarly to the subject and object devices in the access policy specifications, the delegator and delegatee attributes can be the device features or social attributes.

A delegation policy consists of a target, a set of rules, a rule-based combining algorithm, ("optionally") a set of obligations and ("optionally") a set of advice. Additionally, we propose a priority element in order to promote the policy which has the highest priority value.

A delegation rule incorporates a target, an effect, a priority, a set of contextual conditions, ("optionally") a set of obligations and ("optionally") a set of advice. In addition to the contextual conditions, we include the delegation conditions and the social conditions to the delegation policy model. The delegation condition element is included in the rule structure to specify the delegation conditions. The delegation conditions are the delegation validity, the delegation depth, the number of sub-delegatees. The social condition element in the rule structure defines the social conditions. The obligations can contain the validity and other constraints such as the delegation cost, the social relationship type, the friendship contact frequency and duration that must be integrated into the delegated access permission generated once the delegation is performed.

To manage the delegation policies, the Tx_add _delegation_policy_set transaction, the Tx_update_delegation_policy _set transaction or the Tx_delete_delegation_policy_set transaction are available to add, update or delete delegation policies, respectively.

5) DELEGATION MECHANISM

A delegation policy set is evaluated by the delegation mechanism extended from our previous work [57] as illustrated in Fig. 8. For the sake of simplicity, Fig. 8 shows only the EducationalSIoT entities required for the delegation operation. The PDDP (2) extracts the delegation policy set for the specified target via the PAP from PS. Via the CH, the PDDP (4) inquires the PIP to extract the required contextual attributes, (8) inquires the DPK of the DMM module to extract the delegator and delegatee profiles from the DS, and (12) inquires the SReK of the SMM module to extract the delegator-delegatee social relationship metadata from the SS. Then, the PDDP starts by the evaluation of the delegation rules.

The delegation decision is determined based on the effect that can be "Permit" or "Deny", the delegation target evaluation result, the contextual condition evaluation result, the delegation condition evaluation result and the social condition evaluation result. The result of the evaluation of the

TABLE 5. Truth table of the access decision.

Target	Contextual condition	Social condition	Decision
Match	True	True	Effect
		False	"NotApplicable"
		Indeterminate	"Indeterminate{P}" if the Effect is Permit, "Indeterminate{D}" if the Effect is Deny
	False	True	"NotApplicable"
		False	
		Indeterminate	"Indeterminate{P}" if the Effect is Permit, "Indeterminate{D}" if the Effect is Deny
	Indeterminate	-	"Indeterminate{P}" if the Effect is Permit, "Indeterminate{D}" if the Effect is Deny
No match	-	-	"NotApplicable"
Indeterminate	-	-	"Indeterminate{P}" if the Effect is Permit, "Indeterminate{D}" if the Effect is Deny

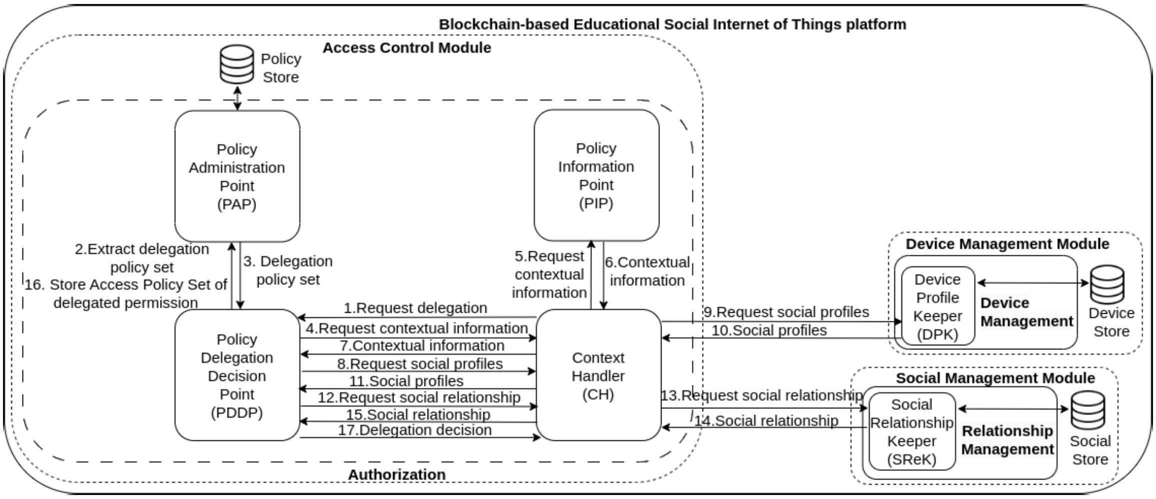

Blockchain-based Educational Social Internet of Things platform
Access Control Module
Policy Store
Policy Administration Point (PAP)
Policy Information Point (PIP)
2.Extract delegation policy set
3. Delegation policy set
16. Store Access Policy Set of delegated permission
5.Request contextual information
6.Contextual information
Policy Delegation Decision Point (PDDP)
Context Handler (CH)
1.Request delegation
4.Request contextual information
7.Contextual information
8.Request social profiles
11.Social profiles
12.Request social relationship
15.Social relationship
17.Delegation decision
9.Request social profiles
10.Social profiles
13.Request social relationship
14.Social relationship
Device Management Module
Device Profile Keeper (DPK)
Device Management
Device Store
Social Management Module
Social Relationship Keeper (SReK)
Relationship Management
Social Store
Authorization

FIGURE 8. Delegation data flow.

Delegation Target DT is determined based on the evaluation of the delegator device attributes DA_{dor}, the matching of the action a to perform and the matching of the permission to delegate p and the evaluation of the delegatee device attributes DA_{dee} as follows:

$$DT(dor, a, p, dee) = \begin{cases} T, & \text{if } \forall x \in \{a, p\}/ef_x = T \\ & and\ DA_{dor} = T\ and\ DA_{dee} = T \\ I, & \text{if } \exists x \in \{a, p\}/ef_x = I \\ & or\ DA_{dor} = I\ or\ DA_{dee} = I \\ F, & \text{otherwise.} \end{cases} \tag{9}$$

The result of the evaluation of the contextual conditions CC is determined based on equation 7 and the result of the evaluation of the social conditions SC is determined based on equation 8. The result of the evaluation of the delegation conditions DC is determined based on the delegation cost dc, delegation validity dv, delegation depth dd and number of redelegation operations rd as follows:

$$DC(dc, dv, dd, rd) = \begin{cases} T, & \text{if } \forall x \in \{dc, dv, dd, rd\} \\ & /ef_x = T, \\ I, & \text{if } \exists\ x \in \{dc, dv, dd, rd\} \\ & /ef_x = I, \\ F, & \text{otherwise.} \end{cases} \tag{10}$$

Table 6 illustrates the truth table of the delegation decision based on the delegation target, contextual conditions, delegation conditions and social conditions.

Once all rules of a delegation policy are evaluated, a rule-combining algorithm is applied to derive a single decision. The authorization decision is the result of combining the set of policy decisions based on the policy-based combining algorithm. If the delegation decision is "Permit", the PDDP creates a new access policy set for the delegated permission and (16) stores the created access policy set in the PS. Finally, it (17) returns the delegation decision to the CH.

V. SIMULATION

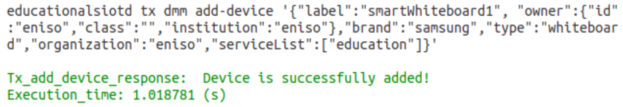
A. SCENARIO IMPLEMENTATION

We implemented the proposed EducationalSIoT platform by leveraging the cosmos-sdk [20] as a proof of concept of our solution. The cosmos-sdk proposed two types of transactions: messages and queries. A message can be leveraged to change the ledger by setting and appending data to it, whereas a query can be used to read data from the ledger. We propose a classroom service use case where the teacher and the student use their tablets to write on the smart whiteboard. The scenario steps are the following:

1) The institution administrator adds "smartwhiteboard1" device by executing the Tx_add_device transaction as shown in Fig. 9. Similarly, the teacher and the student add their tablets. A secret key is shared

TABLE 6. Truth table of the delegation decision.

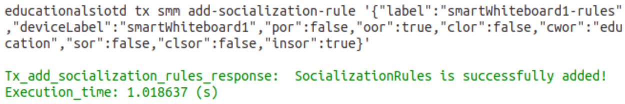
Target	Contextual condition	Delegation condition	Social condition	Decision
Match	True	True	True	Effect
			False	"NotApplicable"
			Indeterminate	"Indeterminate{P}" if the Effect is Permit, "Indeterminate{D}" if the Effect is Deny
		False	True	"NotApplicable"
			False	
			Indeterminate	"Indeterminate{P}" if the Effect is Permit, "Indeterminate{D}" if the Effect is Deny
		Indeterminate	-	"Indeterminate{P}" if the Effect is Permit, "Indeterminate{D}" if the Effect is Deny
	False	True	True	"NotApplicable"
			False	
			Indeterminate	"Indeterminate{P}" if the Effect is Permit, "Indeterminate{D}" if the Effect is Deny
		False	True	"NotApplicable"
			False	
			Indeterminate	"Indeterminate{P}" if the Effect is Permit, "Indeterminate{D}" if the Effect is Deny
		Indeterminate	-	"Indeterminate{P}" if the Effect is Permit, "Indeterminate{D}" if the Effect is Deny
	Indeterminate	-	-	"Indeterminate{P}" if the Effect is Permit, "Indeterminate{D}" if the Effect is Deny
No match	-	-	-	"NotApplicable"
Indeterminate	-	-	-	"Indeterminate{P}" if the Effect is Permit, "Indeterminate{D}" if the Effect is Deny



```
educationalsiotd tx dmm add-device '{"label":"smartWhiteboard1", "owner":{"id"
:"eniso","class":"","institution":"eniso"},"brand":"samsung","type":"whiteboar
d","organization":"eniso","serviceList":["education"]}'

Tx_add_device_response:  Device is successfully added!
Execution_time: 1.018781 (s)
```

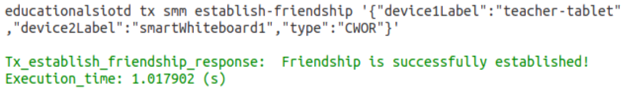
FIGURE 9. Transaction to add "smartwhiteboard1" on the EducationalSIoT platform.



```
educationalsiotd tx smm add-socialization-rule '{"label":"smartWhiteboard1-rules"
,"deviceLabel":"smartWhiteboard1","por":false,"oor":true,"clor":false,"cwor":"edu
cation","sor":false,"clsor":false,"insor":true}'

Tx_add_socialization_rules_response:  SocializationRules is successfully added!
Execution_time: 1.018637 (s)
```

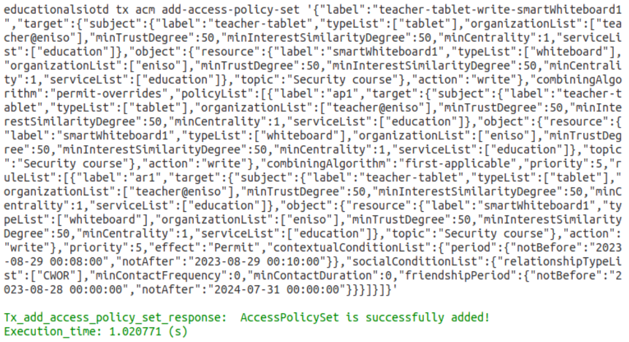
FIGURE 10. Transaction to add the socialization rules associated with "smartwhiteboard1".



```
educationalsiotd tx smm establish-friendship '{"device1Label":"teacher-tablet"
,"device2Label":"smartWhiteboard1","type":"CWOR"}'

Tx_establish_friendship_response:  Friendship is successfully established!
Execution_time: 1.017902 (s)
```

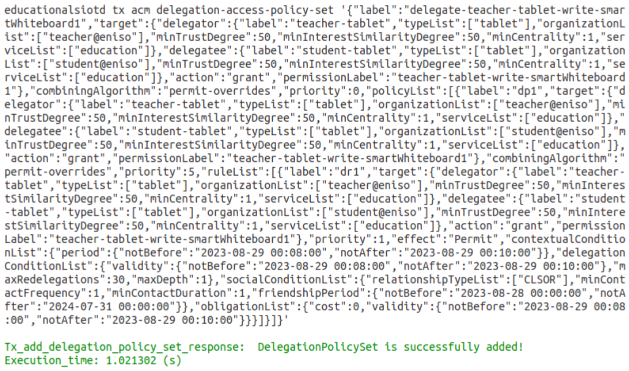
FIGURE 11. Transaction to establish friendship between the teacher tablet and "smartwhiteboard1".



```
educationalsiotd tx acm add-access-policy-set '{"label":"teacher-tablet-write-smartWhiteboard1
","target":{"subject":{"label":"teacher-tablet","typeList":["tablet"],"organizationList":["tea
cher@eniso"],"minTrustDegree":50,"minInterestSimilarityDegree":50,"minCentrality":1,"serviceLi
st":["education"]},"object":{"resource":{"label":"smartWhiteboard1","typeList":["whiteboard"],
"organizationList":["eniso"],"minTrustDegree":50,"minInterestSimilarityDegree":50,"minCentrali
ty":1,"serviceList":["education"]},"topic":"Security course"},"action":"write"},"combiningAlgo
rithm":"permit-overrides","policyList":[{"label":"ap1","target":{"subject":{"label":"teacher-t
ablet","typeList":["tablet"],"organizationList":["teacher@eniso"],"minTrustDegree":50,"minInte
restSimilarityDegree":50,"minCentrality":1,"serviceList":["education"]},"object":{"resource":{
"label":"smartWhiteboard1","typeList":["whiteboard"],"organizationList":["eniso"],"minTrustDeg
ree":50,"minInterestSimilarityDegree":50,"minCentrality":1,"serviceList":["education"]},"topic
":"Security course"},"action":"write"},"combiningAlgorithm":"first-applicable","priority":5,"r
uleList":[{"label":"ar1","target":{"subject":{"label":"teacher-tablet","typeList":["tablet"],"
organizationList":["teacher@eniso"],"minTrustDegree":50,"minInterestSimilarityDegree":50,"minC
entrality":1,"serviceList":["education"]},"object":{"resource":{"label":"smartWhiteboard1","ty
peList":["whiteboard"],"organizationList":["eniso"],"minTrustDegree":50,"minInterestSimilarity
Degree":50,"minCentrality":1,"serviceList":["education"]},"topic":"Security course"},"action":
"write"},"priority":5,"effect":"Permit","contextualConditionList":{"period":{"notBefore":"2023
-08-29 00:08:00","notAfter":"2023-08-29 00:10:00"}},"socialConditionList":{"relationshipTypeLi
st":["CWOR"],"minContactFrequency":0,"minContactDuration":0,"friendshipPeriod":{"notBefore":"2
023-08-28 00:00:00","notAfter":"2024-07-31 00:00:00"}}}]}]}'

Tx_add_access_policy_set_response:  AccessPolicySet is successfully added!
Execution_time: 1.020771 (s)
```

FIGURE 12. Transaction to add the access policy set.



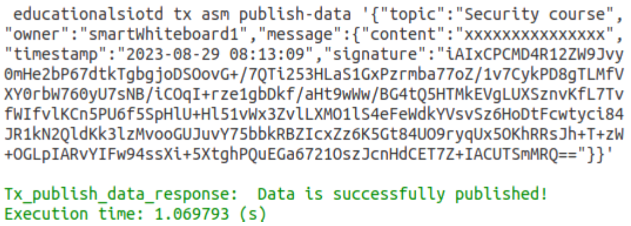
```
educationalsiotd tx acm delegation-access-policy-set '{"label":"delegate-teacher-tablet-write-smar
tWhiteboard1","target":{"delegator":{"label":"teacher-tablet","typeList":["tablet"],"organizationL
ist":["teacher@eniso"],"minTrustDegree":50,"minInterestSimilarityDegree":50,"minCentrality":1,"ser
viceList":["education"]},"delegatee":{"label":"student-tablet","typeList":["tablet"],"organization
List":["student@eniso"],"minTrustDegree":50,"minInterestSimilarityDegree":50,"minCentrality":1,"se
rviceList":["education"]},"action":"grant","permissionLabel":"teacher-tablet-write-smartWhiteboard
1"},"combiningAlgorithm":"permit-overrides","priority":0,"policyList":[{"label":"dp1","target":{"d
elegator":{"label":"teacher-tablet","typeList":["tablet"],"organizationList":["teacher@eniso"],"mi
nTrustDegree":50,"minInterestSimilarityDegree":50,"minCentrality":1,"serviceList":["education"]},"
delegatee":{"label":"student-tablet","typeList":["tablet"],"organizationList":["student@eniso"],"m
inTrustDegree":50,"minInterestSimilarityDegree":50,"minCentrality":1,"serviceList":["education"]},
"action":"grant","permissionLabel":"teacher-tablet-write-smartWhiteboard1"},"combiningAlgorithm":"
permit-overrides","priority":5,"ruleList":[{"label":"dr1","target":{"delegator":{"label":"teacher-
tablet","typeList":["tablet"],"organizationList":["teacher@eniso"],"minTrustDegree":50,"minInteres
tSimilarityDegree":50,"minCentrality":1,"serviceList":["education"]},"delegatee":{"label":"student
-tablet","typeList":["tablet"],"organizationList":["student@eniso"],"minTrustDegree":50,"minIntere
stSimilarityDegree":50,"minCentrality":1,"serviceList":["education"]},"action":"grant","permission
Label":"teacher-tablet-write-smartWhiteboard1"},"priority":1,"effect":"Permit","contextualConditio
nList":{"period":{"notBefore":"2023-08-29 00:08:00","notAfter":"2023-08-29 00:10:00"}},"delegation
ConditionList":{"validity":{"notBefore":"2023-08-29 00:08:00","notAfter":"2023-08-29 00:10:00"},"m
axRedelegations":30,"maxDepth":1},"socialConditionList":{"relationshipTypeList":["CLSOR"],"minCont
actFrequency":1,"minContactDuration":1,"friendshipPeriod":{"notBefore":"2023-08-28 00:00:00","notA
fter":"2024-07-31 00:00:00"}},"obligationList":{"cost":0,"validity":{"notBefore":"2023-08-29 00:08
:00","notAfter":"2023-08-29 00:10:00"}}}]}]}'

Tx_add_delegation_policy_set_response:  DelegationPolicySet is successfully added!
Execution_time: 1.021302 (s)
```

FIGURE 13. Transaction to add the delegation policy set.

using communication channels off the blockchain-based EducationalSIoT platform to encrypt the data published by these IoET devices.

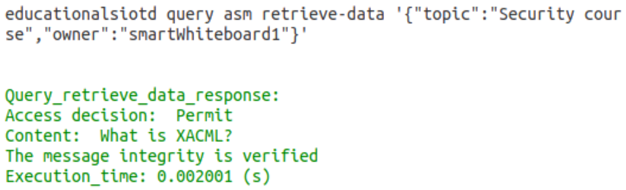
2) Each device owner specifies the socialization rules for his device by sending the Tx_add_social_rule transaction to the SMM module. Fig. 10 illustrates the types of the social relationships that "smartwhiteboard1" can establish.
3) The teacher tablet establishes a CWOR relationship with "smartwhiteboard1", as shown in Fig. 11, and a ClsOR relationship with the student tablet. Additionally, the student tablet establishes a CWOR relationship with "smartwhiteboard1". We suppose that the trustworthiness and the similarity degrees are automatically updated by the relationship management and trustworthiness management services in the SMM module.
4) The administrator specifies an access policy to allow the teacher to "publish" on the whiteboard, as illustrated in Fig. 12, and defines a delegation policy to allow the teacher to grant his "publish" permission to his student during the class. Fig. 13 shows the delegation policy associated with the teacher and the student tablets.
5) To write a question on "smartwhiteboard1", the teacher tablet encrypts the message to publish using the shared secret key, signs it using its private key and executes the Tx_publish transaction. The ASM module receives the transaction and inquires the ACM module for the authorization decision to "publish" a message on the "Security Course" topic of "smartwhiteboard1". If the decision is "Permit", then the message can be published as shown in Fig. 14.



```
 educationalsiotd tx asm publish-data '{"topic":"Security course",
"owner":"smartWhiteboard1","message":{"content":"xxxxxxxxxxxxxxx",
"timestamp":"2023-08-29 08:13:09","signature":"iAIxCPCMD4R12ZW9Jvy
0mHe2bP67dtkTgbgjoDSOovG+/7QTi253HLaS1GxPzrmba77oZ/1v7CykPD8gTLMfV
XY0rbW760yU7sNB/iCOqI+rze1gbDkf/aHt9wWw/BG4tQ5HTMkEVgLUXSznvKfL7Tv
fWIfvlKCn5PU6f5SpHlU+Hl51vWx3ZvlLXMO1lS4eFeWdkYVsvSz6HoDtFcwtyci84
JR1kN2QldKk3lzMvooGUJuvY75bbkRBZIcxZz6K5Gt84UO9ryqUx5OKhRRsJh+T+zW
+OGLpIARvYIFw94ssXi+5XtghPQuEGa67210szJcnHdCET7Z+IACUTSmMRQ=="}}'

Tx_publish_data_response:  Data is successfully published!
Execution time: 1.069793 (s)
```

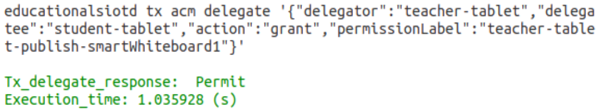
FIGURE 14. Transaction to publish a message on the "Security Course" topic of "smartwhiteboard1".



```
educationalsiotd query asm retrieve-data '{"topic":"Security cour
se","owner":"smartWhiteboard1"}'


Query_retrieve_data_response:
Access decision:  Permit
Content:  What is XACML?
The message integrity is verified
Execution_time: 0.002001 (s)
```

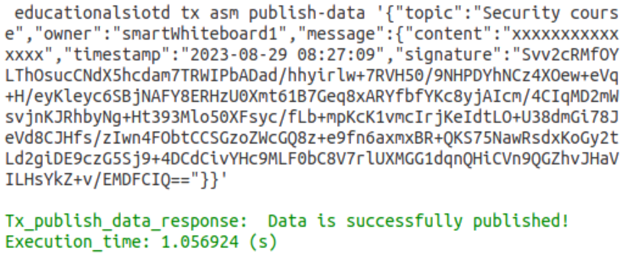
FIGURE 15. Query to retrieve the latest published message on the "Security Course" topic.



```
educationalsiotd tx acm delegate '{"delegator":"teacher-tablet","delega
tee":"student-tablet","action":"grant","permissionLabel":"teacher-table
t-publish-smartWhiteboard1"}'

Tx_delegate_response:  Permit
Execution_time: 1.035928 (s)
```

FIGURE 16. Transaction to delegate "publish" permission to the student tablet.

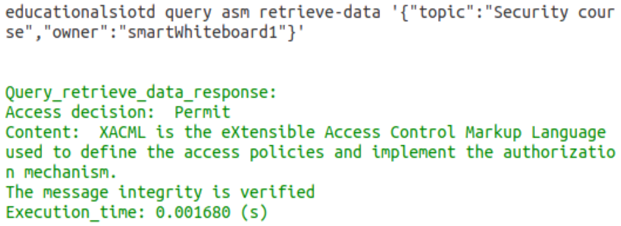


```
 educationalsiotd tx asm publish-data '{"topic":"Security cours
e","owner":"smartWhiteboard1","message":{"content":"xxxxxxxxxxx
xxxx","timestamp":"2023-08-29 08:27:09","signature":"Svv2cRMfOY
LThOsucCNdX5hcdam7TRWIPbADad/hhyirlw+7RVH50/9NHPDYhNCz4XOew+eVq
+H/eyKleyc6SBjNAFY8ERHzU0Xmt61B7Geq8xARYfbfYKc8yjAIcm/4CIqMD2mW
svjnKJRhbyNg+Ht393Mlo50XFsyc/fLb+mpKcK1vmcIrjKeIdtLO+U38dmGi78J
eVd8CJHfs/zIwn4FObtCCSGzoZWcGQ8z+e9fn6axmxBR+QKS75NawRsdxKoGy2t
Ld2giDE9czG5Sj9+4DCdCivYHc9MLF0bC8V7rlUXMGG1dqnQHiCVn9QGZhvJHaV
ILHsYkZ+v/EMDFCIQ=="}}'

Tx_publish_data_response:  Data is successfully published!
Execution_time: 1.056924 (s)
```

FIGURE 17. Transaction to publish the student answer with delegated permission.

6) The whiteboard1 executes a Tx_retrieve transaction to get the latest published message on the "Security Course" topic from the EducationalSIoT platform. The message signature is checked, and the message content is decrypted and is displayed as shown in Fig. 15.
7) To allow the student to write his answer, the teacher delegates his "publish" permission on "smartwhiteboard1" by sending a Tx_delegate transaction to the ACM module as shown in Fig. 16.
8) Once the student introduces his answer, his tablet encrypts the answer using the secret key shared by the teacher and signs it using its private key. The Tx_publish transaction is sent to the ASM module of the EducationalSIoT platform. The ASM module inquires the ACM for the authorization decision. If the authorization decision is "Permit", the message is stored in the "Security Course" topic of "smartwhiteboard1" as illustrated in Fig. 17.
9) "Smartwhiteboard1" retrieves the latest published message and checks its signature using the public key of the publisher device. If the message integrity is verified, the whiteboard decrypts the student answer by using the shared secret key and displays it as shown in Fig. 18.



```
educationalsiotd query asm retrieve-data '{"topic":"Security cour
se","owner":"smartWhiteboard1"}'


Query_retrieve_data_response:
Access decision:  Permit
Content:  XACML is the eXtensible Access Control Markup Language
used to define the access policies and implement the authorizatio
n mechanism.
The message integrity is verified
Execution_time: 0.001680 (s)
```

FIGURE 18. Query to retrieve the student answer from the "Security Course" topic.

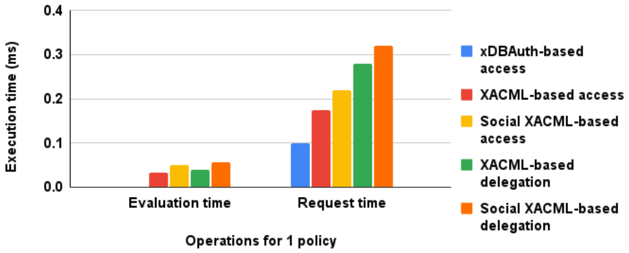


FIGURE 19. Comparison of execution times for 1 policy.

B. PERFORMANCE EVALUATION

We leverage the dataset proposed for SIoT [58] in order to perform a simulation evaluation of our solution based on the execution time. Additionally, we implemented the XACML standard in order to specify the access and delegation policies without involving the social features. For each test, we perform 1000 requests and measure the average time to evaluate a policy set, the average time to process the request and the average time to process the transaction for both the authorization and the delegation.

1) COMPARISONS WITH EXISTING SOLUTIONS

We conduct a comparative analysis of our solution against other existing solutions: XACML standard, xDBAuth framework [26], and the blockchain-based access control [25].

Fig. 19 illustrates the execution times for Social XACML, XACML and xDBAuth. We measure the evaluation time for XACML policies and Social XACML policies. The XACML-based access policy is evaluated in 0.033 ms, while the Social XACML-based access policy evaluation is performed with an average processing time of 0.050 ms. Thus, Social XACML requires more time to evaluate the device social attributes and the social conditions specified for the social relationship established between the subject device and the object device. Additionally, a Social XACML-based delegation policy is evaluated in 0.056 ms. This slight increase in processing the delegation policy is explained by the time required to evaluate the delegation conditions.

To process an access request, xDBAuth [26] requires 0.1 ms to evaluate the Access Control List (ACL), XACML requires 0.175 ms and Social XACML requires 0.22 ms.

TABLE 7. Transaction maximum time (ms).

Transaction	Application-specific blockchain	FISCO BCOS chain
Query (read)	1.28	1000
Message (write)	2031	4600

Obviously, ACL requires less execution time than XACML and social XACML. A request involves several operations performed in either the authorization process or the delegation process. The access request involves the access policy set extraction, the extraction of the subject and object profiles, the extraction of the social relationship data as well as the policy evaluation time. For delegation, the request involves the delegation policy set extraction, the extraction of the subject and object profiles, the extraction of the social relationship data, the extraction of the permission to delegate, the policy evaluation time, the generation of a new access policy for the delegated permission and the update of the extracted delegation policy set. For the delegation request, Social XACML-based delegation requires 0.32 ms to process the delegation request. The delegation request requires more processing time than the access request since it integrates more operations to perform. Additionally, it is based on message transaction which modifies the blockchain ledger when the new access policy generated for the delegated permission is stored in the Policy Store, while the access request is based on a query transaction which requires only to read data from different stores.

According to table 7, the most time-consuming process for reading and writing have a runtime of 1000 ms and 4600 ms, respectively, for FISCO BCOS chain [25] while the maximum transaction processing time for our application-specific blockchain-based EducationalSIoT platform provides requires 1.28 ms and 2031 ms to process the access (i.e. query) and delegation (i.e. message) transactions respectively.

2) ALGORITHM-BASED POLICY EVALUATION TIMES

We measure and compare the execution times of policy evaluation by leveraging two main policy-combining algorithms permit-overrides and highest-priority for access policies and delegation policies. This comparison allows us to assess the scalability and performance of each policy-combining algorithm while varying the number of policies from 10 to 25, 50, 75, up to 100.

Fig. 20 and Fig. 21 demonstrates that algorithms for combining Social XACML-based policies require more evaluation times than algorithms for combining XACML-based policies. According to Fig. 20, the permit-overrides algorithm processes 10 Social XACML policies in 0.050 ms and 10 XACML policies in 0.033 ms. For the highest-priority policy-combining algorithm, the evaluation time for 10 Social XACML policies is equal to 0.054 ms and 0.035 ms for 10 XACML policies. According to Fig. 21, the evaluation time of the highest-priority delegation policy-combining algorithm for 10 Social XACML policies is equal to 0.059 ms and 0.041 ms for 10 XACML policies. Thus, the permit-overrides access policy-combining algorithm takes a rise of approximately 0.0175 ms, the highest-priority access policy-combining algorithm shows an increase near 0.0182 ms while the highest-priority delegation policy-combining algorithm demonstrates an increase of around 0.0175 ms. The increase in the evaluation time is justified by the time required to evaluate the social features to make access and delegation decisions. Therefore, the positive impact of integrating social features on making a reliable decision comes with an average increase of approximately 0.018 ms in the policy evaluation time.

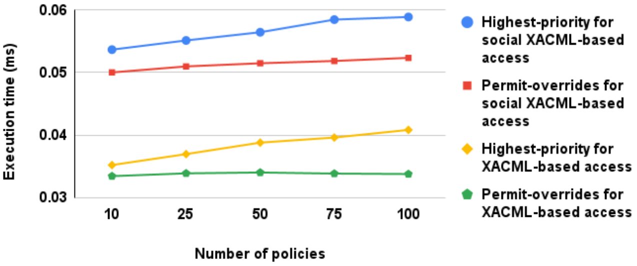


FIGURE 20. Algorithm-based access policy evaluation time.

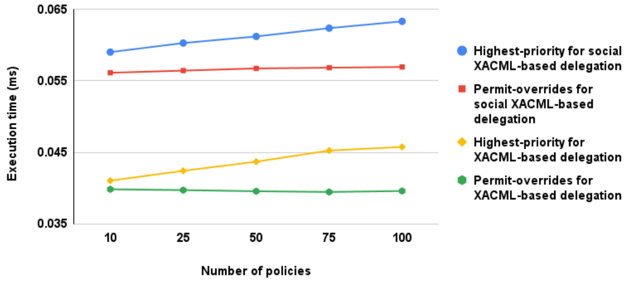


FIGURE 21. Algorithm-based delegation policy evaluation time.

Additionally, we vary the number of policies from 10 to 100 in order to evaluate the impact of increasing the number of policies on the evaluation time. For instance, the evaluation time for the permit-overrides algorithm raises from 0.050 ms for 10 Social XACML policies to 0.052 ms for 100 Social XACML policies as shown in Fig. 20. Thus, the permit-overrides algorithm takes a rise of approximately 0.0023 ms. Therefore, the modest increase in the policy evaluation time ensures the scalability of the policy-combining algorithms.

Moreover, for the highest-priority access policy-combining algorithms, we ought to sort policies in order to ensure that an access or a delegation operation can be guaranteed in emergency situations based on the policy having the highest priority and all conditions are satisfied. Thus, the highest-priority access policy-combining requires more execution time than the permit-overrides policy-combining algorithms.

3) ALGORITHM-BASED REQUEST EXECUTION TIMES

Fig. 22 represents the request time for both access and delegation requests while leveraging the permit-overrides and highest-priority policy-combining algorithms. For each request, the executing time based on permit-overrides is

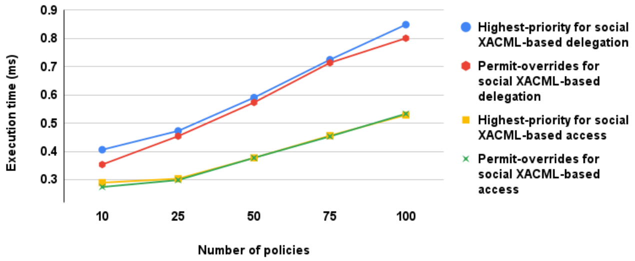


FIGURE 22. Request time.

close to the execution time based on the highest-priority. Additionally, in an emergency situation, a delegation request is performed in 0.405 ms for 10 policies and in 0.850 ms for 100 policies, while an access request is processed in 0.29 ms for 10 policies and in 0.53 ms for 100 policies. We conclude that an access can be guaranteed by delegation in 0.7 ms for 10 policies and in 1.4 ms for 100 policies, while in 0.63 ms for 10 policies and in 1.33 ms for 100 policies in normal situations.

VI. SECURITY CONSIDERATIONS

We ensure the robustness of our EducationalSIoT platform against the security attacks as follows. All transactions provided by the EducationalSIoT platform must be available only for the academic members such as teachers, academic staff members and subscribed students. Thus, the EducationalSIoT platform administrator defines the device management rules, the socialization rule management rules, and the access policy management rules. The device management rules ensure that the device management transactions (i.e. Tx_add_device transaction, Tx_update_device transaction, or Tx_delete_device transaction) are only available for the academic members. The socialization rule management rules guarantee that only the device owner is authorized to specify the device socialization rules associated with his own devices. Therefore, the Tx_add_social_rule transaction, the Tx_update_social_rule transaction, and the Tx_delete_social_rule transaction must be executed only by the academic members who already have added their devices to the EducationalSIoT platform. The policy management rules are leveraged to check whether the creator of the Tx_add_access_policy_set, Tx_update_access_policy_set, Tx_delete_access_policy_set or Tx_add_delegation _policy_set, Tx_update_delegation_policy_set, or Tx_delete _delegation_policy_set transactions is the device owner and is allowed to interact with the PAP to manage his predefined access or delegation policy sets. Therefore, our platform ensures the access control of the device, the socialization rule as well as the access and delegation policy administration.

The messages exchanged between different actors are encrypted and digitally signed to protect the message against unauthorized disclosure and modification. The message encryption and signature ensure the confidentiality, the integrity and the non-repudiation of the sender.

To protect our platform against the man-in-the-middle, digital certificates are leveraged. All transactions are signed by the transaction creator's private keys. These countermeasures prevent any intruder from intercepting the transaction and changing the data to send. In addition, they ensure the integrity of the exchanged data. Therefore, they guarantee that the stored messages are not altered.

To protect our platform against replay attacks, available transactions are timestamped. The transaction timestamp is used to check the freshness of the transaction.

VII. CONCLUSION

In this paper, we propose an Educational Social Internet of Things (EducationalSIoT) platform to provide academic services based on the social network of IoET devices. Our EducationalSIoT platform leverages the class and the institution social relationships to efficiently provide academic services for different stakeholders such as teachers, administration staff and students, in particular students with disabilities. To secure the exchanged data and information, we incorporate the social conditions in the XACML policy model. We extend the XACML authorization mechanism by adjusting the policy evaluation process and proposing new rule-based and policy-based combining algorithms. Furthermore, the access permissions can be guaranteed by delegation operations. Thus, the social constraints are integrated in the access permission delegation process in order to control the delegation operation. The simulation results show that the processing times for policy evaluation and request evaluation ensures the scalability and performance of our access control mechanism. Additionally, we ensure the confidentiality and integrity of data provided by the academic services and the security of our EducationalSIoT platform against the man-in-the-middle and replay attacks. As a future work, we suggest extending our EducationalSIoT platform by adding more services such as the smart disability assistance services in order to incorporate students with disabilities into the learning process. Moreover, we plan to integrate the social features to perform indirect delegation operations based on the Friend of A Friend (FoAF) social relationships.

REFERENCES

[1] K. Polin, T. Yigitcanlar, M. Limb, and T. Washington, "The making of smart campus: A review and conceptual framework," *Buildings*, vol. 13, no. 4, p. 891, Mar. 2023, doi: 10.3390/buildings13040891.

[2] O. Diaz-Parra, A. Fuentes-Penna, R. A. Barrera-Camara, F. R. Trejo-Macotela, J. C. R. Fernandez, J. A. Ruiz-Vanoye, A. Ochoa-Zezzatti, and J. Rodriguez-Flores, "Smart education and future trends," *Int. J. Comb. Optim. Probl. Inform.*, vol. 13, no. 1, pp. 65–74, Jan. 2022.

[3] A. A. Mawgoud, M. H. N. Taha, and N. E. M. Khalifa, "Security threats of social Internet of Things in the higher education environment," in *Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications* (Studies in Computational Intelligence). Berlin, Germany: Springer, 2019, pp. 151–171.

[4] M. Al-Emran, S. I. Malik, and M. N. Al-Kabi, "A survey of Internet of Things (IoT) in education: Opportunities and challenges," in *Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications* (Studies in Computational Intelligence). Berlin, Germany: Springer, 2020, pp. 197–209.

[5] L. E. Holmquist, F. Mattern, B. Schiele, P. Alahuhta, M. Beigl, and H. W. Gellersen, ''Smart-its friends: A technique for users to easily establish connections between smart artefacts,'' in *Ubicomp 2001: Ubiquitous Computing*. Berlin, Germany: Springer, 2001, pp. 116–122.

[6] L. Atzori, A. Iera, and G. Morabito, ''SIoT: Giving a social structure to the Internet of Things,'' *IEEE Commun. Lett.*, vol. 15, no. 11, pp. 1193–1195, Nov. 2011, doi: 10.1109/LCOMM.2011.090911.111340.

[7] A. Zamanifar, ''Social IoT healthcare,'' in *Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications* (Studies in Computational Intelligence), Berlin, Germany: Springer, 2020, pp. 1–11.

[8] J. C. Priya, R. N. Karthika, K. S. Kumar, and P. Valarmathie, ''BlockSIoT: A blockchain-based secure data sharing in SIoT,'' in *Proc. Data Anal. Manag. (ICDAM)*. Singapore: Springer, 2022, pp. 687–700.

[9] S. Kumar and A. Vidhate, ''Issues and future trends in IoT security using blockchain: A review,'' in *Proc. Int. Conf. Intell. Data Commun. Technol. Internet Things (IDCIoT)*, Bengaluru, India, Jan. 2023, pp. 976–984.

[10] M. Khan and A. Malviya, ''Big data approach for sentiment analysis of Twitter data using Hadoop framework and deep learning,'' in *Proc. Int. Conf. Emerg. Trends Inf. Technol. Eng. (IC-ETITE)*, Vellore, India, Feb. 2020, pp. 1–5.

[11] M. Khan, S. Hariharasitaraman, S. Joshi, V. Jain, M. Ramanan, A. SampathKumar, and A. A. Elngar, ''A deep learning approach for facial emotions recognition using principal component analysis and neural network techniques,'' *Photogrammetric Rec.*, vol. 37, no. 180, pp. 435–452, Dec. 2022.

[12] O. Dallel, S. B. Ayed, and J. B. H. Tahar, ''Smart blockchain-based authorization for social Internet of Things,'' in *Proc. Int. Conf. Cyberworlds (CW)*, Sousse, Tunisia, Oct. 2023, pp. 440–447.

[13] A. Badshah, A. Ghani, A. Daud, A. Jalal, M. Bilal, and J. Crowcroft, ''Towards smart education through Internet of Things: A survey,'' *ACM Comput. Surv.*, vol. 56, no. 2, pp. 1–33, Sep. 2023, doi: 10.1145/3610401.

[14] H. M. Knight, P. R. Gajendragadkar, and A. Bokhari, ''Wearable technology: Using Google glass as a teaching tool,'' BMJ Case Rep., U.K., Tech. Rep. 2014-208768, May 2015, doi: 10.1136/bcr-2014-208768.

[15] L. Ting, M. Khan, A. Sharma, and M. D. Ansari, ''A secure framework for IoT-based smart climate agriculture system: Toward blockchain and edge computing,'' *J. Intell. Syst.*, vol. 31, no. 1, pp. 221–236, Feb. 2022.

[16] E. Rissanen. (2013). *Extensible Access Control Markup Language (XACML) Version 3.0*. OASIS Open. [Online]. Available: http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html

[17] J. B. Bernabe, I. Elicegui, E. Gandrille, N. Gligoric, A. Gluhak, C. Hennebert, J. L. Hernandez-Ramos, C. Lopez, A. Manchinu, K. Moessner, and M. Nati, ''SocIoTal—The development and architecture of a social IoT framework,'' in *Proc. Global Internet Things Summit (GIoTS)*, Geneva, Switzerland, 2017, pp. 1–6.

[18] A. Mohamed, D. Auer, D. Hofer, and J. Kung, ''Extended authorization policy for graph-structured data,'' *Social Netw. Comput. Sci.*, vol. 2, no. 5, p. 351, Sep. 2021, doi: 10.1007/s42979-021-00684-8.

[19] R. Abassi and S. G. El Fatmi, ''Delegation management modeling in a security policy based environment,'' in *Proc. Int. Symp. Symbolic Comput. Softw. Sci.*, 2013, pp. 1–11.

[20] J. Kwon and E. Buchman. *Cosmos Whitepaper: A Network of Distributed Ledgers*. Cosmos Network. Accessed: Sep. 19, 2023. [Online]. Available: https://cosmos.network/resources/whitepaper

[21] H. Zhang, P. Ma, and B. Liu, ''Adaptive fine-grained access control method in social Internet of Things,'' *Int. J. Netw. Secur.*, vol. 23, no. 1, pp. 42–48, Jan. 2021, doi: 10.6633/IJNS.202101_23(1).06.

[22] J. Wu, M. Dong, K. Ota, J. Li, and B. Pei, ''A fine-grained cross-domain access control mechanism for social Internet of Things,'' in *Proc. IEEE 11th Int. Conf Ubiquitous Intell. Comput. IEEE 11th Int. Conf Autonomic Trusted Comput. IEEE 14th Int. Conf Scalable Comput. Commun. Associated Workshops*, Bali, Indonesia, Dec. 2014, pp. 666–671.

[23] P. Chinnasamy, A. Albakri, M. Khan, A. A. Raja, A. Kiran, and J. C. Babu, ''Smart contract-enabled secure sharing of health data for a mobile cloud-based E-Health system,'' *Appl. Sci.*, vol. 13, no. 6, p. 3970, Mar. 2023.

[24] H. Saidi, N. Labraoui, A. A. A. Ari, L. A. Maglaras, and J. H. M. Emati, ''DSMAC: Privacy-aware decentralized self-management of data access control based on blockchain for health data,'' *IEEE Access*, vol. 10, pp. 101011–101028, 2022.

[25] Z. Du, Y. Li, Y. Fu, and X. Zheng, ''Blockchain-based access control architecture for multi-domain environments,'' *Pervas. Mobile Comput.*, vol. 98, Feb. 2024, Art. no. 101878, doi: 10.1016/j.pmcj.2024.101878.

[26] G. Ali, N. Ahmad, Y. Cao, S. Khan, H. Cruickshank, E. A. Qazi, and A. Ali, ''XDBAuth: Blockchain based cross domain authentication and authorization framework for Internet of Things,'' *IEEE Access*, vol. 8, pp. 58800–58816, 2020.

[27] (2007). *Geospatial EXtensible Access Control Markup Language (GeoXACML)*. Accessed: Jun. 20, 2023. [Online]. Available: https://www.ogc.org/standard/geoxacml/

[28] A. Ashutosh, A. Gerl, S. Wagner, L. Brunie, and H. Kosch, ''XACML for mobility (XACML4M)—An access control framework for connected vehicles,'' *Sensors*, vol. 23, no. 4, p. 1763, Feb. 2023, doi: 10.3390/s23041763.

[29] J. Lin, H. Tao, and G. Zhu, ''An access control mechanism for geospatial information services,'' in *Proc. 1st Int. Conf. Inf. Sci. Eng.*, Nanjing, China, Dec. 2009, pp. 1971–1974.

[30] P. Xie, H. J. Fan, T. Feng, Y. Yan, G. Ma, and X. M. Han, ''Adaptive access control model of vehicular network big data based on XACML and security risk,'' *Int. J. Netw. Secur.*, vol. 22, no. 2, pp. 347–357, Mar. 2020, doi: 10.6633/IJNS.202003.

[31] Y. Cai, H. Zhang, Y. Fan, and H. Xia, ''A survey on routing algorithms for opportunistic mobile social networks,'' *China Commun.*, vol. 18, no. 2, pp. 86–109, Feb. 2021, doi: 10.23919/JCC.2021.02.007.

[32] D. Wei, H. Ning, Y. Qian, and T. Zhu, ''Social relationship for physical objects,'' *Int. J. Distrib. Sensor Netw.*, vol. 14, no. 1, 2018, Art. no. 1550147718754968, doi: 10.1177/1550147718754968.

[33] A. Arjunasamy and S. Rathi, ''Relationship based heuristic for selecting friends in social Internet of Things,'' *Wireless Pers. Commun.*, vol. 107, no. 4, pp. 1537–1547, Aug. 2019, doi: 10.1007/s11277-019-06344-8.

[34] M. S. Roopa, S. Pattar, R. Buyya, K. R. Venugopal, S. S. Iyengar, and L. M. Patnaik, ''Social Internet of Things (SIoT): Foundations, thrust areas, systematic review and future directions,'' *Comput. Commun.*, vol. 139, pp. 32–57, May 2019, doi: 10.1016/j.comcom.2019.03.009.

[35] B. Li, Y. Lin, and I. A. Khan, ''Self-supervised learning IoT device features with graph contrastive neural network for device classification in social Internet of Things,'' *IEEE Trans. Netw. Service Manag.*, vol. 20, no. 4, pp. 4255–4267, Dec. 2023.

[36] K. M. Alam, M. Saini, and A. E. Saddik, ''Toward social Internet of Vehicles: Concept, architecture, and applications,'' *IEEE Access*, vol. 3, pp. 343–357, 2015, doi: 10.1109/ACCESS.2015.2416657.

[37] V. Loscri, P. Manzoni, M. Nitti, G. Ruggeri, and A. M. Vegni, ''A social Internet of Vehicles sharing SIoT relationships,'' in *Proc. ACM MobiHoc Workshop Pervasive Syst. IoT Era*, Catania, Italy, Jul. 2019, pp. 1–6.

[38] A. M. Esfahani, A. M. Rahmani, and A. Khademzadeh, ''MSIoT: Mobile social Internet of Things, a new paradigm,'' in *Proc. 10th Int. Symp. onTelecommunications (IST)*, Tehran, Iran, Dec. 2020, pp. 187–193.

[39] M. S. Roopa et al., ''Social interaction-enabled industrial Internet of Things for predictive maintenance,'' in *ICT Systems and Sustainability*. Singapore: Springer, 2021, pp. 661–673.

[40] N. Malik, S. K. Awasthi, and N. Sood, ''Centrality as a friendship selection heuristic in social Internet of Things,'' in *Proc. 11th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Kharagpur, India, Jul. 2020, pp. 1–6.

[41] Q. Du, H. Song, and X. Zhu, ''Social-feature enabled communications among devices toward the smart IoT community,'' *IEEE Commun. Mag.*, vol. 57, no. 1, pp. 130–137, Jan. 2019, doi: 10.1109/MCOM.2018.1700563.

[42] B. Zhang, Y. Li, D. Jin, P. Hui, and Z. Han, ''Social-aware peer discovery for D2D communications underlaying cellular networks,'' *IEEE Trans. Wireless Commun.*, vol. 14, no. 5, pp. 2426–2439, May 2015, doi: 10.1109/TWC.2014.2386865.

[43] K. Das, S. Samanta, and M. Pal, ''Study on centrality measures in social networks: A survey,'' *Social Netw. Anal. Mining*, vol. 8, no. 1, pp. 1–11, Dec. 2018, doi: 10.1007/s13278-018-0493-2.

[44] B. Yin, Y. Yang, and W. Liu, ''Exploring social activeness and dynamic interest in community-based recommender system,'' in *Proc. 23rd Int. Conf. World Wide Web*, Apr. 2014, pp. 771–776.

[45] A. Rahim, T. Qiu, Z. Ning, J. Wang, N. Ullah, A. Tolba, and F. Xia, ''Social acquaintance based routing in vehicular social networks,'' *Future Gener. Comput. Syst.*, vol. 93, pp. 751–760, Apr. 2019, doi: 10.1016/j.future.2017.07.059.

[46] S. Ullah, G. Abbas, M. Waqas, Z. H. Abbas, and Z. Halim, ''Multi-hop emergency message dissemination through optimal cooperative forwarder in grid-based 5G-VANETs,'' *J. Ambient Intell. Humanized Comput.*, vol. 14, no. 4, pp. 4461–4476, Apr. 2023, doi: 10.1007/s12652-023-04563-3.

[47] L. Wan, X. Li, J. Xu, L. Sun, X. Wang, and K. Liu, "Application of graph learning with multivariate relational representation matrix in vehicular social networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 3, pp. 2789–2799, Mar. 2023, doi: 10.1109/TITS.2022.3224326.

[48] S. Sagar, A. Mahmood, J. Kumar, and Q. Z. Sheng, "A time-aware similarity-based trust computational model for social Internet of Things," in *Proc. IEEE Global Commun. Conf.*, Taipei, Taiwan, Dec. 2020, pp. 1–6.

[49] A. Khanfor, H. Ghazzai, Y. Yang, and Y. Massoud, "Application of community detection algorithms on social Internet-of-Things networks," in *Proc. 31st Int. Conf. Microelectron. (ICM)*, Cairo, Egypt, Dec. 2019, pp. 94–97.

[50] W. Yang, Y. Qin, and R. Li, "A network-embedding-based approach for scalable network navigability in content-centric social IoT," *IEEE Internet Things J.*, vol. 9, no. 17, pp. 16418–16428, Sep. 2022, doi: 10.1109/JIOT.2022.3151488.

[51] H. Zhang, F. Fan, D. Zhao, B. Liu, Y. Wang, and J. Liu, "Social Internet of Tings trust management based on implicit social relationship," in *Security and Privacy in New Computing Environments*. Cham, Switzerland: Springer, 2022, pp. 129–139.

[52] U. Jayasinghe, G. M. Lee, T.-W. Um, and Q. Shi, "Machine learning based trust computational model for IoT services," *IEEE Trans. Sustain. Comput.*, vol. 4, no. 1, pp. 39–52, Jan. 2019, doi: 10.1109/TSUSC.2018.2839623.

[53] I.-R. Chen, J. Guo, and F. Bao, "Trust management for SOA-based IoT and its application to service composition," *IEEE Trans. Services Comput.*, vol. 9, no. 3, pp. 482–495, May 2016, doi: 10.1109/TSC.2014.2365797.

[54] H. Zhou, V. C. M. Leung, C. Zhu, S. Xu, and J. Fan, "Predicting temporal social contact patterns for data forwarding in opportunistic mobile networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 11, pp. 10372–10383, Nov. 2017, doi: 10.1109/TVT.2017.2740218.

[55] T. V. Le, "A secure socially-aware content retrieval framework for delay tolerant networks," Ph.D. dissertation, Dept. Comput. Sci., Univ. California, Los Angeles, CA, USA, 2016.

[56] R. U. Mustafa, A. McGibney, and S. Rea, "Establishing trustworthy rational friendships in social Internet of Things," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, Bangkok, Thailand, Jan. 2023, pp. 318–327.

[57] O. Dallel, S. B. Ayed, and J. B. H. Taher, "Secure IoT-based emergency management system for smart buildings," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Nanjing, China, Mar. 2021, pp. 1–7.

[58] C. Marche, L. Atzori, and M. Nitti, "A dataset for performance analysis of the social Internet of Things," in *Proc. IEEE 29th Annu. Int. Symp. Pers., Indoor Mobile Radio Commun. (PIMRC)*, Bologna, Italy, Sep. 2018, pp. 1–5.

OLFA DALLEL (Member, IEEE) received the Engineering and master's degrees in computer science from the National School of Computer Sciences (ENSI), University of La Manouba, Tunisia, in 2012 and 2013, respectively. She is currently pursuing the Ph.D. degree with the National Engineering School of Tunis (ENIT), University of Tunis El Manar, Tunisia.

She is also a Visiting Lecturer with the National Engineering School of Sousse (ENISo), University of Sousse, Tunisia. Her current research interests include security, machine learning, and distributed systems.

SOUHEIL BEN AYED received the Engineering and master's degrees in telecommunication from Carthage University, Tunisia, in 2005 and 2008, respectively, and the Ph.D. degree in computer science from Keio University, Japan, in 2012.

From 2005 to 2009, he had the opportunity to work as an Engineer in multinational companies in Tunisia. Currently, he is affiliated with the Networked Objects, Control, and Communication Systems (NOCCS) Laboratory, National Engineering School of Sousse (ENISo), University of Sousse. He is conducting his research activities in the area of computer networks, network security, the Internet of Things, and distributed systems.

JAMEL BEL HADJ TAHAR received the Ph.D. degree from the Polytechnic Institute of Grenoble, INPG, France, in 1993.

In 2011, he became master conference with the Higher School of Communications of Tunis, Information and Communication Technologies. Currently, he is a Professor with the National Engineering School of Sousse, responsible for the training of masters research in telecommunications engineering and the Director of the Networked Objects, Control, and Communication Systems (NOCCS) Laboratory. His research interests include wireless communication techniques and optical systems whereas the other is information treatments and exploitations.