IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received May 27, 2021, accepted June 11, 2021, date of publication June 29, 2021, date of current version July 16, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3093327

Survey on Delegated and Self-Contained Authorization Techniques in CPS and IoT

SREELAKSHMI VATTAPARAMBIL SUDARSAN, OLOV SCHELÉN, (Member, IEEE), AND ULF BODIN
EISLAB, Luleå University of Technology, 97187 Luleå, Sweden

Corresponding author: Sreelakshmi Vattaparambil Sudarsan (sreelakshmi.vattaparambil.sudarsan@ltu.se)

This work was supported by the Electronic Components and Systems for European Leadership (ECSEL) Joint Undertaking (JU) through the Arrowhead Tools Project under Grant 826452.

ABSTRACT Authentication, authorization, and digital identity management are core features required by secure digital systems. In this, authorization is a key component for regulating the detailed access credentials with respect to required service resources. Authorization, therefore, plays a significant role in the trust management of autonomous devices and services. Due to the heterogeneous nature of cyber-physical systems and the Internet of Things, several authorization techniques using different access control models, accounts, groups, tokens, and delegations have both strengths and weaknesses. Many studies exist in the literature that focus on other main security requirements, such as authentication, identity management, and confidentiality. However, there is a need for a comprehensive review of different authorization techniques in cyber-physical systems and the Internet of Things. A specific target of this paper is authorization in the cyber-physical system and Internet of Things networks with *non*-constrained devices in an industrial context with mobility, subcontractors, and autonomous machines that are able to carry out advanced tasks on behalf of others. We study the different authorization techniques using our three-dimensional classification, including access control models, subgranting models, and authorization governance. We focus on the state of the art of authorization subgranting, including delegation techniques by access control/authorization server and self-contained authorization using a new concept of power of attorney. Comparisons are performed with respect to several parameters, such as type of communication, method of authorization, control of expiration, and use of techniques such as public key certificate, encryption techniques, and tokens. The results show the differences and similarities of server-based and power of attorney-based authorization subgranting. The most common standards are also analyzed in light of those classifications.

INDEX TERMS Authorization, access control models, cyber-physical systems (CPS), Internet of Things (IoT), subgranting, delegation, power of attorney (PoA), OAuth.

I. INTRODUCTION

The wider implementation of connected devices yields a significant increase in business revenue. Currently, enterprises invest in machine-to-machine (M2M) communication, the Internet of Things (IoT) and cyber physical systems (CPSs) to increase competitiveness in different domain areas, such as vehicular communication [1], [2], healthcare [3], smart homes [4], [5] and smart grids [6].

IoT technology connects things and smart objects that can sense and monitor the surrounding environments and process and transmit the collected sensor data. Currently, the number of connected things in the world has reached billions or trillions. The industrial IoT (IIoT) is a subset of the IoT that is used in automated M2M and industrial communications to connect all industrial assets. A CPS system integrates Internet technology and advanced electronic/mechanical devices so that they can communicate with each other through data exchanges. The CPS uses computer-based algorithms for the automated and controlled functioning of hardware and software components in the network. Compared to the IoT, which primarily pertains to the interconnection of things by the Internet and exchanging data between them, a CPS is typically more domain-specific, with the interaction between

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

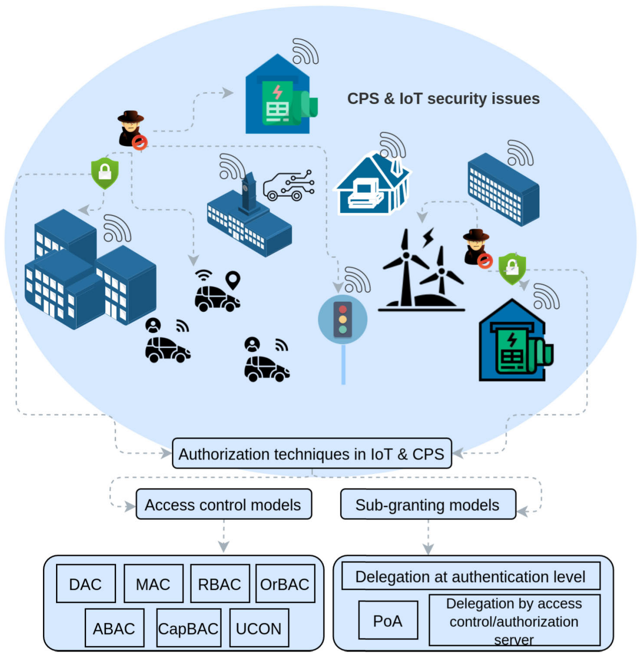

CPS & IoT security issues
Authorization techniques in IoT & CPS
Access control models
Sub-granting models
DAC
MAC
RBAC
OrBAC
ABAC
CapBAC
UCON
Delegation at authentication level
PoA
Delegation by access control/authorization server

FIGURE 1. Authorization techniques in CPS and IoT.

more advanced, often semi-autonomous, physical, and cyber environments achieved by the integration of algorithmic computations. A common aspect is that both the IoT and CPS pose high security and privacy concerns [7] (Fig. 1).

A. SECURITY REQUIREMENTS

The main security requirements [8] are identity management, authentication, authorization, confidentiality, and integrity, which are interconnected to provide different aspects of security. *Identity management* is the process of managing identity information such as user ID, certificates, biometric information, tokens, etc. Identity information is the basis of security mechanisms such as authentication and authorization [9].

Authentication is the process of verifying users in a system to prevent malicious access. Digital signatures and public key certificates are typically used to achieve authentication. Public key certificates are issued by a third-party certificate authority (CA) to certify the public key of the user [8]. Several works have been conducted on authentication schemes for IoT applications, such as smart grids [10] and vehicular networks based on VANETs (vehicular ad hoc networks) with vehicles equipped with an onboard unit (OBU), a trusted authority (TA), and a roadside unit (RSU), along with two modes of communication types: V2V (vehicle-to-vehicle) and V2I (vehicle-to-infrastructure) [2], [11].

Authorization is the process of controlling access to protected resources using different access control models and access privileges. Authorization techniques ensure that only legitimate users access protected resources, thus preventing unauthorized access.

Confidentiality includes techniques such as encryption to protect the privacy of the data transmission. *Integrity* includes security techniques such as hashing to protect the data from unauthorized modifications.

B. CHALLENGES

Traditional challenges in the area of CPS and IoT are meeting different security requirements that prevent attackers from exploiting vulnerabilities.

CPS and IoT devices are heterogeneous and complex in nature and part of critical infrastructure. This demands high-level security in *all* systems and subsystems [12]. Security challenges have emerged, making people more vigilant in CPS and IoT device security because several attacks have caused enormous revenue losses [13]. Many malicious attacks are caused by illegitimate access [14]. An illegitimate user logging in to a device may establish a backdoor that enables the attacker to perform malicious activities throughout the entire network [15]. Several attacks, such as Denial of Service-Mirai and other botnets [16] [17], Sybil attacks [18], routing attacks [19], etc., demand high-level security requirements.

New challenges occur when CPS is used to perform tasks on behalf of owners or managers. In such cases, there is a need to delegate various responsibilities from time to time. For this, there is a strong dependence on authorization techniques. There are different access control models with both strengths and weaknesses employed to achieve authorization in connected devices. However, finding an appropriate authorization model according to the specific application scenario is a challenge. In CPS and IoT applications, there are OAuth-like solutions that enable third-party services to access authorized resources stored in protected locations on behalf of a resource owner. There are different open research questions and challenges, such as cross-site request forgeries, redirect attacks, and state leak attacks with these delegation-based authorization techniques. In industrial CPS and IoT ecosystems, with contractors and device mobility, the devices owned by contractors are used to sign on to the systems of the main industry owner. This introduces the need for subgranting systems that are used to grant the power or privileges from the main industry owner to trusted contractors and further on to their trusted IoT and CPS devices to perform tasks on their behalf. This area of subgranting techniques poses several challenges and open research questions.

C. OTHER SURVEYS

In the area of authorization techniques in CPS and IoT, many interesting works have been done that survey different security mechanisms that outline and analyze similar research findings. Michal Trnka [20] discusses authentication, authorization, and identity management for CPS and IoT applications. The author successfully categorizes different security approaches from multiple perspectives. El-hajj M *et al.* [21] survey different authentication schemes in the IoT. The paper also discusses the challenging integration of different authentication mechanisms in CPS and IoT applications. Bilal *et al.* [22] identify security issues that could cause session hijacking in web applications using OpenID and provide a solution to prohibit such hijacking in single sign-on web scenarios. The survey by A. Ouaddah *et al.* [23] points out the use of eXtensible Access Control Markup Language (XACML) access control policies in the IoT to solve many issues related to interoperability, context awareness, and granularity. Bertin *et al.* [24] survey different access control models and access control architectures and protocols, such as Security Assertion Markup Language (SAML), XACML, and Open Authorization (OAuth). A comprehensive literature review of access control in the IoT is discussed by Sowmya Ravidas *et al.* [25], which is very helpful to categorize CPS and IoT applications based on different access control models, and J. Qiu *et al.* [26] also summarize various access control models based on IoT systems. Saghir M *et al.* [27] address the differences in using traditional and decentralized access control models in the IoT.

D. SCOPE

In contrast to the abovementioned surveys, which mainly address CPS and IoT security based on different authentication techniques and access control models, the scope of this paper is primarily authorization. Taking the new security challenges into consideration, the relevance of authorization techniques is increasing, as they allow devices to access allocated resources that can be managed by access control mechanisms [28]. The authorization mechanisms used in CPS and IoT systems can differ depending on the nature of heterogeneous devices with varying capabilities, memory, and CPU capacities [29].

Many studies in CPS and IoT domain areas pertain to resource-constrained devices such as sensors and actuators. However, many mobile and industrial application scenarios assume semi-autonomous devices with sufficient resources and computing power. For instance, an autonomous car can access protected resources on behalf of the user. In this case, the autonomous car is not a resource-constrained device. The scope of this paper is authorization techniques in CPS and IoT domains with devices that are *not* resource constrained.

In mobile and industrial scenarios, an important authorization concept is subgranting, in which a primary user delegates his/her access privileges to another user (secondary user) whom he/she trusts. The scope of this paper covers general authorization models at a high level and subgranting models more specifically. In this, the OAuth protocol is a well-known example of delegation-based authorization, in which services are given access to protected resources on behalf of authorized users. The PoA-based authorization approach provides authorization for devices to sign on behalf of their owner using PoA, which is a completely generic and self-contained document. PoAs are not generated by any third-party security servers; it is the user who creates and signs the PoA. The user has full control over the PoA generation, and the information contained in the PoA is defined by the principal or the person who generates PoA. This does not require a specific account for the device. This approach uses the owner's account with limited features for a defined time. These newer self-contained techniques have their own set of issues and challenges.

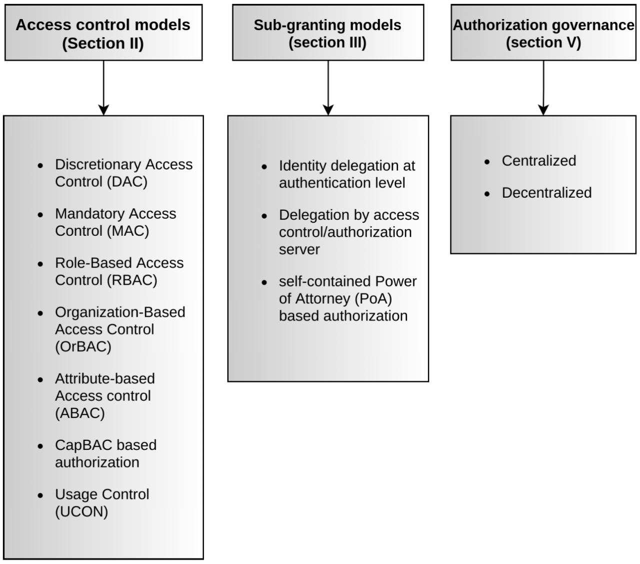

Access control models (Section II)
Discretionary Access Control (DAC)
Mandatory Access Control (MAC)
Role-Based Access Control (RBAC)
Organization-Based Access Control (OrBAC)
Attribute-based Access control (ABAC)
CapBAC based authorization
Usage Control (UCON)
Sub-granting models (section III)
Identity delegation at authentication level
Delegation by access control/authorization server
self-contained Power of Attorney (PoA) based authorization
Authorization governance (section V)
Centralized
Decentralized

FIGURE 2. Our classification in three dimensions performed in the paper.

E. CONTRIBUTIONS

We focus on *authorization* techniques, providing general contributions and special contributions. The *general contributions* of this paper are as follows:

- A high-level overview and evaluation of access control models with respect to authorization, including an analysis of strengths and weaknesses of each approach.
- We cover different access management standards and protocols in light of the above evaluation and to build the foundation for our ensuing special contributions.

We specifically target authorization techniques that are used in the CPS and IoT networks. In particular, industrial and business contexts, which involve mobility, subcontractors, and autonomous machines that are *not* resource-constrained, such as autonomous vehicles [11], are able to carry out advanced tasks on behalf of others. The *special contributions* of this paper are the following:

- A description of the state of the art with respect to subgranting techniques including identity delegation at the authentication level, delegation by access control/authorization server, and a new concept of PoA.
- A brief comparison of benefits and drawbacks of governance strategies based on centralization vs. decentralization. This is presented to place the subgranting models into context.

In our approach, the classification is done in three different dimensions: access control models, subgranting models, and authorization governance [Fig. 2]. The classes of access control models include discretionary access control (DAC), mandatory access control (MAC), role-based access control (RBAC), organization-based access control (OrBAC), attribute-based access control (ABAC), CapBAC-based authorization, and usage control (UCON). The classes of subgranting models include identity delegation at the authentication level, delegation by access control/authorization server, and self-contained PoA-based authorization. The classes of authorization governance include centralized and decentralized authorization.

The access management standards that we discuss in this paper, related to our classification, are OAuth, SAML, XACML, and next-generation access control (NGAC).

F. PAPER STRUCTURE

In this survey, we first discuss and analyze different access control models (section II). After the discussion of traditional authorization techniques using access control models, section III defines and compares different subgranting models: A) identity delegation at the authentication level, B) delegation by access control/authorization server, and C) PoA-based authorization. In section IV, we discuss different access management standards which are related to or fall under either of the two dimensions in our classification: access control models (section II) and subgranting models (section III). In section V, we define different types of authorization governance. In this survey, we also provide our observations, analysis, and describe open research issues (section VI). Section VII concludes the paper.

II. ACCESS CONTROL MODELS

Access control is the first dimension of our classification. It is the mechanism to determine whether a user is granted or denied access to a resource or object based on certain rules (authorization) [28]. Access control policies mainly include two phases: the policy definition phase and the policy enforcement phase. Authorization is the function implemented in the policy definition phase to authorize access.

In the second phase, the policy enforcement phase, the decision is made for the access requests based on the authorizations in the first phase. Traditional access control models such as DAC and MAC to newer and secure access control models are used as part of authorization frameworks in CPS and IoT ecosystems. The subsections below discuss different access control models based on authorization.

A. DISCRETIONARY ACCESS CONTROL

DAC is an identity-based access control model in which the user has complete control over his/her resources (objects). The owner or user determines the set of permissions and access to his/her resources by other users. DAC can be implemented using several approaches, such as access control lists (ACL) [28], access matrix, capability list, and authorization table [25]. The model is called discretionary because the user has all the rights to specify the permissions and controls for his/her objects. This model is commonly used by various operating systems, such as Linux, UNIX, Windows, and many other network operating systems, for file system management [30].

B. MANDATORY ACCESS CONTROL

MAC, unlike DAC, is controlled by a centralized administration or controller. Even though the user owns certain resources, the permissions and access control over these resources are decided by the administrator. Access control is based on a hierarchical model, where users are classified and distinguished based on a certain security level. Users at a higher security level have more access power than others. Because of this centralized control, MAC is said to be a more secure access control model and is used by many governmental organizations. However, it is not practically feasible to use this model in a large network because of its centralized administration nature. This makes it inappropriate for use in Internet-based applications [31].

C. ROLE-BASED ACCESS CONTROL

Role-based authorization is widely used, and various commercial implementations are available. This type of authorization regulates access to a network or system based on the role of the user. The role is defined as a set of actions, permissions, or responsibilities provided to a user in a particular network or organization. The rights assigned for different roles overlap; therefore, role hierarchies are commonly used in role-based authorization [32]. Most of the organizations have role groups such as top secret, secret, confidential, and sensitive. The authorization is based on these role groups or roles. The major components involved in role-based authorization are users, roles, and permissions.

D. ORGANIZATION-BASED ACCESS CONTROL

Authorization-based security policies of organizations are commonly implemented and evaluated using OrBAC. The OrBAC model, which is an extension to RBAC, is a centralized authorization model with two levels of abstraction: the concrete level and the abstract level. The subjects, actions, and objects are included at the concrete level, and the abstract level defines roles, activities, and views [33].

E. ATTRIBUTE-BASED ACCESS CONTROL

In an attribute-based authorization system, users are identified and authorized using the attributes provided by them. The client who requests a service can provide attributes such as X.509 entity certificates, X.509 attribute certificates, SAML attribute assertions, lightweight directory access protocol (LDAP) attributes, and handle system attributes. Sometimes, attributes are sent before digital signing using private keys, while a few others are embedded in encrypted messages and received over protected channels.

The attributes are presented to the authorization server or module to access the requested service. In this type of authorization system, users and authorization systems need not be in the same security domain. Attribute-based authorization along with SAML and XACML is used by several systems, such as organization management, web services [34], and grid computing [35].

Encryption-based access control uses public key cryptography for access control. Access control combines an encryption algorithm with ABAC. Encryption-based access control achieves security requirement confidentiality by protecting the privacy of user data. Using encryption-based access control, the access control policy attributes can be incorporated into the ciphertext, making the access control mobile [36]. Incorporating access policies into the ciphertext allows the policy enforcement point (PEP) to be mobile and even decentralized and distributed, as each data hosting party can serve as a PEP. Encryption-based access control fits naturally into ABAC due to its attribute nature but can also support RBAC in considering attributes to validate its group-based roles.

The different types of encryption-based access control models are role-based encryption (RBE), timed-release encryption (TRE), identity-based encryption (IBE), and attribute-based encryption (ABE) [37]. ABE [38] includes two types: ciphertext policy ABE (CP-ABE) and key policy ABE (KP-ABE). The CP-ABE type integrates the user's key with the attributes and the ciphertext with the access policy. The KP-ABE type integrates the user's key with the access policy and the ciphertext with the attributes [39].

F. CapBAC-BASED AUTHORIZATION

Capability-based access control (CapBAC) is based on token authorization, where the users are granted access based on tokens (such as keys or tickets). Here, the capability points to the authorization token. This token uniquely refers to the resources (object) along with a set of permissions and controls [26], [40].

Unlike DAC, CapBAC does not provide much importance for identity management, which makes it less complicated in dealing with access control in cross-domain contexts. In this system, the user submits his/her capability to the service provider to demonstrate his/her permissions over the object or resource. Hence, the service provider does not have to check whether the user is authorized to access the requested resource [41].

G. USAGE CONTROL

UCON is a newer security model that combines traditional access control, trust management, and digital rights management (DRM) to provide more general-purpose access control, which protects digital resources and controls the usage of sensitive information [42]. In this model, policies are specified in terms of the attributes of the subject and object [25].

H. ANALYSIS OF ACCESS CONTROL MODELS

There have been many works that have focused on CPS and IoT authorization using different access control models. The qualitative analysis of different access control models in CPS and IoT has been done by others using metrics such as scalability, usability, flexibility, interoperability, context awareness, distribution, real-time, heterogeneity, lightweight, user-driven, and granularity [43].

In Table 1, we analyze and classify the strengths and weaknesses of the above-defined access control models [26], [37], which shows the significant differences between these access control models. This may help to determine a suitable access control model according to its strengths and weaknesses.

The appropriate access control model for a specific use-case scenario is selected based on needs, considering the strengths and weaknesses of the access control model. In Table 4, we classify the existing CPS and IoT application frameworks based on different access control models. The classification shows the use of specific access control models according to the use-case scenario along with other metrics such as authorization governance and subgranting models. Table 2 provides the strengths and weaknesses of the existing authorization frameworks in Table 4.

III. SUBGRANTING MODELS

Subgranting models are the second dimension of our classification. In a classical society, people tend to provide access to certain resources (granting) by sharing their credentials, such as passwords or passcodes. This way of granting access often results in unauthorized access or misuse of the credentials provided.

Delegation-based authorization is the process of granting authorization of a user to another user in a more secure way. For example, in an organization, there will be employees at different authority levels. On specific occasions, the employee at a top level can grant his/her credentials to another employee at a lower level so that the low-level employee can access protected resources on behalf of the high-level employee with the user permissions and features of the high-level employee. This is the procedure of user delegation to access protected resources. There are three main types of delegations: A) identity delegation at the authentication level, B) delegation by access control/authorization server, and C) power-of-attorney-based authorization. Subgranting is independent of the first dimension in our classification, i.e., access control models. However, in current proposals, we see that thus far, subgranting is often used with ABAC or RBAC.

A. IDENTITY DELEGATION AT AUTHENTICATION LEVEL

In identity delegation at the authentication level, the effective identity, which is the identity granted to the access control system, is different from the validated identity, which is the identity concluded by the authentication system. Here, the identity of the person who grants authorization (delegator) and the person who receives the authorization (delegate) are considered effective. The sudo and su commands in UNIX are an example of identity delegation in operating systems [77].

Mercredi and Frey [78] propose a user delegation model in which the principal (the user who grants access) allows the other user to sign on his/her behalf.

TABLE 1. Strength and weakness of access control models.

Access Control model	Strength	Weakness
DAC	Flexibility-user can specify the permissions and controls for his/her objects	Not suitable in large-scale networks that require high-level security
MAC	Addresses decentralization of resource management and scalability	Limited user flexibility in large networks
RBAC	Provides user role-based access	Scalability issues with large amounts of resources. Flexibility issues with multiple admins
OrBAC	Introduction of the organization dimension to RBAC	Trust management issues
ABAC	Addresses problems of fine-grained user access control. Large-scale user dynamic expansion	Privacy leakage on attribute submission
CapBAC	Use of authorization tokens	Limited identity management
UCON	Supports access control in heterogeneous and distributed domains	Complex authorization management

Anggorojati *et al.* [81] propose an access delegation method based on the capability-based context-aware access control (CCAAC) model for machine-to-machine communication in the IoT. They also propose models of the delegation of authority to achieve the flexibility of the access control system, which is suitable for pervasive IoT. Here, an entity referred to as the IoT Federation Manager (IoT-FM) authorizes the delegator upon request and grants it to the delegate.

There are two main types of delegation granularity: fine-grained and coarse-grained. Both of these methods have merits and demerits. The fine-grained method is commonly used to achieve the least privilege. However, it is error-prone and presents certain large-scale usability issues. On the other hand, coarse-grained systems violate the principle of least privilege.

B. DELEGATION BY ACCESS CONTROL/AUTHORIZATION SERVER

In this model, the delegation from a resource owner to a client is performed via a server, e.g., an authorization server, that coordinates the delegation. There are several methods for interaction between the resource owner and this server. When a client needs access, it communicates with such a server.

Delegation by access control/authorization servers is most often based on RBAC. This is to authorize users for specific tasks by performing fine-grained access. Here, the identity of the delegate is considered an effective identity. For the end-to-end security of independent IP networks, protocols such as datagram transport layer security (DTLS) have been used in delegation systems. However, they are based on public key cryptography, which makes them less feasible for constrained devices.

Rene Hummen *et al.* [54] have proposed a new approach based on the session resumption mechanism, which is a delegation architecture for secure communication between independent IoT network domains. The system improves the feasibility of DTLS-protected communication. The main component of the delegation architecture is the delegation server (DS). Here, the DS provides a constrained device with the required security to participate in remote communication. Hence, when a new device enters the network, the delegation server imprints a master key into this new device and performs a certificate-based DTLS handshake with the remote endpoint on behalf of the device. Later, DS grants the secure access to the device.

Giada Sciarretta *et al.* [55] present a delegated authorization mechanism using OAuth 2.0 in smart city mobile applications. Here, the data owner delegates access to his/her resources to the client application.

Similarly, Victoria and Antonio [79] discuss IoT delegated access control. IoT devices access the available resources using the tokens in the form of an authorization pass. In that paper, delegated access control over IoT devices relying on CoAP is discussed. The authentication server issues an access token to the client, and the client uses this access token to request resources from the resource server. The resource server who trusts the authentication server trusts the client transitively.

Sanaz Rahimi *et al.* [3] explain the security analysis of delegation-based authorization servers in IoT systems. According to them, the sensitive data in the delegation server can be lost, and the server can be compromised by a DoS attack. They discuss security loopholes such as unauthorized access to master keys, transmission overhead, and communication latency.

C. POWER OF ATTORNEY-BASED AUTHORIZATION

PoA-based authorization is a self-contained authorization technique. Conventional PoAs are official paper documents signed by a person to grant his/her privileges to another person. Currently, PoAs are digital, where electronic signatures are used to sign [82].

Here, the person or device that generates and signs the PoA is called the principal, and the device that receives it is called the agent. The principal authenticates themselves using their public key certificate and signs the PoA using his/her private key, and the agent at the other end uses the PoA after proper validation. This is a novel approach to authorization because, in traditional machine-to-machine communication, the devices use their own account to make use of privileges. A PoA typically expires and becomes invalid after a short time predefined by the principal.

TABLE 2. Strength and weakness of existing authorization frameworks in CPS and IoT (same list as that used in Table 2).

Authorization framework	Strength	Weakness
L. Seitz et al. (2013) [44]	Fine-grained and flexible access control	Additional overload protection mechanisms
S. Cirani et al.(2015) [45]	Performance evaluation using simulations are presented	-
S. Sciancalepore et al. (2017) [46]	Use of gateway for data collection and management of access requests from third-party applications	-
S. Emerson et al. (2015) [47]	Resistance to impersonation and replay attacks	-
S. Chung et al. (2018) [48]	Use of OAuth Authorization Code grant type to authorize CoAP-based devices	Evaluation results are not presented.
P. Solapurkar (2016) [49]	Use JWT in OAuth2.0	JWT usage by gateways or third-party applications
S. Jonnada et al. (2018) [50]	Use of OAuth to authorize remote workers for collaboration	Security analysis is not provided
José L. Hernández-Ramos et al. (2015) [51]	Security and performance results are presented	-
Marlon C. Domenech et al. (2016) [52]	Proof of concept is provided and integrated with a real case study	-
Sergio Gusmeroli et al. (2013) [40]	Capability-based security approach for authorization using capability token	-
Ebinger P. et al. (2012) [53]	Use of XACML improves user privacy	Performance evaluation is not discussed.
R. Hummen et al. (2014) [54]	Improves the feasibility of DTLS-protected communication	-
G. Sciarretta et al. (2016) [55]	Resistance to impersonation and phishing attacks	-
F. Fernández et al. (2017) [56]	as-a-service access control mechanism is presented	Performance evaluation is not presented.
A. Alshehri and R. Sandhu (2017) [57]	Resistance to unauthorized access and privacy related attacks	-
Oscar Garcia-Morchon and Klaus Wehrle (2010) [58]	Pervasive health monitoring using access control	Security evaluation and results are not provided.
Ouaddah A. et al. (2017) [59]	Resistance to attacks on central server of the authorization system	Performance measurement is not provided
Guoping Zhang and Jiazheng Tian (2010) [60]	Capturing of security-relevant contextual information	-
J. Jindou et al. (2012) [61]	Extended RBAC model with user-role and permission-role assignments	-
Barka E. et al. (2015) [62]	Integration of RBAC in Web of Things	Proof of concept is not provided
O. J. A. Pinno et al. (2017) [63]	Address the issue of token revocation	-
R. Neisse et al. (2014) [64]	Use MQTT security for IoT devices	-
D. Hussein et al. (2017) [65]	Access rights for a community of smart objects with the proof of concept	-
S. M. R. Islam et al. (2018) [66]	Introduction of security access token (SAT)	Results and evaluation are not provided
I. Ray et al. (2017) [67]	Use of NGAC with ABAC for access control policy management	Performance evaluation is not discussed.
J. E. Kim et al. (2012) [68]	Evaluation of access control in smart homes	-
Guoping and Wentao (2011) [69]	Services-Oriented Architecture (SOA)-based security	Practical ease and feasibility are not presented
R. Xu et al. (2013) [70]	Use of smart contracts to manage capability tokens	-
A. Lohachab and Karambir (2018) [71]	Integration of UCON in hybrid access control architecture	-
Bruhadeshwar Bezawada et al. (2018) [72]	Securing smart homes based on ABAC	-
Andersen M.P. et al. (2017) [73]	Resistance to DDoS attack. Blockchain not used to store all data	-
Shafagh et al. (2018) [74]	Cryptographically enforced access control service	Usability considerations are open.
A. F. Skarmeta et al. (2014) [75]	Design and evaluation of a lightweight token along with ECDSA	-
N. Tapas et al. (2018) [76]	Primary evaluation and experimental results for average time required are provided	-

The PoA-based authorization model uses public key cryptography, digital signatures, and the CA for the security of the entire signatory system. PoAs have several applications, such as an agent collecting mail from a post office on behalf of the principal, or prescribing medication at the pharmacy. PoAs are mainly implemented to be used by devices with a reasonable amount of memory and computing power.

With PoAs, the devices need not have a special account system; instead, they use the owner's account for a short time. In this type of system, they may use a signatory registry, which is a database to store PoAs and other data. This will make it easier to manage data storage and validation issues.

Compared to delegation by access control/authorization servers, PoAs are completely generic and self-contained documents. Table 3 shows that delegation-based authorization is primarily used for service-to-service communication and that new versions of OAuth-based delegation techniques are also used for micro service-to-micro service communication. On the other hand, PoA-based authorization is mainly used for user-to-device and device-to-device communication. Both

TABLE 3. Comparison of authorization models.

Authorization model	Communication	Authorize on user's behalf	Public key certificate	Encryption	Tokens	Control of expiration	Strength(+) Weakness(-)
Basic Authorization	User and User account	No	No	No	No	No	+Easy to deploy -Vulnerable to most of the attacks
Delegation (OAuth)	Service-to-service or micro service-to micro service	Yes	No	No	Yes	Yes	+Allow third-party services to access resources securely -Vulnerable to certain security breaches
PoA	User-to-device or device-to-device	Yes	Yes	Yes	No	Yes	+Allow device to access resources on behalf of the principal using PoA -Not suitable with resource constrained devices

TABLE 4. Classification of existing CPS and IoT authorization frameworks (to be extended with strengths and weaknesses in Table 3).

Authorization framework	Authorization governance	Access control model	Subgranting model	Domain area
L. Seitz et al. (2013) [44]	Centralized	ABAC	Delegation	-
S. Cirani et al.(2015) [45]	Centralized	-	Delegation	-
S. Sciancalepore et al. (2017) [46]	Centralized	-	Delegation	-
S. Emerson et al. (2015) [47]	Centralized	-	Delegation	-
S. Chung et al. (2018) [48]	Centralized	-	Delegation	IoT cloud
P. Solapurkar (2016) [49]	Centralized	-	Delegation	Healthcare
S. Jonnada et al. (2018) [50]	Centralized	-	Delegation	Remote collaboration system
José L. Hernández-Ramos et al. (2015) [51]	Centralized	ABAC	-	Smart buildings
Marlon C. Domenech et al. (2016) [52]	Centralized	any	-	Web of Things
Sergio Gusmeroli et al. (2013) [40]	Centralized	CAPBAC	-	-
Ebinger P. et al. (2012) [53]	Centralized	ABAC	-	Smart metering
R. Hummen et al. (2014) [54]	Centralized	-	Delegation	IP-based IoT
G. Sciarretta et al. (2016) [55]	Centralized	-	Delegation	Smart city mobile applications
V. Beltran and A. F. Skarmeta (2016) [79]	Centralized	-	Delegation	Constrained environment
F. Fernández et al. (2017) [56]	Centralized	RBAC	Delegation	-
A. Alshehri and R. Sandhu (2017) [57]	Centralized	ACL RBAC ABAC	-	Virtual object communication
Oscar Garcia-Morchon and Klaus Wehrle (2010) [58]	Centralized	RBAC	-	Medical sensor network
Ouaddah A. et al. (2017) [59]	Decentralized	RBAC	-	-
Guoping Zhang and Jiazheng Tian (2010) [60]	Centralized	RBAC	-	-
J. Jindou et al. (2012) [61]	Centralized	RBAC	-	Web of Things
Barka E. et al. (2015) [62]	Centralized	RBAC	-	Web of Things
O. J. A. Pinno et al. (2017) [63]	Decentralized	RBAC, ABAC, CAPBAC, ORBAC, UCON	-	-
R. Neisse et al. (2014) [64]	Centralized	ABAC	-	-
D. Hussein et al. (2017) [65]	Distributed	CAPBAC	-	-
S. M. R. Islam et al. (2018) [66]	Centralized	CAPBAC	-	Healthcare
I. Ray et al. (2017) [67]	Centralized	ABAC	-	Healthcare
J. E. Kim et al. (2012) [68]	Centralized	ABAC	-	Smart home
Guoping and Wentao (2011) [69]	Centralized	UCON	-	-
Bouij-Pasquier I et al. (2015) [80]	Centralized	ORBAC	-	-
R. Xu et al. (2013) [70]	Decentralized	CAPBAC	-	-
A. Lohachab and Karambir (2018) [71]	Centralized	CAPBAC,UCON	-	-
Bruhadeshwar Bezawada et al. (2018) [72]	Centralized	ABAC	-	Smart home
Andersen M.P. et al. (2017) [73]	Decentralized	-	Delegation	-
Shafagh et al. (2018) [74]	Decentralized	-	Delegation	-
A. F. Skarmeta et al. (2014) [75]	Decentralized	CAPBAC	-	-
N. Tapas et al. (2018) [76]	Decentralized	-	Delegation	-

are similar in certain aspects that they can authorize on the user's behalf.

Delegation-based authorization uses secure tokens for authorization. Here, tokens are issued by authorization servers and are granted to appropriate users. On the other hand, in PoA-based authorization, PoAs are used to authorize a user or device. Here, the PoA is generated by the owner/principal itself.

Public key certificates are used in PoA-based authorization, which is not discussed in the basic OAuth-based delegation systems. Both of these techniques involve control of expiration. Delegation-based methods include tokens that

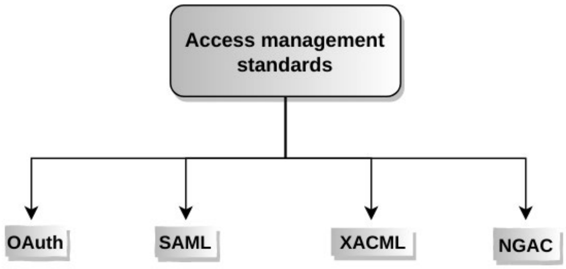


FIGURE 3. List of access management standards in IoT.

expire after a short time. Similarly, PoAs also expire after the user-defined time, so stale PoAs will not remain active.

In PoA-based authorization, no public-private key encryption is carried out on the agent side. All resource-consuming tasks, such as PoA generation, validation, and execution, are performed by the principal. In contrast, in a delegation-based authorization that is apt for resource-constrained devices, public-private key encryption is done on the client device, which is costly and makes it less flexible. However, PoA-based authorization is not used for resource-constrained devices. It is only used with CPS and IoT devices such as autonomous cars with adequate memory and CPU capacity.

PoA-based authorization is by nature decentralized since the PoAs are self-contained. The signatory registry can be either centralized or decentralized depending on the use case. It can use centralized third-party security techniques such as CA [82].

IV. ACCESS MANAGEMENT STANDARDS

One of the main components of identity and access management (IAM) is authorization. With the wide use of digital applications in the cloud, several access management standards have been introduced in recent decades to solve identity and access management challenges. Most of the access management standards are implemented based on certain access control models and delegation models. This section discusses different access management standards, such as A) OAuth authorization, B) SAML and XACML, and C) NGAC [Fig. 3].

A. OAuth AUTHORIZATION

OAuth is a popular authorization standard that falls under the second dimension of our classification: delegation-based authorization of subgranting models (section III). OAuth enables a third-party service to access user resources with limited features on the user's behalf [83], [84] [85]. Here, the *user* is the person who owns the resource or can be referred to as the *resource owner*. The *third party application/service (client)* is the application that requires and requests the resources on behalf of the resource owner or user. Here, we also use the term *consumer* to refer to the person or third party application that consumes the resources on behalf of the resource owner.

OAuth is used for secure authorization between various CPS and IoT applications and services and is based on the representational state transfer (REST) web architecture. OAuth authorizes the identity of both the client (third party) and the actual resource owner before providing access to the server-hosted user resources using OAuth tokens.

The access tokens issued by the authorization server (AS) contain information on the grant's scope, expiration, and other attributes. There are specifications, namely, OAuth 2.0: bearer token usage and OAuth 2.0: message authentication code (MAC) token. The MAC is more secure than the bearer token. However, most clients use bearer tokens due to their simplicity. The access tokens will expire after a short time. To obtain new access tokens, refresh tokens are used, which are stored securely on the client side.

Seung-Hwa Chung [48] describes a pragmatic approach for IoT device authorization in the cloud using the OAuth mechanism. In the OAuth 2.0 framework, there are four different types of authorization grants. First is the authorization code type; here, the access token is generated based on the communication between the client and the authorization server. Second is the implicit type; here, the client can directly access the authorization server for the access token. Third is the resource owner password credential type; here, the client submits the user ID and password as an authorization grant. Last is the client credentials type; here, the authorization server trusts the client and delegates all the authorization control to the client. [48] makes use of the authorization code type to authorize the CoAP-based device.

Simone Cirami *et al.* [45] discuss OAuth using tokens that contain the IDs of both user and consumer; here, the user issues tokens to consumers to access user information on his/her behalf. This is an external authorization mechanism that smart objects invoke to conduct authorization checks to reach sensitive information. The newer version, OAuth 2.0, reduces the client developer complexity as compared with its earlier version, OAuth 1.0.

Feng Yang and Sathyamoorthy [86] discuss various security loopholes in the OAuth 2.0 framework. According to them, the authorization endpoint is vulnerable to phishing attacks if TLS is not chosen for the implementation.

According to Francisco and Keren P. Lewison [87], OAuth is a double redirection protocol that opens several vulnerabilities. In OAuth, the application redirects the browser into a third-party authentication endpoint, and again, the application redirects the browser to a callback endpoint of the application. Here, if the third-party authorization endpoint is not protected with TLS, it is vulnerable to a phishing attack.

Suhas Pai [88] successfully discovered the known security vulnerability in OAuth using an alloy analyzer. They use the knowledge flow analysis technique to verify security protocols, especially authentication protocols. Here, the known security vulnerability concerns the client credentials stored on a desktop. According to Ryan Paul [89], a trained hacker can reverse engineer the code to access the client's credentials.

Security issues in OAuth have been discovered and evaluated in several other works. Common web application vulnerabilities, such as cross-site request forgeries and open redirectors, are discussed by Chetan Bansal *et al.* [90].

A formal analysis covering all four OAuth grant types (authorization code grant, implicit grant, resource owner password credentials grant, and client credentials grant) is discussed by D. Fett *et al.* [91]. They discover attacks such as the 307 redirect attack, Idp mix-up attack, state leak attack, and naive RP session integrity attack.

Savio [46] presents the OAuth-IoT framework for access control of resources in the IoT domain. The key element here is the gateway, which collects information from resource-constrained devices and controls access requests from third-party applications through the OAuth 2.0 authorization framework.

Srikanth [50] defines a system named Collaborative Appliance for Remote-help (CARE) that allows remote workers to access IoT devices to fix issues within devices. CARE uses OAuth to authorize the remote workers. According to this model, the worker is the OAuth resource owner, and the helper is the OAuth client.

Shami *et al.* [47] propose an approach to use the OAuth 2.0 protocol to provide secure authentication and authorization in IoT networks. The paper aims to efficiently manage the access control of the IoT with the use of a security manager. It consists of two steps: authentication and authorization. Here, two entities are involved in the authorization process: the security manager and service provider. The user who tries to access IoT networks is redirected to the security manager, who in turn is redirected to the service provider and is provided with an authorization code. This code, along with the client ID, is used by the security manager to request the access token. With this approach, the IoT network manager controls user access using the OAuth protocol.

The Internet Engineering Task Force (IETF) Authentication and Authorization for Constrained Environments (ACE) working group [92] extend authorization to IoT devices using OAuth 2.0. Here, OAuth 2.0 is used along with CoAP and concise binary object representation (CBOR) instead of JSON.

Solapurker [49] discusses a new approach of authentication in the healthcare system using OAuth 2.0 by removing the storage overhead of refresh tokens. Instead of refresh tokens, they use the JWT token to obtain the access token whenever needed. The JWT token includes details such as issuer, audience, subject, expiration, etc.

B. SECURITY ASSERTION MARKUP LANGUAGE AND eXtensible ACCESS CONTROL MARKUP LANGUAGE

SAML and XACML, defined by OASIS, are often used in combination to address different problems that fall under the first dimension of our classification: ABAC in the access control models section (section II).

SAML is an XML-based framework for exchanging authorization, identity, authentication, and attribute-related security information between entities. The terms subject and principal are interchangeably used to represent SAML assertions. These assertions are made by asserting parties or SAML authorities. He/she can be a user running the web browser with a SAML-enabled application. The primary use case of SAML is multi-domain single-sign-on (SSO). The SSO is defined using the SAML roles called the identity provider (IdP) and the service provider (SP) [97]. SAML can support different access control models, such as ABAC and RBAC.

The XACML language that defines ABAC policies is an XML-based language that defines requests, responses, and policies for secure communication [98]. In XACML, access control is defined based on ABAC. Various attributes, such as subject attributes, resource attributes, and environmental attributes, are used for access control [51].

T. Gross [99] presents a security analysis of the most important use case of SAML, SSO. This work discovers security loopholes that cause attacks on the protocol. The various attacks involve man-in-the-middle attacks, attacks by information leakage, and message replay/connection hijacking.

According to Francisco Corella [87], SAML is vulnerable to impersonation attacks. This work categorizes SAML into a double redirection protocol and defines the loophole. However, SAML along with XACML seems to be used in several IoT applications for authorization purposes.

According to Chongshan Ran and Guili Guo [100], the traditional XACML access control mechanism is not sufficiently secure. The major security components in XACML, such as the policy administration point (PAP), the policy decision point (PDP), and the policy information point (PIP), are interdependent. This may result in threats such as unauthorized information disclosure and thereby allow loss of message integrity.

According to Juan Deng *et al.* [101], XACML does not support a common class of security policies called security automata (SA). They validated security using validation tools such as Casper and FDR. To make XACML more secure, they propose a mechanism where XACML is extended to support SA.

However, the survey done by Aaff Ouaddah [23] points out the use of XACML access control policies in the IoT to solve several issues related to interoperability, content awareness, and granularity.

An adaptive risk-based control (AdRBAC) for IoT using XACML was proposed by Hany F. *et al.* [95]. They evaluate various other efficient languages and consider XACML to be the best for access control in the IoT.

Peter Ebinger [53] proposes a smart metering ecosystem for sustainable energy consumption. Here, XACML is used to design access control policies to manage access requests for sensor data or actuators. The use of XACML improves user privacy in smart grids. Similarly, an XACML-based access control architecture and design are implemented by Ji Eun Kim [68].

TABLE 5. Analysis of existing authorization frameworks in CPS and IoT based on access management standards.

Authorization framework in IoT	Authorization standards				Authorization protocol	Domain area
	OAuth	XACML	SAML	NGAC		
L. Seitz et al. (2013) [44]		yes	yes		CoAP	-
S. Cirani et al.(2015) [45]	yes				HTTP/CoAP	-
A. Niruntasukrat et al. (2016) [93]	yes				MQTT	-
S. Sciancalepore et al. (2017) [46]	yes				CoAP, HTTP	-
S. Emerson et al. (2015) [47]	yes				-	-
S. Chung et al. (2018) [48]	yes				CoAP	-
P. Solapurkar (2016) [49]	yes				HTTP	Healthcare
S. Jonnada et al. (2018) [50]	yes				HTTP	Remote collaboration systems
José L. Hernández-Ramos et al. (2015) [51]		yes	yes		CoAP, HTTPS	Smart buildings
Marlon C. Domenech et al. (2016) [52]		yes	yes		HTTP/HTTPS	Web of Things
Sergio Gusmeroli et al. (2013) [40]		yes	yes		HTTP	-
Ebinger P. et al. (2012) [53]		yes			-	Smart metering
J. E. Kim et al. (2012) [68]		yes			-	Smart homes
L. A. Charaf et al. (2020) [94]		yes			-	-
Atlam et al. (2018) [95]		yes			-	-
Bruhadeshwar Bezawada et al. (2018) [72]				yes	-	Smart homes
K. K. Kolluru et al. (2018) [96]				yes	CoAP	IIoT (district heating)
I. Ray et al. (2017) [73]				yes	-	Healthcare

Recently, Lalla Amina *et al.* [94] have proposed an access control system for the IoT using XACML. They assign the XACML module to each node or device in IoT networks to manage the access requests.

Jose L. H. [51] proposes an ARM-compliant IoT security framework for smart buildings. They extend the city explorer platform with discovery and security mechanisms. Here, authorization decisions based on access control policies are adopted using SAML and XACML. Here, the authentication manager who authenticates users to access services and devices in the smart building is based on SAML. The authentication manager uses SAML to generate and deliver authentication assertions to authorized users. The authorization decisions are made using XACML, which acts here as a standard language for access control policies.

Marlon [52] presents a security infrastructure for the Web of Things (WoT) (AA14WoT) that enables SSO for users and devices. The authentication and authorization are based on SAML and XACML. The solution is appropriate for cross-domain M2M applications. The SAML active client component of AA14WoT is the software component that implements SAML.

IdP is the other important component that authenticates the user and device, also performing SAML assertion validations. The infrastructure is flexible with respect to the implementation of different access control models using XACML, and the interoperability among entities using different models is achieved using SAML.

Sergio [40] proposes a capability-based security approach for authorization and access control mechanisms in the IoT. Here, the capability token elements are SAML/XACML-based. This approach can be used by enterprises and individuals to manage access control processes.

C. NEXT-GENERATION ACCESS CONTROL

NGAC is the next-generation access control policy introduced by NIST, which falls under the first dimension of our classification: ABAC in access control models (section II). In NGAC, the access control functionality of data services is almost completely separated from the operating environments. The basic elements of NGAC are users, objects, and operations.

The NGAC standard structure consists of a policy enforcement point (PEP), which handles user/device request; a policy decision point (PDP), which determines access and privileges; and a policy information point (PIP), where the elements and relations for decision making are stored [96].

NGAC is similar to XACML because they both use ABAC. However, they are different in various respects. The degree of separation of access control logic from operating environments and operational efficiency is greater for NGAC than for XACML. Because of the inheritance of XML benefits and drawbacks in XACML, its ability for attribute and policy management is poor compared to the relations-based NGAC standard. In addition, NGAC is more flexible in implementing DAC policies than XACML [102].

NGAC is compatible with authorization in the IoT framework, which is discussed in several works. Bruhadeshwar Bezawada *et al.* [72] have proposed an ABAC mechanism to secure home IoT environments using NGAC. NGAC is considered for the home IoT environment because of the highly contextual and dynamic environment of the home IoT environment. Here, security challenges such as home user awareness and DDoS attacks are addressed by populating each user's attributes according to ABAC into the policy information point (PIP) of NGAC.

K. K. Kolluru *et al.* [96] use ABAC to define access control policies using the NGAC standard. They selected NGAC over XACML because of the complex nature of XACML. Here, IoT devices are authorized using the NGAC, and the entire authorization system is integrated with the arrowhead framework [96] for precise access control for the IoT devices. The authorization system is tested using a simple district heating use case and infers the compatibility of NGAC for authorization in IoT devices.

I. Ray *et al.* [67] use ABAC with NGAC for policy management in healthcare systems. NGAC separates the access control logic from different operating environments, which makes it the most IoT-compatible standard of ABAC authorization.

In Table 5, we analyze different existing authorization frameworks in CPS and IoT based on access management standards along with different authorization protocols such as hypertext transfer protocol (HTTP), constrained application protocol (CoAP), and message queuing telemetry transport (MQTT) and discuss the use of different access management standards in different domain areas.

V. AUTHORIZATION GOVERNANCE

The third dimension of our classification is authorization governance. The different types of authorization governance are centralized and decentralized.

A. CENTRALIZED MODEL

The *centralized* authorization technique is the most common and traditional authorization governance approach. In this system, there is a central authority such as an administrator who controls and manages the entire authorization system. Most of the traditional access control models discussed in section II are based on centralized governance [24]. The delegation-based authorization discussed in section III and the delegation-based authorization standard OAuth are examples of centralized authorization techniques.

B. DECENTRALIZED MODEL

Decentralization was introduced early by the start of the internet in most aspects and applications, such as email, FTP, and the world wide web (i.e., no single company solely owns or governs these technologies and their deployments). Later, the introduction of the cloud accomplished centralization, where each cloud source is governed by specific centralized systems. The decentralization of authorization techniques does not rely on the traditional central authority of authorization. Here, anyone in the network can delegate their permissions autonomously without the need for a central administrator. Early private-public key frameworks such as pretty good privacy (PGP) were also completely decentralized [103]. Later, some central trust was added by introducing CA into this, effectively combining decentralized operation with centralized trust through the authentication/authorization server(s).

Recently, there has been a move towards decentralization of these servers/services. Decentralized authorization addresses problems such as a single attack on the main centralized server in traditional authorization systems, which makes the entire network vulnerable, and the ability of the central authority in the traditional authorization system to view all the permissions in the system [73].

Security schemes such as encryption, public key certificate, multi-tier authentication, lightweight authentication, and ID-based authentication are used to protect applications from attacks such as the DoS attack, man-in-the-middle attack, insider attack, eavesdropping, forgery, impersonation, insider attack, replay, and timing attacks. However, decentralization can address these attacks in a more effective way [104].

Shafagh *et al.* [74] present a decentralized authorization system with a cryptographically enforced access control service called Droplet. They discuss the existing approaches and their limitations. For instance, end-to-end encryption using a third party's public key results in hard-coded access control, which is not suitable for fine-grained access control, especially with high-volume data streams. Another current approach is ABAC, which is not cost-effective when considering a large volume of data.

VI. OBSERVATIONS AND ANALYSIS

Our paper studies and analyses various authorization techniques based on our three-dimensional classification of access control models, subgranting models, and authorization governance in CPS and IoT ecosystems with use cases in an industrial context that involves mobility, subcontractors, and autonomous machines that are not resource constrained and are able to carry out advanced tasks on behalf of others.

Access control models are one of the major key security systems related to authorization. We analyze and evaluate the importance of access control models in authorization systems in section II. Table 1 provides a comparative study of different access control models based on their strengths and weaknesses.

In addition, Table 4 shows a comprehensive analysis of different access control models along with subgranting models and centralized/decentralized approaches in previously proposed authorization frameworks.

According to the table, most of the centralized approaches rely on traditional access control models such as RBAC and ABAC. Most of the decentralized platforms that we have evaluated make use of the CAPBAC model, which is a token-based authorization model. Table 2 extends Table 4 by providing the strengths and weaknesses of the existing authorization frameworks.

Section III, which defines subgranting models such as delegation-based authorization and PoA-based authorization, is the main focus of this paper. We use Table 5 to show that delegation-based authorization is commonly applicable in IoT applications using OAuth. Most articles do not address the particular IoT domain in which OAuth is used. In addition, they propose that OAuth-based authorization models be applied to most smart networks.

Along with the conventional delegation-based authorizations that are increasing in the field of CPS and IoT, newer subgranting models using PoA are also discussed in this paper. We compare and evaluate different subgranting models using metrics such as type of authorization, communication type, tokens, control of expiration, and public key certificate. In addition, we provide an analysis based on strengths and weaknesses (Table 3). The PoA-based authorization approach is different from delegation-based authorization techniques in various aspects, as described in section III. However, it does exhibit similarities with OAuth-based delegation (see Table 3).

We survey OAuth and a range of other authorization standards, such as SAML, XACML, and NGAC, to evaluate the standards used in different CPS and IoT frameworks and to analyze the compatibility of different standards and techniques in different CPS and IoT application domains. SAML, XACML, and NGAC are used in specific domain areas, such as smart houses, smart metering, smart buildings, and healthcare. The different technologies that we surveyed in this paper can be used in combination for better security and usability. SAML and XACML are used together to build better authorization frameworks. Section IV B explains both SAML and XACML and how they are combined in different works.

The different types of authorization governance that we discussed in this paper are centralized and decentralized. OAuth-based delegation authorization is mostly used in a centralized environment. However, there are several approaches based on decentralized delegation-based authorization. The PoA-based approach can be categorized into a decentralized approach because the PoAs are independent documents and do not rely on a centralized server. However, the use of a centralized signatory registry and third-party CA makes it partially centralized.

There are still open research issues pertaining to PoA-based systems. Details on PoA syntax and semantics are needed, and protocol(s) to carry them out should be proposed based on suitable standards. Additionally, some proof of concept, including the integration of security principles, is needed. In a fully decentralized operation, the principal generates the PoA and sends it to the agent, and the agent submits it to the resource provider, so all of these parties must be capable of understanding and processing PoAs to various degrees. In particular, the resource provider must be able to provide access according to the PoA in cases where it could offer more information than what is defined/restricted in the PoA by the principal. Solutions to easily deploy such functionality are needed. Additionally, the signatory registry could be defined for storage of PoAs and to act as a third-party trust authority (making the solution partially centralized).

There are also open research issues related to the standards we covered. OAuth mentions certain processes to be out of scope, meaning that they have to be solved by extending the features. In the future, delegation-based authorization can be done in different ways in different situations. In addition to the use of a single access token, multiple access tokens for specific deployments are also possible. Access token management to manage the access tokens by providing a management URL that manages token revocation, rotation, etc. requires further studies. Moreover, future work is needed in terms of privacy and security considerations [105]. Certain vulnerabilities in well-deployed standards, protocols, and authorization mechanisms are still exploitable. Newer mechanisms are needed to analyze and correct these vulnerabilities. There is a trade-off with increased security in certain standards and techniques that can lead to less flexibility and scalability.

VII. CONCLUSION

Many mobile and industrial application scenarios assume semi-autonomous devices with sufficient resources and computing power that are able to access protected resources on behalf of the user and carry out advanced tasks. In this paper, we survey different authorization techniques in CPS and IoT with such non-resource constrained devices based on our three-dimensional classification, including access control models, subgranting models, and authorization governance. Here, we have studied the authorization techniques with respect to two different contributions: (i) general contributions and (ii) special contributions. In general contributions, we provide a high-level evaluation of access control models, including an analysis of the strengths and weaknesses of different approaches and access management standards based on our three-dimensional classification. In special contributions, we have described the subgranting techniques and the newer PoA-based authorization. We study, analyze, and compare different subgranting models with PoA-based authorizations using metrics such as type of authorization, communication type, tokens, control of expiration, and public key certificate. We also provide a comparison of the benefits and drawbacks of different authorization governances, such as centralized and decentralized approaches. Our observations and analysis (section VI) provide a summary of the findings and some open research issues.

APPENDIX

NOMENCLATURE

ABAC	Attribute-Based Access Control
ABE	Attribute-Based Encryption
ACE	Authorization for Constrained Environments
ACL	Access Control List
AdRBAC	Adaptive Risk-Based Control
CA	Certificate Authority
CapBAC	Capability-Based Access Control
CARE	Collaborative Appliance for Remote-help
CBOR	Concise Binary Object Representation
CCAAC	Capability-Based Context-Aware Access Control
CoAP	Constrained Application Protocol
CP-ABE	Ciphertext Policy ABE
CPS	Cyber Physical Systems
DAC	Discretionary Access Control
DRM	Digital Rights Management
DS	Delegation Server
DTLS	Datagram Transport Layer Security
HTTP	Hypertext Transfer Protocol

IAM	Identity and Access Management
IBE	Identity-Based Encryption
IETF	Internet Engineering Task Force
IdP	Identity Provider
IoT	Internet of Things
IoT-FM	IoT Federation Manager
IIoT	Industrial Internet of Things
KP-ABE	Key Policy ABE
LDAP	Lightweight Directory Access Protocol
MAC	Mandatory Access Control
MAC	Message Authentication Code
MQTT	Message Queuing Telemetry Transport
M2M	Machine-to-Machine
NGAC	Next-Generation Access Control
OBU	Onboard Unit
OAuth	Open Authorization
PAP	Policy Administration Point
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PGP	Pretty Good Privacy
PIP	Policy Information Point
PoA	Power of Attorney
RBAC	Role-Based Access Control
RBE	Role-Based Encryption
REST	Representational State Transfer
RSU	Roadside Unit
SA	Security Automata
SAML	Security Assertion Markup Language
SSO	Single-Sign-On
TA	Trusted Authority
TRE	Timed-Release Encryption
UCON	Usage Control
VANET	Vehicular ad hoc Network
V2V	Vehicle-to-Vehicle
V2I	Vehicle-to-Infrastructure
WoT	Web of Things
XACML	eXtensible Access Control Markup Language

REFERENCES

[1] M. Gupta and R. Sandhu, "Authorization framework for secure cloud assisted connected cars and vehicular Internet of Things," in *Proc. 23nd ACM Symp. Access Control Models Technol.* New York, NY, USA: ACM, Jun. 2018, pp. 193–204.

[2] S. S. Vattaparambil, R. Koduri, S. Nandyala, and M. Manalikandy, "Scalable decentralized solution for secure vehicle-to-vehicle communication," SAE Tech. Paper 2020-01-0724, 2020.

[3] S. R. Moosavi, T. N. Gia, A.-M. Rahmani, E. Nigussie, S. Virtanen, J. Isoaho, and H. Tenhunen, "SEA: A secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways," *Procedia Comput. Sci.*, vol. 52, pp. 452–459, Jan. 2015.

[4] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for smart cities," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 22–32, Feb. 2014.

[5] S. D. T. Kelly, N. K. Suryadevara, and S. C. Mukhopadhyay, "Towards the implementation of IoT for environmental condition monitoring in homes," *IEEE Sensors J.*, vol. 13, no. 10, pp. 3846–3853, Oct. 2013.

[6] N. Bui, A. Castellani, P. Casari, and M. Zorzi, "The Internet of energy: A Web-enabled smart grid system," *IEEE Netw.*, vol. 26, no. 4, pp. 39–45, 2012.

[7] R. Basir, S. Qaisar, M. Ali, M. Aldwairi, M. I. Ashraf, A. Mahmood, and M. Gidlund, "Fog computing enabling industrial Internet of Things: State-of-the-art and research challenges," *Sensors*, vol. 19, no. 21, p. 4807, Nov. 2019.

[8] M. El-hajj, M. Chamoun, A. Fadlallah, and A. Serhrouchni, "Taxonomy of authentication techniques in Internet of Things (IoT)," in *Proc. IEEE 15th Student Conf. Res. Develop. (SCOReD)*, Dec. 2017, pp. 67–71.

[9] X. Zhu and Y. Badr, "Identity management systems for the Internet of Things: A survey towards blockchain solutions," *Sensors*, vol. 18, no. 12, p. 4215, Dec. 2018.

[10] H. Nicanfar, P. Jokar, and V. C. M. Leung, "Smart grid authentication and key management for unicast and multicast communications," in *Proc. IEEE PES Innov. Smart Grid Technol.*, Nov. 2011, pp. 1–8.

[11] J. S. Alshudukhi, Z. G. Al-Mekhlafi, and B. A. Mohammed, "A lightweight authentication with privacy-preserving scheme for vehicular ad hoc networks based on elliptic curve cryptography," *IEEE Access*, vol. 9, pp. 15633–15642, 2021.

[12] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial Internet of Things: Challenges, opportunities, and directions," *IEEE Trans. Ind. Informat.*, vol. 14, no. 11, pp. 4724–4734, Nov. 2018.

[13] M. Park, H. Oh, and K. Lee, "Security risk measurement for information leakage in IoT-based smart homes from a situational awareness perspective," *Sensors*, vol. 19, no. 9, p. 2148, May 2019.

[14] M. Abdur, S. Habib, M. Ali, and S. Ullah, "Security issues in the Internet of Things (IoT): A comprehensive study," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 6, p. 383, 2017.

[15] C.-W. Tien, T.-T. Tsai, I.-Y. Chen, and S.-Y. Kuo, "UFO–Hidden backdoor discovery and security verification in IoT device firmware," in *Proc. IEEE Int. Symp. Softw. Rel. Eng. Workshops (ISSREW)*, Oct. 2018, pp. 18–23.

[16] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.

[17] I. Ali, A. I. A. Ahmed, A. Almogren, M. A. Raza, S. A. Shah, A. Khan, and A. Gani, "Systematic literature review on IoT-based botnet attack," *IEEE Access*, vol. 8, pp. 212220–212232, 2020.

[18] K. Zhang, X. Liang, R. Lu, and X. Shen, "Sybil attacks and their defenses in the Internet of Things," *IEEE Internet Things J.*, vol. 1, no. 5, pp. 372–383, Oct. 2014.

[19] A. Raoof, A. Matrawy, and C.-H. Lung, "Routing attacks and mitigation methods for RPL-based Internet of Things," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1582–1606, 2nd Quart., 2019.

[20] M. Trnka, T. Cerny, and N. Stickney, "Survey of authentication and authorization for the Internet of Things," *Secur. Commun. Netw.*, vol. 2018, pp. 1–17, Jun. 2018.

[21] M. El-hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni, "A survey of Internet of Things (IoT) authentication schemes," *Sensors*, vol. 19, no. 5, p. 1141, Mar. 2019.

[22] M. Bilal, M. Asif, and A. Bashir, "Assessment of secure OpenID-based DAAA protocol for avoiding session hijacking in Web applications," *Secur. Commun. Netw.*, vol. 2018, pp. 1–10, Nov. 2018.

[23] A. Ouaddah, H. Mousannif, A. A. Elkalam, and A. A. Ouahman, "Access control in IoT: Survey & state of the art," in *Proc. 5th Int. Conf. Multimedia Comput. Syst. (ICMCS)*, Sep. 2016, pp. 272–277.

[24] E. Bertin, D. Hussein, C. Sengul, and V. Frey, "Access control in the Internet of Things: A survey of existing approaches and open research questions," *Ann. Telecommun.*, vol. 74, nos. 7–8, pp. 375–388, Aug. 2019.

[25] S. Ravidas, A. Lekidis, F. Paci, and N. Zannone, "Access control in Internet-of-Things: A survey," *J. Netw. Comput. Appl.*, vol. 144, pp. 79–101, Oct. 2019.

[26] J. Qiu, Z. Tian, C. Du, Q. Zuo, S. Su, and B. Fang, "A survey on access control in the age of Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 4682–4696, Jun. 2020.

[27] M. Saghir, B. A. H. A. Al Khair, J. Hamodi, and N. Abdullah, "Traditional versus decentralized access control for Internet of Things (IoT): Survey," in *Proc. Int. Conf. Reliable Inf. Commun. Technol.* Cham, Switzerland: Springer, 2019, pp. 486–494.

[28] S. De Capitani di Vimercati, S. Foresti, and P. Samarati, *Authorization and Access Control.* Berlin, Germany: Springer, 2007, pp. 39–53.

[29] F. Ullah, J. Wang, M. Farhan, S. Jabbar, M. K. Naseer, and M. Asif, "LSA based smart assessment methodology for SDN infrastructure in IoT environment," *Int. J. Parallel Program.*, vol. 48, no. 2, pp. 162–177, Apr. 2020.

[30] J. Faircloth, "Information security," in *Enterprise Applications Administration*, J. Faircloth, Ed. Boston, MA, USA: Morgan Kaufmann, 2014, ch. 5, pp. 175–220.

[31] D. Rountree, "What is federated identity?" in *Federated Identity Primer*, D. Rountree, Ed. Boston, MA, USA: Syngress, 2013, ch. 2, pp. 13–36.

[32] G.-J. Ahn and R. Sandhu, "Role-based authorization constraints specification," *ACM Trans. Inf. Syst. Secur.*, vol. 3, no. 4, pp. 207–226, Nov. 2000.

[33] A. A. El Hassani, A. A. El Kalam, and A. A. Ouahman, "Integrity-organization based access control for critical infrastructure systems," in *Critical Infrastructure Protection VI*, J. Butts and S. Shenoi, Eds. Berlin, Germany: Springer, 2012, pp. 31–42.

[34] J. Shu, L. Shi, B. Xia, and L. Liu, "Study on action and attribute-based access control model for Web services," in *Proc. 2nd Int. Symp. Inf. Sci. Eng.*, Dec. 2009, pp. 213–216.

[35] B. Lang, I. Foster, F. Siebenlist, R. Ananthakrishnan, and T. Freeman, "A flexible attribute based access control method for grid computing," *J. Grid Comput.*, vol. 7, no. 2, p. 169, 2009.

[36] D. Huang, Q. Dong, and Y. Zhu, *Attribute-Based Encryption and Access Control*. Boca Raton, FL, USA: CRC Press, 2020.

[37] F. Cai, N. Zhu, J. He, P. Mu, W. Li, and Y. Yu, "Survey of access control models and technologies for cloud computing," *Cluster Comput.*, vol. 22, no. S3, pp. 6111–6122, May 2019.

[38] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proc. Annu. Int. Conf. theory Appl. Cryptograph. Techn.* Berlin Springer, 2005, pp. 457–473.

[39] C.-L. Hsu, W.-X. Chen, and T.-V. Le, "An autonomous log storage management protocol with blockchain mechanism and access control for the Internet of Things," *Sensors*, vol. 20, no. 22, p. 6471, Nov. 2020.

[40] S. Gusmeroli, S. Piccione, and D. Rotondi, "A capability-based security approach to manage access control in the Internet of Things," *Math. Comput. Model.*, vol. 58, nos. 5–6, pp. 1189–1205, Sep. 2013.

[41] S. Gusmeroli, S. Piccione, and D. Rotondi, "IoT access control issues: A capability based approach," in *Proc. 6th Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput.*, Jul. 2012, pp. 787–792.

[42] J. Park and R. Sandhu, "The UCON$_{ABC}$ usage control model," *ACM Trans. Inf. Syst. Secur.*, vol. 7, no. 1, pp. 128–174, 2004.

[43] A. Ouaddah, H. Mousannif, and A. A. Ouahman, "Access control models in IoT: The road ahead," in *Proc. IEEE/ACS 12th Int. Conf. Comput. Syst. Appl. (AICCSA)*, Nov. 2015, pp. 1–2.

[44] L. Seitz, G. Selander, and C. Gehrmann, "Authorization framework for the Internet-of-Things," in *Proc. IEEE 14th Int. Symp. World Wireless, Mobile Multimedia Netw. (WoWMoM)*, Jun. 2013, pp. 1–6.

[45] S. Cirani, M. Picone, P. Gonizzi, L. Veltri, and G. Ferrari, "IoT-OAS: An OAuth-based authorization service architecture for secure services in IoT scenarios," *IEEE Sensors J.*, vol. 15, no. 2, pp. 1224–1234, Feb. 2015.

[46] S. Sciancalepore, G. Piro, D. Caldarola, G. Boggia, and G. Bianchi, "OAuth-IoT: An access control framework for the Internet of Things based on open standards," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Jul. 2017, pp. 676–681.

[47] S. Emerson, Y.-K. Choi, D.-Y. Hwang, K.-S. Kim, and K.-H. Kim, "An OAuth based authentication mechanism for IoT networks," in *Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Oct. 2015, pp. 1072–1074.

[48] S.-H. Chung, J. H. Kim, and Y. Kim, "Pragmatic approach using OAuth mechanism for IoT device authorization in cloud," in *Proc. Int. Conf. Adv. Comput., Commun. Control Netw. (ICACCCN)*, Oct. 2018, pp. 1–4.

[49] P. Solapurkar, "Building secure healthcare services using OAuth 2.0 and JSON Web token in IoT cloud scenario," in *Proc. 2nd Int. Conf. Contemp. Comput. Informat. (IC3I)*, Dec. 2016, pp. 99–104.

[50] S. Jonnada, R. Dantu, P. Shrestha, I. Ranasinghe, and L. Widick, "An OAuth-based authorization framework for access control in remote collaboration systems," in *Proc. Nat. Cyber Summit (NCS)*, Jun. 2018, pp. 38–44.

[51] J. L. Hernández-Ramos, M. V. Moreno, J. B. Bernabé, D. G. Carrillo, and A. F. Skarmeta, "SAFIR: Secure access framework for IoT-enabled services on smart buildings," *J. Comput. Syst. Sci.*, vol. 81, no. 8, pp. 1452–1463, Dec. 2015.

[52] M. C. Domenech, A. Boukerche, and M. S. Wangham, "An authentication and authorization infrastructure for the Web of things," in *Proc. 12th ACM Symp. QoS Secur. Wireless Mobile Netw.* New York, NY, USA: ACM, Nov. 2016, pp. 39–46.

[53] P. Ebinger, J. L. Hernández Ramos, P. Kikiras, M. Lischka, and A. Wiesmaier, "Privacy in smart metering ecosystems," in *Smart Grid Security*, J. Cuellar, Ed. Berlin, Germany: Springer, 2013, pp. 120–131.

[54] R. Hummen, H. Shafagh, S. Raza, T. Voig, and K. Wehrle, "Delegation-based authentication and authorization for the IP-based Internet of Things," in *Proc. 11th Annu. IEEE Int. Conf. Sens., Commun., Netw. (SECON)*, Jun. 2014, pp. 284–292.

[55] G. Sciarretta, R. Carbone, and S. Ranise, "A delegated authorization solution for smart-city mobile applications," in *Proc. IEEE 2nd Int. Forum Res. Technol. Soc. Ind. Leveraging Better Tomorrow (RTSI)*, Sep. 2016, pp. 1–6.

[56] F. Fernández, A. Alonso, L. Marco, and J. Salvachúa, "A model to enable application-scoped access control as a service for IoT using OAuth 2.0," in *Proc. 20th Conf. Innov. Clouds, Internet Netw. (ICIN)*, Mar. 2017, pp. 322–324.

[57] A. Alshehri and R. Sandhu, "Access control models for virtual object communication in cloud-enabled IoT," in *Proc. IEEE Int. Conf. Inf. Reuse Integr. (IRI)*, Aug. 2017, pp. 16–25.

[58] O. Garcia-Morchon and K. Wehrle, "Modular context-aware access control for medical sensor networks," in *Proc. 15th ACM Symp. Access Control Models Technol. (SACMAT)*. New York, NY, USA: ACM, 2010, pp. 129–138.

[59] A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, "Towards a novel privacy-preserving access control model based on blockchain technology in IoT," in *Proc. Eur. MENA Cooperation Adv. Inf. Commun. Technol.*, Á. Rocha, M. Serrhini, and C. Felgueiras, Eds. Cham, Switzerland: Springer, 2017, pp. 523–533.

[60] G. Zhang and J. Tian, "An extended role based access control model for the Internet of Things," in *Proc. Int. Conf. Inf., Netw. Autom. (ICINA)*, vol. 1, Oct. 2010, pp. V1-319–V1-323.

[61] J. Jindou, Q. Xiaofeng, and C. Cheng, "Access control method for Web of things based on role and SNS," in *Proc. IEEE 12th Int. Conf. Comput. Inf. Technol.*, Oct. 2012, pp. 316–321.

[62] E. Barka, S. S. Mathew, and Y. Atif, "Securing the Web of things with role-based access control," in *Codes, Cryptology, and Information*, S. El Hajji, A. Nitaj, C. Carlet, and E. M. Souidi, Eds. Cham, Switzerland: Springer, 2015, pp. 14–26.

[63] O. J. A. Pinno, A. R. A. Gregio, and L. C. E. De Bona, "ControlChain: Blockchain as a central enabler for access control authorizations in the IoT," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2017, pp. 1–6.

[64] R. Neisse, G. Steri, and G. Baldini, "Enforcement of security policy rules for the Internet of Things," in *Proc. IEEE 10th Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob)*, Oct. 2014, pp. 165–172.

[65] D. Hussein, E. Bertin, and V. Frey, "A community-driven access control approach in distributed IoT environments," *IEEE Commun. Mag.*, vol. 55, no. 3, pp. 146–153, Mar. 2017.

[66] S. M. R. Islam, M. Hossain, R. Hasan, and T. Q. Duong, "A conceptual framework for an IoT-based health assistant and its authorization model," in *Proc. IEEE 8th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Jan. 2018, pp. 616–621.

[67] I. Ray, B. Alangot, S. Nair, and K. Achuthan, "Using attribute-based access control for remote healthcare monitoring," in *Proc. 4th Int. Conf. Softw. Defined Syst. (SDS)*, May 2017, pp. 137–142.

[68] J. E. Kim, G. Boulos, J. Yackovich, T. Barth, C. Beckel, and D. Mosse, "Seamless integration of heterogeneous devices and access control in smart homes," in *Proc. 8th Int. Conf. Intell. Environ.*, Jun. 2012, pp. 206–213.

[69] G. Zhang and W. Gong, "The research of access control based on UCON in the Internet of Things," *J. Softw.*, vol. 6, no. 4, pp. 724–731, Apr. 2011.

[70] R. Xu, Y. Chen, E. Blasch, and G. Chen, "BlendCAC: A BLockchain-enabled decentralized capability-based access control for IoTs," in *Proc. IEEE Int. Conf. Internet Things (iThings), IEEE Green Comput. Commun. (GreenCom), IEEE Cyber, Phys. Social Comput. (CPSCom), IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1027–1034.

[71] A. Lohachab and Karambir, "Next generation computing: Enabling multilevel centralized access control using UCON and CapBAC model for securing IoT networks," in *Proc. Int. Conf. Commun., Comput. Internet Things (IC IoT)*, Feb. 2018, pp. 159–164.

[72] B. Bezawada, K. Haefner, and I. Ray, "Securing home IoT environments with attribute-based access control," in *Proc. 3rd ACM Workshop Attribute-Based Access Control*. New York, NY, USA: ACM, Mar. 2018, pp. 43–53.

[73] M. P. Andersen, J. Kolb, K. Chen, G. Fierro, D. E. Culler, and R. A. Popa, "Wave: A decentralized authorization system for IoT via blockchain smart contracts," Univ. California Berkeley, Berkeley, CA, USA, Tech. Rep. UCB/EECS-2017-234, 2017.

[74] H. Shafagh, L. Burkhalter, A. Hithnawi, and S. Ratnasamy, "Droplet: Decentralized authorization and access control for encrypted data streams," 2018, *arXiv:1806.02057*. [Online]. Available: http://arxiv.org/abs/1806.02057

[75] A. F. Skarmeta, J. L. Hernández-Ramos, and M. V. Moreno, "A decentralized approach for security and privacy challenges in the Internet of Things," in *Proc. IEEE World Forum Internet Things (WF-IoT)*, Mar. 2014, pp. 67–72.

[76] N. Tapas, G. Merlino, and F. Longo, "Blockchain-based IoT-cloud authorization and delegation," in *Proc. IEEE Int. Conf. Smart Comput. (SMARTCOMP)*, Jun. 2018, pp. 411–416.

[77] N. Ahmed and C. D. Jensen, "A mechanism for identity delegation at authentication level," in *Identity and Privacy in the Internet Age*, A. Jøsang, T. Maseng, and S. J. Knapskog, Eds. Berlin, Germany: Springer, 2009, pp. 148–162.

[78] D. Mercredi and R. Frey, "User login delegation," U.S. Patent App. 10 398 356, Jan. 22, 2004.

[79] V. Beltran and A. F. Skarmeta, "An overview on delegated authorization for CoAP: Authentication and authorization for constrained environments (ACE)," in *Proc. IEEE 3rd World Forum Internet Things (WF-IoT)*, Dec. 2016, pp. 706–710.

[80] I. Bouij-Pasquier, A. A. El Kalam, A. A. Ouahman, and M. De Montfort, "A security framework for Internet of Things," in *Cryptology and Network Security*, M. Reiter and D. Naccache, Eds. Cham, Switzerland: Springer, 2015, pp. 19–31.

[81] B. Anggorojati, P. N. Mahalle, N. R. Prasad, and R. Prasad, "Capability-based access control delegation model on the federated IoT network," in *Proc. 15th Int. Symp. Wireless Pers. Multimedia Commun.*, 2012, pp. 604–608.

[82] S. Vattaparambil Sudarsan, O. Schelén, and U. Bodin, "A model for signatories in cyber-physical systems," in *Proc. 25th IEEE Int. Conf. Emerg. Technol. Factory Autom. (ETFA)*, Sep. 2020, pp. 15–21.

[83] B. Leiba, "OAuth Web authorization protocol," *IEEE Internet Comput.*, vol. 16, no. 1, pp. 74–77, Jan. 2012.

[84] D. Hardt, *The OAuth 2.0 Authorization Framework*, document RFC 6749, Oct. 2012.

[85] E. Hammer-Lahav, D. Recordon, and D. Hardt, *The OAuth 1.0 Protocol*, document RFC 5849, Apr. 2010.

[86] F. Yang and S. Manoharan, "A security analysis of the OAuth protocol," in *Proc. IEEE Pacific Rim Conf. Commun., Comput. Signal Process. (PACRIM)*, Aug. 2013, pp. 271–276.

[87] F. Corella and K. Lewison, "Security analysis of double redirection protocols," Pomcor, Tech. Rep., 2011. [Online]. Available: https://pomcor.com/techreports/DoubleRedirection.pdf

[88] S. Pai, Y. Sharma, S. Kumar, R. M. Pai, and S. Singh, "Formal verification of OAuth 2.0 using alloy framework," in *Proc. Int. Conf. Commun. Syst. Netw. Technol.*, Jun. 2011, pp. 655–659.

[89] G. Stringhini, M. Egele, C. Kruegel, and G. Vigna, "Poultry markets: On the underground economy of Twitter followers," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 42, no. 4, pp. 527–532, 2012.

[90] C. Bansal, K. Bhargavan, and S. Maffeis, "Discovering concrete attacks on Website authorization by formal analysis," in *Proc. IEEE 25th Comput. Secur. Found. Symp.*, Jun. 2012, pp. 247–262.

[91] D. Fett, R. Küsters, and G. Schmitz, "A comprehensive formal security analysis of OAuth 2.0," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.* New York, NY, USA: ACM, Oct. 2016, pp. 1204–1215.

[92] L. Seitz, G. Selander, E. Wahlstroem, S. Erdtman, and H. Tschofenig, "Authorization for the Internet of Things using OAuth 2.0," Internet Eng. Task Force (IETF), Fremont, CA, USA, Tech. Rep., 2015. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-ace-oauth-authz/00/

[93] A. Niruntasukrat, C. Issariyapat, P. Pongpaibool, K. Meesublak, P. Aiumsupucgul, and A. Panya, "Authorization mechanism for MQTT-based Internet of Things," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC)*, May 2016, pp. 290–295.

[94] L. A. Charaf, I. Alihamidi, A. Addaim, and A. A. Madi, "A distributed XACML based access control architecture for IoT systems," in *Proc. 1st Int. Conf. Innov. Res. Appl. Sci., Eng. Technol. (IRASET)*, Apr. 2020, pp. 1–5.

[95] H. F. Atlam, M. O. Alassafi, A. Alenezi, R. J. Walters, and G. B. Wills, "XACML for building access control policies in Internet of Things," in *Proc. 3rd Int. Conf. Internet Things, Big Data Secur.*, 2018, pp. 253–260.

[96] K. K. Kolluru, C. Paniagua, J. van Deventer, J. Eliasson, J. Delsing, and R. J. DeLong, "An AAA solution for securing industrial IoT devices using next generation access control," in *Proc. IEEE Ind. Cyber-Phys. Syst. (ICPS)*, May 2018, pp. 737–742.

[97] S. Cantor, J. Moreh, R. Philpott, and E. Maler, "Metadata for the OASIS security assertion markup language (SAML) V2.0," Tech. Rep. saml-metadata-2.0-os, 2005. [Online]. Available: https://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf

[98] R. Sinnema and E. Wilde, "eXtensible access control markup language (XACML) XML media type," Internet Eng. Task Force (IETF), Fremont, CA, USA, Tech. Rep., 2013, pp. 1–8. [Online]. Available: https://datatracker.ietf.org/doc/draft-sinnema-xacml-media-type/00/

[99] T. Gross, "Security analysis of the SAML single sign-on browser/artifact profile," in *Proc. 19th Annu. Comput. Secur. Appl. Conf.*, 2003, pp. 298–307.

[100] C. Ran and G. Guo, "Security XACML access control model based on SOAP encapsulate," in *Proc. Int. Conf. Comput. Sci. Service Syst. (CSSS)*, Jun. 2011, pp. 2543–2546.

[101] J. Deng, R. Brooks, and J. Taiber, "Security automata integrated XACML and security validation," in *Proc. IEEE SoutheastCon (SoutheastCon)*, Mar. 2010, pp. 338–343.

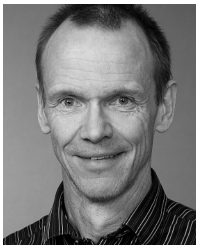
[102] D. Ferraiolo, R. Chandramouli, R. Kuhn, and V. Hu, "Extensible access control markup language (XACML) and next generation access control (NGAC)," in *Proc. ACM Int. Workshop Attribute Access Control (ABAC)*, 2016, pp. 13–24.

[103] S. Garfinkel, *PGP: Pretty Good Privacy*. Newton, MA, USA: O'Reilly Media, 1995.

[104] M. Tahir, M. Sardaraz, S. Muhammad, and M. S. Khan, "A lightweight authentication and authorization framework for blockchain-enabled IoT network in health-informatics," *Sustainability*, vol. 12, no. 17, p. 6960, Aug. 2020.

[105] F. I. J. Richer and A. Parecki. (2020). *Grant Negotiation Authorization Protocol WG (GNAP)*. [Online]. Available: https://datatracker.ietf.org/doc/charter-ietf-gnap/

SREELAKSHMI VATTAPARAMBIL SUDARSAN received the M.Sc. degree in computer science with a specialization in cyber security from the Cochin University of Science and Technology (CUSAT). She is currently pursuing the Ph.D. degree with the Luleå University of Technology. Her master's thesis was on secure, decentralized vehicle-to-vehicle communication. Her current research interest includes authorization techniques in the IoT.



OLOV SCHELÉN (Member, IEEE) is currently a Professor with the Luleå University of Technology and the CEO at Xarepo AB. He has more than 25 years of experience in industry and academia. His research interests include mobile and distributed systems, industrial IoT and CPS, software orchestration, computer networking, artificial intelligence, and blockchain.

ULF BODIN is currently a Professor with the Luleå University of Technology, where he is conducting research on the industrial IoT, distributed system of systems, computer communications, distributed ledgers, and applied machine learning. His experience includes working more than 15 years in the software industry, ETSI, and in several other standardization organizations.