ABAC-CC: Attribute-Based Access Control and Communication Control for Internet of Things

Smriti Bhatt
Department of Computing and Cyber Security,
Texas A&M University-San Antonio
San Antonio, Texas
sbhatt@tamusa.edu

Ravi Sandhu
Institute for Cyber Security and CREST C-SPECC
Department of Computer Science,
University of Texas at San Antonio
ravi.sandhu@utsa.edu

Abstract

Internet of Things (IoT) is revolutionizing the capabilities of the Internet with billions of connected devices in the cyberspace. These devices are commonly referred to as *smart things* enabling smart environments, such as Smart Home, Smart Health, Smart Transportation, and overall Smart Communities, together with key enabling technologies like Cloud Computing, Artificial Intelligence (AI) and Machine Learning (ML). Security and privacy are major concerns for today's diverse autonomous IoT ecosystem. Autonomous things and a large amount of data associated with things have fueled significant research in IoT access control and privacy in both academia and industry. To enable futuristic IoT with sustainable growth, dynamic access and communication control framework that adequately addresses security and privacy issues in IoT is inevitable. In this paper, we analyze the access and communication control requirements in Cloud-Enabled IoT (CE-IoT) and propose an ***attribute-based*** framework for access control and communication control, known as **ABAC-CC**, to secure accesses and communications (data flow) between various entities in the IoT architecture. We also introduce a novel Attribute-Based Communication Control (ABCC) model, which focuses on securing communications and data flow in IoT and enables users to define privacy policies using attributes of various entities. Furthermore, we analyze the applicability of ABAC-CC in specific IoT application domains, and finally, we present future research directions in the context of Cloud and Edge computing enabled IoT platforms.

CCS Concepts

• **Security and privacy** → **Access control**; **Authorization**.

Keywords

Internet of Things; Attributes; Message Attributes; Cloud-Enabled IoT; Communication Control; Attribute-Based Communication Control;

ACM Reference Format:
Smriti Bhatt and Ravi Sandhu. 2020. ABAC-CC: Attribute-Based Access Control and Communication Control for Internet of Things. In *Proceedings of the 25th ACM Symposium on Access Control Models and Technologies (SACMAT '20), June 10–12, 2020, Barcelona, Spain.* ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3381991.3395618

SACMAT '20, June 10–12, 2020, Barcelona, Spain

ACM ISBN 978-1-4503-7568-9/20/06…$15.00
https://doi.org/10.1145/3381991.3395618

1 Introduction

Internet of Things (IoT), with "anything" and "everything" being connected to the Internet, is becoming a pervasive reality of our lives today. IoT devices are rapidly expanding both in terms of numbers and capabilities. With advancements in IoT enabling technologies, such as Cloud and Edge computing, Artificial Intelligence (AI), and Machine Learning (ML), users envision an autonomous smart ecosystem where everything will be connected and continuously communicating with each other. For example, in a Smart Home scenario, you will be able to turn on smart appliances when leaving from work to home, for your convenience. More specifically, turn on the thermostat with desired set temperature, set and play your desired music, and turn on your smart cooker with set timer, so that as you reach home you have a relaxing ambience with your food ready. Some of these are already shaping into reality with IoT devices like a smart thermostat by NEST [8], or a smart watch monitoring health and fitness, e.g., Fitbit [5], Apple watch [2].

However, this smart vision brings several challenges and concerns with huge number of Internet-connected devices and other services involved, e.g., Cloud and Edge Computing services. For users, managing billion of IoT devices and data in their associated Cloud platforms can soon become a nightmare. Moreover, the exponential growth of connected smart devices, with expected number of IoT devices to reach 25 billion devices by 2025 [46], tremendously expands the IoT attack surface and raises various security and privacy concerns for the users. It is a challenging task to address security and privacy issues in dynamic and evolving IoT space with heterogeneous devices, communication platforms and protocols. Therefore, a systematic and dynamic research approach is essential to secure access, authorization, communication and data flow in IoT for its continued success in the future.

1.1 Motivation

IoT devices have some unique characteristics which makes them distinct compared to other Internet-connected user devices, such as computers and smartphones. Some of these distinct characteristics are discussed as follows.

- **Distributed and Remote Location:** IoT devices are widely distributed and remotely located in different locations where sometimes users do not have any physical control over these devices, unlike their personal laptops or smartphones.
- **Diverse Nature:** IoT devices vary in size, capability and functionality, communication and networking mechanisms or protocols, and are manufactured by various vendors that

have their own Cloud platforms to enable authentication, authorization, and communication.
- **Autonomicity:** IoT devices, once deployed, can act autonomously with technologies like AI and ML along with Cloud capabilities (e.g., storage, computation, analytics).
- **Dynamic Behavior**: IoT devices behave differently in different scenarios based on the characteristics and contexts for different users. Thus, contextual parameters play a vital role in securing and managing these devices.

With such evolving characteristics of IoT devices, managing security and privacy in IoT becomes even bigger challenge. In this paper, we mainly focus on access control and communication control aspects of security and privacy in Cloud-Enabled IoT. Traditional access control models are inadequate to address the dynamic and diverse access control requirements for the future IoT ecosystem with new emerging capabilities and applications. Most of the current IoT access control models [46] in the literature have focused on a single centralized cloud IoT platform and are based on the dominant access control model, viz Role-Based Access Control (RBAC) [27, 42]. However, IoT will soon move beyond a single Cloud platform and access control and authorization will be managed or shared across a set of collaborating Cloud providers or servers and become decentralized [46]. In the realm of the diverse and dynamic nature of IoT, we believe that different characteristics (or attributes) of users, devices, and context need to be employed beyond *roles* in identifying the authorizations associated with IoT devices and applications.

In addition to access control, communications in terms of data flow in the IoT architecture need to be secured from unauthorized data access and modifications. With pervasive IoT devices (e.g., smart wearable devices and medical IoT devices), collecting, storing, and sharing sensitive user data, novel communication and data flow control mechanisms need to be developed with detailed research for preserving user data privacy. However, an access and communication control framework for IoT remains yet to be developed. In this paper, we propose an ***attribute-based access control and communication control framework***, known as **ABAC-CC**, to secure accesses and communications in the context of Cloud-Enabled IoT architecture with multiple devices, gateways, and multiple Cloud services providers. It utilizes attributes of different entities, such as users, devices, gateways, etc., to secure access and authorizations, and to determine allowed communications and data flow among various entities in IoT. While Attribute-Based Access Control (ABAC) [29] has received significant attention in academia, it is still in early transition phase in the industry.

On the other hand, in this research, we introduce the novel **Attribute-Based Communication Control (ABCC)** model, which can secure data communication and flow between different entities in Cloud and edge network based on specified attribute-based communication control policies. These policies are written using the attributes of relevant IoT entities (e.g., devices, gateways, and virtual objects (VOs)) including a new type of attribute, i.e., the **message attributes**. In the ABCC model, we introduce *message attributes* where attributes of the message are derived from the content or data in the message. IoT devices are continuously gathering and sharing messages with different entities in the IoT architecture. Messages are the *unit of communication*, and communication control policies utilize message/data attributes *(attribute name and value)* along with other attributes of relevant entities, such as users, devices, and gateways [16]. Users can also define communication control policies based on their privacy requirements. Besides, with expected IoT advancements in the future and a collaborative IoT framework, we identify the Attribute-Based Communication Control (ABCC) model as an essential component of the ABAC-CC framework to enable secure communications across multiple smart devices, gateways, and multiple Cloud platforms.

The rest of the paper is divided into six sections. Section 2 discusses brief background and related work. Section 3 presents current and future access control and communication control requirements in diverse and evolving IoT architecture. Section 4 introduces the basic conceptual ABCC model and discusses various entities and types of attributes involved in ABCC policies. Section 5 presents the ABAC-CC framework and depicts its applicability in IoT use case scenarios. Section 6 presents potential future research directions, followed by conclusion in Section 7.

2 Background and Related Work

In this section, we first provide brief overview of today's dominant IoT paradigm - the Cloud-Enabled Internet of Things that we are considering in this research. We then briefly discuss related work on attribute-based access control and communication control mechanisms.

2.1 Cloud-Enabled Internet of Things (IoT)

Today, IoT is being explored in various sectors, such as commerce, government, academia, and industry. Generally, IoT devices or "things" are resource-constrained with limited storage, power, and computation capabilities. An emerging IoT architecture today is the integration of Cloud and IoT, with major cloud service providers (CSPs) offering IoT services and applications on top of their existing cloud framework [9, 20]. Cloud computing has become a key enabling technology with virtually unlimited capabilities (e.g., storage, computation, analytics) for IoT devices that supports its ongoing and future success in a sustainable manner.

The integration of Cloud and IoT has been widely suggested in the literature [12, 15, 24, 31, 38, 41]. In industry, major CSPs, such as Amazon Web Services (AWS) [1], Microsoft Azure [11], Google Cloud [6] Cloud, including others, have introduced new IoT services. The integration of Cloud and IoT forms a new powerful Cloud-Enabled Internet of Things (CE-IoT) paradigm [20]. Consequently, it also introduces new security and privacy challenges in IoT, including traditional Cloud threats and vulnerabilities and emerging security and privacy threats to IoT sensors, devices, and applications. Within a CE-IoT architecture, edge computing services and capabilities are being explored which generates an interesting research direction in the context of IoT security and privacy.

The developments of IoT has been maintained based on underlying IoT architectures. A basic IoT architecture comprises three layers: *i) Object or perception layer*, comprising devices and physical objects, *ii) One or more Middleware layer(s)*, that include virtual objects (digital counterpart of physical objects) [36], and Service-Oriented Architecture (SOA) management services, and *iii) An Application layer*, which is at the top of the architecture where users and administrators can directly interact with IoT applications. Many different layered IoT architectures have been proposed in

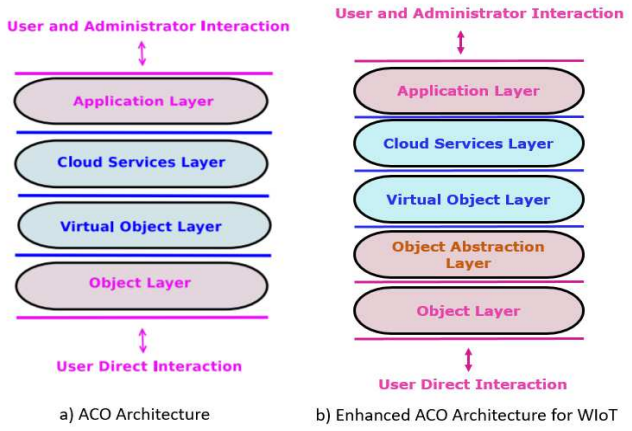

Figure 1: Access Control Oriented (ACO) [13] and Enhanced ACO [20] CE-IoT Architectures

the literature [12, 15, 39, 49]. In particular, an access control oriented (ACO) architecture for Cloud-Enabled IoT is proposed in [13]. The ACO architecture has four layers: *an object layer, virtual object layer, cloud services layer,* and *applications layer*. Each of these layers encapsulates different entities, associated data, and their access control requirements in the CE-IoT framework. To abstract the heterogeneity of IoT devices, and enable edge computing capabilities, particularly in domains like Wearable IoT (WIoT), we extended the ACO architecture and proposed an Enhanced ACO architecture (EACO) in [20]. Figure 1 shows the two layered CE-IoT architectures. In this paper, we focus on access and communications between various entities in the EACO architecture.

2.2 Related Work

Most access control models for IoT have been developed based on few popular models in the industry, such as Role-based Access Control (RBAC) and Capability-Based Access Control (CapBAC) [33]. A more flexible access control model that has recently gained attention in academia is Attribute-Based Access Control (ABAC) [29, 30] where permissions are determined based on attributes (properties) of users (or subjects) and objects. Despite the development of numerous access control models, there is no consensus on a standard formal access control model for Cloud-Enabled IoT due to its evolving characteristics. Cloud-Enabled IoT platforms are rapidly being developed and deployed by major CSPs. However, these platforms have a heterogeneous set of capabilities for their IoT architectures, including different communication protocols, e.g., MQTT [10], CoAP [4], and HTTP, and different authentication and authorization mechanisms. Similarly, there are many IoT manufacturers and vendors, which also results in heterogeneity in devices' characteristics, and networking and communication protocols. This diverse and a rapidly growing number of industry players in the IoT space makes it even more difficult to develop a standard access control and communication control framework for CE-IoT.

There are various IoT access control models developed to address access and authorization in single cloud enabled IoT architectures [13, 14, 20, 21, 25, 47, 48, 50]. Ouaddah et al. in [37] present a comprehensive review of IoT access control models. In Ye et al. [50], the authors proposed an efficient authentication and access control scheme for IoT where they employed an ABAC-based authorization method as access control policy with an efficient mutual authentication mechanism based on secure key establishment using ECC (Elliptic Curve Cryptosystem). Currently, in CE-IoT, major Cloud service providers utilize a cryptographic authentication mechanism to secure IoT devices. Some CE-IoT platforms, such as AWS IoT [3] and Google IoT Core [7], have started to explore ABAC capabilities. However, an ABAC authorization mechanism for authorizing users and devices based on their attributes is yet to be adopted and implemented in real-world Cloud-based IoT platforms.

Besides, with large amount of IoT data, communication control to secure data flow in IoT is a critical aspect of ensuring security and privacy in IoT. With billions of connected devices, there is a huge amount of data continuously being generated, collected, shared/transmitted, and analyzed in IoT components [17]. This IoT data can be categorized into two general categories: *i) static data or data at rest*, and *ii) dynamic data or data in motion*. Currently, access control mechanisms are being applied to secure the static data where the data is considered as an object in the system. In CE-IoT, IoT devices, gateways, Virtual objects, and multiple Clouds are continuously communicating and sharing data with each other. It is critical to address security and privacy concerns associated with communication and data flow by developing secure and flexible communication control models. However, a communication control model in the context of IoT is currently lacking.

While access control models secure access to objects by authorized subjects, communication control models are essential to secure communication and data flow from one component to the other and to enable user-defined privacy policies in CE-IoT architecture. Unlike extensive literature on access control models, there is very limited research on communication control models. However, researchers have developed access control models to secure access to the data in databases [26, 40] based on role-based approach with some special attribute.

Generally, communication control has been widely studied in the networking domain. In networks, there are distinct devices and systems, such as routers and firewalls, which control communication occurring in the form of packets based on some predefined rules and algorithms. A more specific example of a communication control device or system in information security is a **Guard** device. *Guards* control communication from one component to the other in a network [16]. In Section 4, we develop and present a conceptual model of Attribute-Based Communication Control (ABCC) and discuss its design and components. This is a first general conceptual model of ABCC to the best of our knowledge. Similarly, formal communication control models based on attributes of IoT entities can be designed and developed to secure communications among various authorized entities in the CE-IoT architecture.

2.3 Scope and Assumptions

In this research, we mainly focus on current and emerging access control and communication control requirements in CE-IoT. Unlike access control, communication control is a novel concept which need to be explored in detail for IoT devices and applications, especially when these devices and applications are continuously gathering and transmitting sensitive user data between different

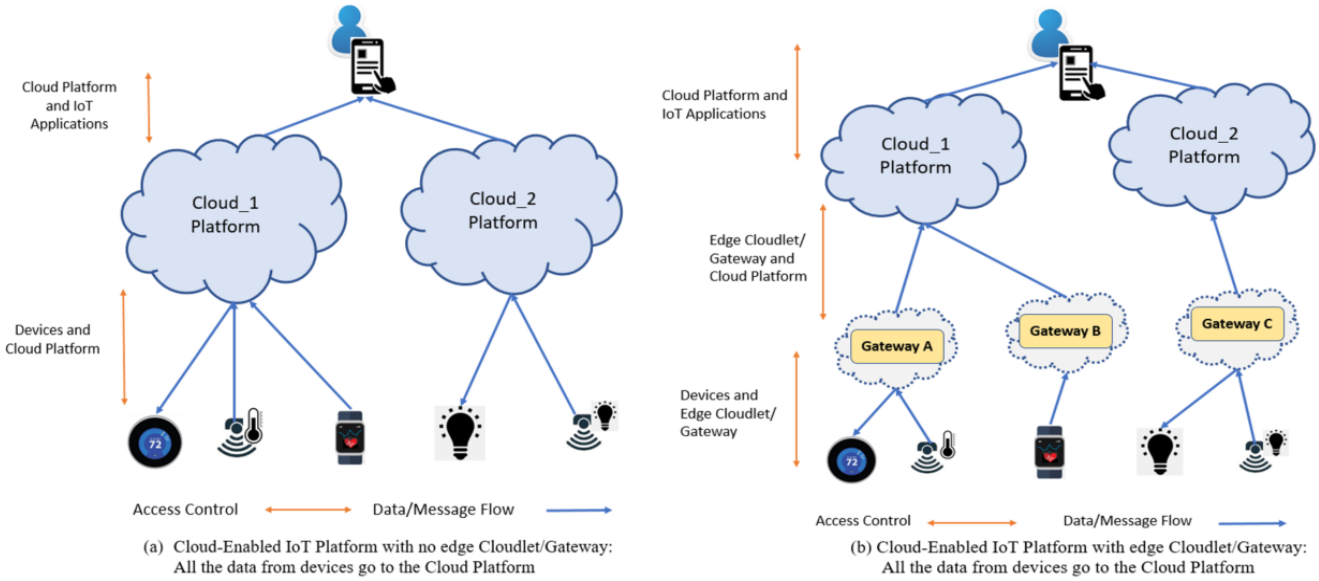

Figure 2: CE-IoT Architectures - Access and Communication Control shown in Cloud with and without Edge Cloudlets

entities in a CE-IoT architecture. Besides, as shown in Figure 1, we assume the **Device-to-Device** communication will occur through the *Object Abstraction layer*, i.e., encapsulating the edge gateways. In some IoT domains, such as Vehicular IoT and Internet of Battlefield or Military Things (IoMT/IoBT), device-to-device communication is critical and would be enabled by edge or fog computing. Here, we assume authentication on physical devices is enabled through cryptographic keys and certificates. Hence, discussions associated with device-to-device communications at the object layer are outside the scope of this paper.

3 Access Control and Communication Control Requirements in IoT

In order to develop an access control and communication control framework for CE-IoT, we first need to identify access control and communication control requirements in CE-IoT by analyzing existing limitations, differences, and gaps in the CE-IoT architecture. In this section, we discuss some relevant issues within the IoT ecosystem and analyze current and future access control and communication control requirements for CE-IoT.

Today, most popular CE-IoT architecture is a single Cloud-IoT architecture where IoT devices connect and communicate with a Cloud platform. However, to support communication between billions of IoT devices and provide local computation, analytics, and storage at the edge of the network, we envision a CE-IoT architecture with edge computing capabilities enabled through small edge cloudlets [43]. One mechanism to implement cloudlets is through gateways which have sufficient capabilities, such as storage and computation power, to act as a small cloud on the edge. However, influenced by different instances of the Cloud-IoT architecture, the access control and communication control requirements will evolve accordingly based on the architecture being used for IoT devices and applications.

As discussed earlier, there is no unified CE-IoT architecture for IoT yet. Based on different scenarios users can adapt different instances of the CE-IoT architecture. It is partly due to the current marketing strategy of CSPs to develop and deploy their IoT devices, for example numerous Smart Home Assistants, which are compatible and can communicate only with the Cloud platform that developed it. Therefore, with billions of IoT devices, these single centralized Cloud-IoT architecture creates an **interoperability** issue, which is already being realized by the users who own multiple smart devices from different manufacturers or vendors. Therefore, single cloud-IoT architecture will soon evolve with real-time communications and collaboration across several Cloud platforms [46]. With inter-Cloud collaboration being inevitable in the future, we need dynamic and flexible access control and communication control mechanisms to enable collaborations and trust across single-cloud and multi-cloud environments.

Figure 2 shows two different instances of the Cloud-Enabled IoT architecture. Figure 2 (a) shows a Cloud-IoT architecture without edge computing consistent with the ACO architecture shown in Figure 1 (a). Figure 2 (b) shows a Cloud-IoT architecture with edge cloudlets which enable edge computation, communication, and storage consistent with the ACO architecture shown in Figure 1 (b). The CE-IoT architecture in Figure 2 (b) is more suitable to support local computation and analysis towards the edge by utilizing AI and ML techniques and support real-time communications with fast response even in intermittent network once the gateway (cloudlet) and devices are authenticated and configured through the Cloud. Now, in both architectures, the access control and communication control requirements will vary based on different entities involved and user privacy concerns. For example, in Figure 2 (a), IoT devices connect to the Cloud and send all the data to the Cloud. Here the devices access and communicate with the virtual objects (VOs) hosted in the Cloud platform and the VOs can be access by IoT

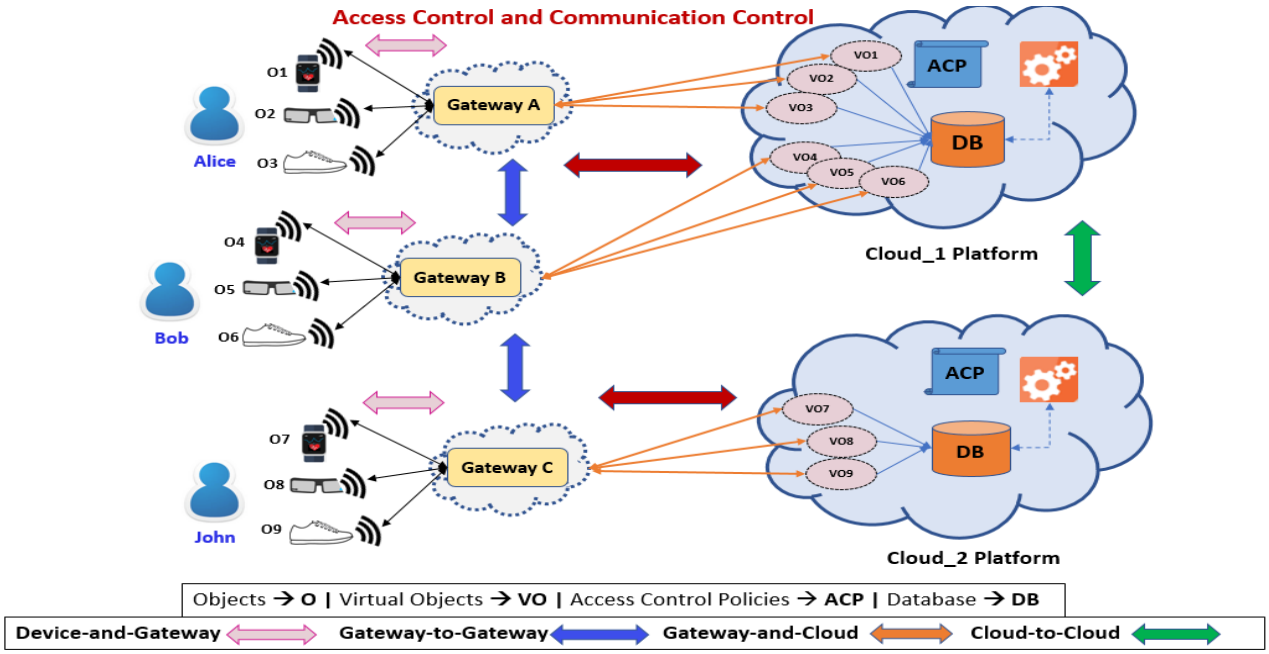

Figure 3: Access Control and Communication Control Requirements in CE-IoT

applications and other services to get and send or update data to physical devices.

However, in Figure 2 (b), the devices connect and communicate with the edge gateway/cloudlet which provide edge computation and enables access control and communication control towards the edge of the network. The gateway enabled communication with the VOs in the cloud and makes sure that physical devices can communicate with respective VOs in the Cloud platform. Moreover, the edge cloudlets enables users to define privacy preserving communication control policies. For example, users with higher privacy concerns do not want all their data to move to the Cloud platform at all times and would rather prefer that their data remains within the edge network, possibly stored in the edge cloudlet (gateway) unless some emergency or extraordinary condition occurs.

Figure 3 shows a holistic view of CE-IoT with different users, devices, gateways in cloudlets, and virtual objects in the Cloud platform along with other services. This figure is a more specific version of the Figure 2 (b) which shows various access control and communication control requirements in the CE-IoT architecture. Here, it depicts a Smart Health scenario, where users have multiple wearable IoT devices that connect to some gateways and the gateways are connected to the Cloud. In this scenario, there are various accesses and authorizations involved between devices, gateways, and virtual objects. Many Cloud-Enabled IoT platforms, such as AWS IoT and Google IoT Core manage access control and authorization through some customized form of RBAC models in an Identity and Access Management (IAM) service in the Cloud shown as ACP (access control policies). However, they have realized the limitations of RBAC and have already started looking into ABAC, but not yet fully implemented it successfully. At the same time, how would you control the flow of data from one end to the other, such as device to gateway, or gateway to VO in the Cloud platform, and even across gateways and across multiple Cloud platforms. The possible accesses and communications are shown through various colors in Figure 3 as **Device-and-Gateway** (access and communication from device to gateway and gateway to device), **Gateway-to-Gateway** (access and communication between gateway and gateway), **Gateway-and-Cloud** (access and communication from gateway to VO in the Cloud platform and from VO in the Cloud platform to gateway), and **Cloud-to-Cloud** (access and communication between VOs in different Cloud platforms).

3.1 Use Case Scenario

With the in figure, some use case scenarios are discussed below.

- **Scenario 1:** In the smart health monitoring example in Figure 3, the users do not want their data to be shared with the Cloud at all times and rather confine the data at the edge network and only send important updates to the Cloud platform based on some predefined conditions.
- **Scenario 2:** Similarly, users want to restrict messages (e.g., recommendations for health, exercise, etc. which are less critical in nature) coming from Cloud to users through IoT applications.

Within these scenarios, there are several questions that need to be answered. For example, *How would a user be able to control communications in these scenarios? What is a secure and flexible way to do so? How would they define access control policies together with communication control policies?* These are some of the specific questions that require further research and can be facilitated through the ABAC-AC framework. The ultimate goal is to enable the users to have the flexibility to define fine-grained access control and communication control policies for their smart devices. A promising

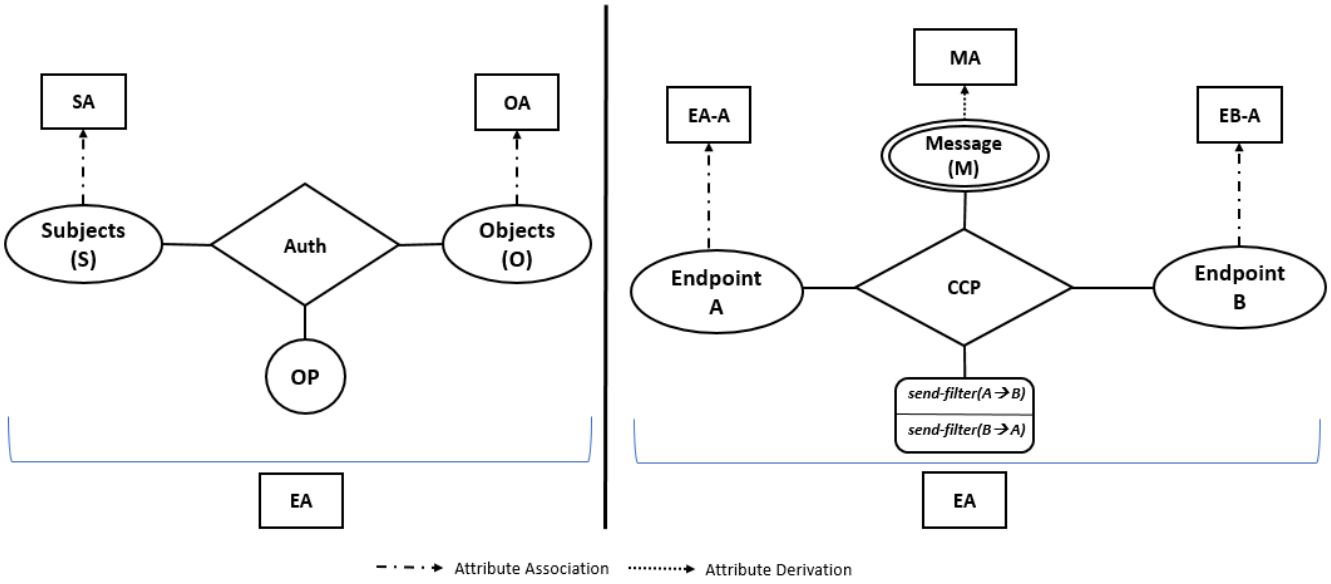

Figure 4: Attribute-Based Access Control (ABAC) vs. Attribute-Based Communication Control (ABCC)

approach is to utilize the **attribute-based** approach for access and communication control within the ABAC-CC framework.

4 Attribute-Based Communication Control

In this section, we propose a general conceptual Attribute-Based Communication Control (ABCC) and compare the structure of Attribute-Based Access Control (ABAC) and Attribute-Based Communication Control (ABCC) models. In general, access control refers to controlling access (e.g., read, write) to a protected entity (e.g., an object, or a subject) from another entity (e.g., a user or a subject) requesting that access on it. Whereas, in communication control, the communication of a specific element (e.g., message) is being controlled from one entity (or endpoint) to another. The specific entities, elements and their characteristics in the models depend on the system or domain they are designed for and are more concretely designed during the model implementation.

4.1 Attribute-Based Access Control (ABAC)

There have been many ABAC models proposed for various domains in the literature [18, 19, 23, 32, 44, 45, 51]. ABAC models have also been applied in administrative context for controlling administrators accesses, such as CRUD (create, delete, update, revoke) operations on model entities – users, objects, subjects, roles, and virtual objects [14, 28, 34, 35]. Figure 4(a) presents a simplified structure of a conceptual ABAC model. In simplest form of ABAC model, there are subjects (S), objects(O), subject attributes (SA), objects attributes (OA) and operations (OP). A subject is a user or a process, and an object is a resource (e.g., printer, file) or data stored in a system. An operation is an access right (e.g., read, write, credit, debit) to be performed on the object. The subject attributes represent the characteristics of the subject, for example, for a user the attributes could be the name, age, title, etc. Similarly, the object attributes represent the characteristics of the objects, such as owner, type, sensitivity level, etc.

Besides subject and object attributes, there are contextual attributes, also known as environment attributes (EA), such as time of day, location and so on, which can be employed to define more fine-grained authorization policies. An example of an attribute-based authorization policy is – *a user with title as manager can read an object with sensitivity level as high when the time of the day is between 9:00 am to 5:00 pm and location is office.* ABAC policies can be specified in two ways: *logical formulas with predicate logic* and *enumerations policy* [22]. An authorization function – $Auth\_func = (s, o, r)$ which identifies the authorization of a subject s on an object o to perform some right (or operation) r, is evaluated based on the attributes of subject s and object o and specified authorization policies. If a policy is satisfied based on the attributes of subject and object to perform the right r, then access is granted, otherwise denied.

4.2 A Conceptual Model of Attribute-Based Communication Control (ABCC)

In ABAC models, attributes of different entities are used to determine allowed accesses on protected resources and data from authorized entities. However, in Attribute-Based Communication Control (ABCC) models, both the attributes of entities communicating with each other and the attributes of the communication unit are taken into consideration while determining if the communication should be allowed or denied. Some of the prior work has identified the need to control data and communication in IoT and also developed models to control VO to VO communications

[13, 14]. However, a general conceptual model for attribute-based communication control is still lacking.

Here, we propose a conceptual model for attribute-based communication control as shown in Figure 4 (b). ABCC has unique characteristics compared to ABAC. There are two endpoints **EndpointA** and **EndpointB**, and a **Message** is being communicated between these two endpoints. The endpoints could be devices as routers (stateless/stateful or internal/external routers), systems, or even IoT devices. *EndpointA* and *EndpointB* have attributes which represent the properties of these endpoints, such as *type, owner,* etc. The attributes of *EndpointA* and *EndpointB* are represented as **EA-A** and **EB-A** respectively. The *message* is a unique new element which is created and is in existence when an endpoint generates it, sends it, and receives it during the communication and data flow process. It is a structured message (e.g., JSON, XML) that comprises a set of properties. Thus, the message attributes and their values are derived from these properties within a message rather than being assigned by an administrator. **MA** represents the *message* attributes. The properties in the message content, which are in the form of key and value(s), can be derived as the message attributes. For example, if the message has a property as *temp = 80* where temp is the *key* and 80 is the *value*, then it can be derived as a message attribute *temp* with value *80.*

In ABCC, there is only one operation **send-filter**. The send-filter operation is a directional one-way operation from a sender to a receiver, so we have two instances to capture two-way communications. For example, from an IoT device (sender) to the Cloud (receiver), and from Cloud (sender) to devices (receiver). The two instances are distinguished due to different communication control and information flow requirements in the two directions. The *send-filter*($A \rightarrow B$) represents a *send-filter* operation where the sender of a message is *EndpointA* and receiver is *EndpointB.* Similarly, *send-filter*($B \rightarrow A$) represents the communication from *EndpointB* to *EndpointA*, where *EndpointB* is the sender and *EndpointA* is the receiver.

The send-filter function is defined with 2 inputs, a *sender* and a *receiver.* Evaluation of this function also requires an attribute-based communication control policy. This policy is specified in terms of attributes of the sender, receiver, messages, and environment and is evaluated in the communication control policy function (CCP in Figure 4 (b)). The evaluation results in the message being blocked, forwarded as is or forwarded with some portions removed or sanitized. Assume there is an "ownerâĂİ attribute for endpointA and endpointB, thus, examples of communication control policies areas follows.

- *If the owner attribute values for a gateway (endpoint A) and owner attribute values for a virtual wearable IoT device (endpoint B) in Cloud are same, and the temperature value (a message attribute) is greater than 102 degrees Fahrenheit, then send the unfiltered (original) message from A to B.*
- *If the temperature value is in normal range, then either send a filtered message removing some sensitive information such as location of the user, or even do not send the message and store it at the gateway (endpoint A) since it is not a critical scenario.*

In order to secure communication and data flow, a set of communication control policies are defined by a user or an administrator based on the attributes of endpoints and messages in a system. For a specific sender, receiver (target), and a message, the **Communication Control Policy (CCP)** function is evaluated to identify if the message should be sent unfiltered (original message), filtered (removing sensitive information), or should not be sent from a sender to a receiver. As per the direction of communication and data flow, either of the endpoints can act as a sender or a receiver of a message. Similar to ABAC, **Environment attributes (EA)** can also be included in *CCP* to enable more fine-grained and dynamic communication control based on respective context (e.g., time of day, location). A simple communication control policy is given as: *"if the owner of endpoint A and endpoint B is the same, then allow the message to be sent from A to B, otherwise deny."* The CCP function is defined and co-located with one of the two endpoints, or in some cases be hosted in a separate system between two endpoints. In CE-IoT architecture, the data and information is continuously flowing between several components. For instance, in a wearable IoT scenario, IoT messages are communicated between wearable devices, gateways, virtual objects (VOs), cloud services, and applications. Therefore, the endpoints, the messages, and the direction of communication and data flow will change as per the type of communication architecture under consideration.

While there have been many ABAC models proposed in the literature, this is a first general conceptual ABCC model presented for controlling communication between two endpoints based on their attributes as well as message attributes, to the best of our knowledge. This model is abstract in nature and can be shaped into concrete entities and components based on the communication paradigm being used in real scenario. Some of the prevalent communication models are **publish/subscribe model** for IoT devices, and widely adopted **TCP/IP communication model,** for Internet communications, etc.

4.3 ABAC vs. ABCC

Both the ABAC and ABCC models utilize attributes of various entities in the system, however, the units being controlled are distinctly different. Additionally, the uniqueness of ABCC lies in its use of the attributes of the communication unit together with attributes of other entities in the communication control policies. Another major difference is that ABAC protects data and information stored in the system which is static, whereas ABCC secures data and information in motion, such as communications and data flowing from one entity to the other. ABCC model is also distinct compared to ABAC since it is responsible for addressing two major security concerns. First, it identifies if two endpoints should be allowed to communicate with each other utilizing their attributes. Second, it controls the flow of data and information from one endpoint to another endpoint while considering the content of data and information. This is critical especially to preserve user privacy and data security while data is in motion.

Moreover, in ABCC, the endpoints are system entities rather than individuals and represent machines in active states. A user's identity is embedded in the attributes of the endpoints and the message being communicated between these endpoints. While ABCC and its capabilities are pertinent to many domains, this paper focuses on ABCC models in realm of the CE-IoT architecture.

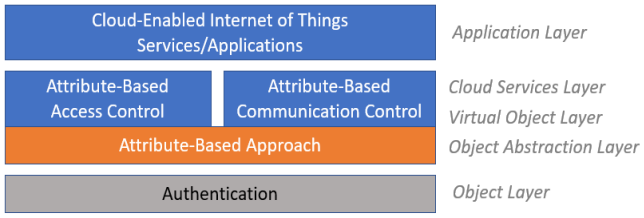

Figure 5: Attribute-Based Access and Communication Control Framework in EACO Layers

5 Attribute-Based Access and Communication Control Framework

In a CE-IoT architecture, there are various entities and components continuously interacting with each other, such as users, IoT things/devices, gateways, virtual objects, Cloud services, and applications. These interactions includes access and authorizations defined for several components and communications and data flow among these components. IoT has some unique characteristics compared to Cloud computing, especially due to the distributed and autonomous nature of IoT devices (e.g., sensors, actuators) and gateways deployed in the wild. Therefore, in order to rethink and reevaluate traditional access control models and mechanisms, currently being employed by CSPs for their Cloud services, we propose an Attribute-Based Access Control and Communication Control framework to adequately capture and address the evolving access control and communication control requirements in Cloud-Enabled IoT architecture.

5.1 ABAC-CC Framework

Figure 5 represents the attribute-based access control and communication control (ABAC-CC) framework across the Enhanced ACO layers. The ABAC-CC framework is based on the attribute-based approach which forms the foundation of the framework to control access to various entities and to control communication in terms of data flow from one end to another in CE-IoT services/applications.

The core components of ABAC-CC framework are described as follows.

- **Authentication**: Here, we assume the authentication for devices is enabled through cryptographic key coupling between physical devices and virtual objects, and is managed at the cloud platform level.
- **Attribute-Based Access Control and Authorization**: For proper access control decisions, there has to be secure ABAC models developed with a mechanism to define fine-grained access control and authorization policies. These models can be applied and implemented at the Cloud Level and enforced on entities at lower levels.
- **Attribute-Based Communication Control**: Attribute-Based communication control policies defined based on entities and message attributes which allows the users to define their desired privacy policies. Including the message attributes by inspecting the message content itself introduces a lot of flexibility and enhanced data security and privacy in controlling the flow of IoT data/messages from one components to the other in the CE-IoT architecture with edge computing capability. The ideal place to enforce communication control policies would change and can be adapted as required. For example, if the user want to control data flow from edge to Cloud, then they should deploy ABCC policies at the gateway/cloudlet level.
- **Cloud-Enabled IoT Services and Applications**: Utilizing the attribute-based approach, CE-IoT applications and services can enable fine-grained access and communications compare to their existing role-based and policy-based approaches.

ABAC-CC framework can be employed to control access and communication between different components, *Devices-and-Gateways*, *Gateways-to-Gateways*, *Gateways-and-Cloud(Virtual Objects)*, and *Cloud-to-Cloud*, as discussed in Section 3 in Figure 3. For *Devices-to-Devices*, currently we consider a cryptographic key coupling authentication and authorization on physical devices due to resource constrained nature of IoT devices. For now, we assume the device-to-device access and communication is enabled through the edge gateways. However, in the future with Vehicular IoT and IoBT/IoMT domains where devices become capable to support edge computation, we might need to expand the ABAC-CC framework to incorporate relevant Device-to-Device access and communication.

Figure 6 shows a Smart Health use case scenario where is a user has wearable devices continuously collecting data and monitoring the physiological parameters. It also shows a general mapping of the ABAC-CC framework and its application in context of the use case with attribute-based access and communication control policies. Here, the user wants to restrict her *location* and other data values, such as *temperature* and *heartrate* (if they are in normal range) to flow from the gateway to Cloud virtual object.

The first thing that will be checked here will be the attribute-based access control policy, if a device and gateway have the same value for an *owner* attribute, then only they will be able to access each other. Now, for communication control, the attribute-based communication control policy will be checked with message attribute values, such as if *heartrate*, *location*, and *temperature* are message attributes, then if we they are in the specified range of values, the data will be stored in gateway and will not flow from gateway to Cloud VO for the device. However, there need to be more research to be done to answers specific questions, such as *How the formal models and definitions will be devised for ABCC models?*, *How the ABAC and ABCC policies can be defined together in a single or distributed platform?*, etc. Moreover, there has to be a gradual shift from current RBAC models to the ***attribute-based*** ABAC-CC framework in current and future CE-IoT platforms enabled by relevant real-world use case scenarios and applications.

6 Future Research Directions

With the proposed ABAC-CC framework, we aim to enable secure and user-privacy enhanced access and communication control in CE-IoT. Furthermore, here we expand on additional research challenges and directions in different areas beyond the ABAC-CC framework to support the goal of enabling security and privacy enhanced CE-IoT and smart communities.

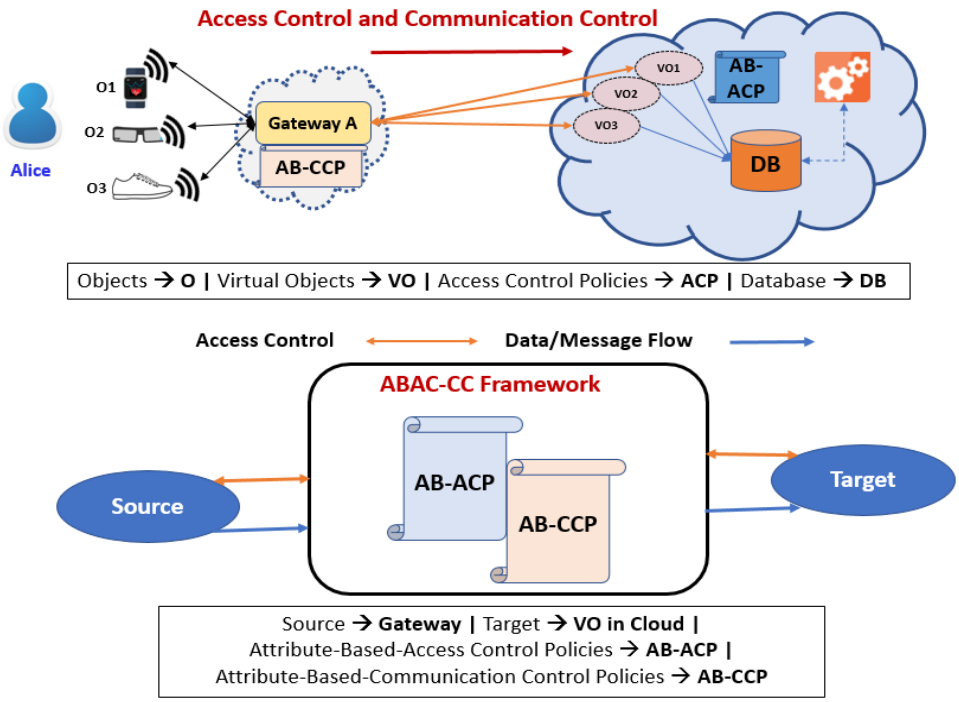

Figure 6: Access and Communication Control from Edge Cloudlet to Cloud Utilizing ABAC-CC Framework

- **Artificial Intelligence and Machine Learning:** With various intelligent and autonomous systems in the IoT context, AI and ML technologies can enable autonomous interactions, secure communication and information flow between smart entities and devices. Therefore, research on utilizing AI and ML techniques for efficient autonomicity and IoT security and privacy is a promising research direction.
- **Distributed Computing**: To enable secure smart whole communities in the future, research in areas of trusted distributed computing infrastructure and technologies is necessary. Some of the research areas are: Blockchain trust frameworks, distributed and dynamic access and communication control models, efficient and low-latency communication protocols and distributed Cloud and edge computing.
- **Collaborative IoT Models:** For a sustainable growth of IoT, collaboration among multiple Cloud platforms and cloudlets at the edge of the network is inevitable. Secure and trustworthy collaboration, possibly based on sharing of attributes of entities, can be utilized in developing trust relationships across several Cloud and IoT platforms for developing ubiquitous IoT network and connectivity.
- **Insider Threats and Rogue Devices:** With ABCC, we identified that the users will be able to define privacy preserving communication control policies. The other aspect that needs further exploration is offensive attackers perspective in IoT, such as an insider threats or unauthorized physical access gained to IoT devices for creating IoT-Bot devices. Further research on attacks and defenses in these scenarios is in demand, currently and in the future.
- **Dynamic Edge and Fog Computing:** IoT devices and sensors at the edge of network and users, especially in domains such as Internet of Vehicles (IoV), Wearable IoT, and Internet of Battlefield Things (IoBT), are continuously mobile along with highly sensitive data in motion. Significant research on edge and fog computing technology is crucial for IoT frameworks, such as ABCC-CC to enable data security and communication in a distributed and dynamic environment for futuristic IoT.

7 Conclusion

In this paper, we introduced the Attribute-based Communication Control (ABCC) model and compared its structure with the basic ABAC model. We also proposed an **Attribute-Based** approach to secure access and communication in CE-IoT architecture with edge computing capabilities and discussed its utility in a Smart Health use case. We also presented future research directions and challenges. Overall, the main goal of this research is to reevaluate and rethink current access control mechanisms and design new models on top of the attribute-based approach to secure IoT access, communication, and data at rest and in motion. Furthermore, the objective here is to introduce and stimulate research on ABCC models for real-world IoT application domains, such as Smart Home, Smart Health, etc. In addition, real-world implementation and enforcement of ABAC is still a challenge. Therefore, real-world use cases implementation and enforcement employing ABAC together with ABCC models are necessary. In the future work, we plan to develop formal ABCC models for securing communication between various components in the context of CE-IoT.

Acknowledgments

This work is partially supported by NSF CREST Grant HRD-1736209 and the Texas A&M System Chancellor Research Initiative (CRI) Grant.

References

[1] Amazon Web Services (AWS) - Cloud Computing Services. https://aws.amazon.com. Accessed: 2020-01-08.
[2] Apple Smart Watch. https://www.apple.com/apple-watch-series-5/. Accessed: 2020-01-08.
[3] AWS Internet of Things. http://docs.aws.amazon.com/iot/latest/developerguide/what-is-aws-iot.htm. Accessed: 2020-01-10.
[4] Constrained Application Protocol. http://coap.technology note = Accessed: 2019-12-10..
[5] Fitbit. https://www.fitbit.com/us/home. Accessed: 2020-01-08.
[6] Google Cloud Platform. https://cloud.google.com/. Accessed: 2019-12-10.
[7] Google Internet of Things. https://cloud.google.com/solutions/iot-overview/. Accessed: 2019-12-10.
[8] Google Nest. https://nest.com/. Accessed: 2020-01-08.
[9] Here's How the Internet of Things (IoT) Will Change Workplaces. http://www.insight.com/enUS/learn/content/2017/02072017-heres-how-the-internet-of-things-iot-will-change-workplaces
[10] Message Queuing Telemetry Transport. http://mqtt.org/
[11] Microsoft Azure. https://azure.microsoft.com. Accessed: 2019-11-10.
[12] Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari, and Moussa Ayyash. 2015. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials* 17, 4 (2015), 2347–2376.
[13] Asma Alshehri and Ravi Sandhu. 2016. Access control models for cloud-enabled internet of things: A proposed architecture and research agenda. In *2nd International Conference on Collaboration and Internet Computing (CIC), 2016, IEEE*. IEEE, 530–538.
[14] Asma Alshehri and Ravi Sandhu. 2017. Access Control Models for Virtual Object Communication in Cloud-Enabled IoT. In *International Conference on Information Reuse and Integration (IRI), IEEE*. IEEE, 16–25.
[15] Luigi Atzori, Antonio Iera, and Giacomo Morabito. 2010. The Internet of Things: A Survey. *Computer Networks* 54, 15 (2010), 2787–2805.
[16] Smriti Bhatt. 2018. *Attribute-Based Access and Communication Control Models for Cloud and Cloud-Enabled Internet of Things*. Ph.D. Dissertation. University of Texas at San Antonio.
[17] Smriti Bhatt, A Tawalbeh Loái, Pankaj Chhetri, and Paras Bhatt. 2019. Authorizations in Cloud-Based Internet of Things: Current Trends and Use Cases. In *2019 Fourth International Conference on Fog and Mobile Edge Computing (FMEC)*. IEEE, 241–246.
[18] Smriti Bhatt, Farhan Patwa, and Ravi Sandhu. 2016. An Attribute-Based Access Control Extension for OpenStack and its Enforcement Utilizing the Policy Machine. In *IEEE 2nd International Conference on Collaboration and Internet Computing (CIC)*. IEEE, 37–45.
[19] Smriti Bhatt, Farhan Patwa, and Ravi Sandhu. 2017. ABAC with group attributes and attribute hierarchies utilizing the policy machine. In *Proceedings of the 2nd ACM Workshop on Attribute-Based Access Control*. ACM, 17–28.
[20] Smriti Bhatt, Farhan Patwa, and Ravi Sandhu. 2017. An Access Control Framework for Cloud-Enabled Wearable Internet of Things. In *3rd International Conference on Collaboration and Internet Computing (CIC), IEEE*.
[21] Smriti Bhatt, Farhan Patwa, and Ravi Sandhu. 2017. Access Control Model for AWS Internet of Things. In *International Conference on Network and System Security*. Springer, 721–736.
[22] Prosunjit Biswas, Ravi Sandhu, and Ram Krishnan. 2016. A Comparison of Logical-formula and Enumerated Authorization Policy ABAC Models. In *IFIP Annual Conference on Data and Applications Security and Privacy*. Springer, 122–129.
[23] Prosunjit Biswas, Ravi Sandhu, and Ram Krishnan. 2016. Label-based access control: An ABAC model with enumerated authorization policy. In *Proceedings of the 2016 ACM International Workshop on Attribute Based Access Control*. ACM, 1–12.
[24] Alessio Botta, Walter De Donato, Valerio Persico, and Antonio Pescapé. 2014. On the integration of cloud computing and internet of things. In *Future internet of things and cloud (FiCloud), 2014 international conference on*. IEEE, 23–30.
[25] Imane Bouij-Pasquier, Abdellah Ait Ouahman, Anas Abou El Kalam, and Mina Ouabiba de Montfort. 2015. SmartOrBAC security and privacy in the Internet of Things. In *2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA)*. IEEE, 1–8.
[26] Ji-Won Byun, Elisa Bertino, and Ninghui Li. 2005. Purpose based access control of complex data for privacy protection. In *Proceedings of the tenth ACM symposium on Access control models and technologies*. 102–110.
[27] David F Ferraiolo, Ravi Sandhu, Serban Gavrila, D Richard Kuhn, and Ramaswamy Chandramouli. 2001. Proposed NIST Standard for Role-Based Access Control. *ACM Transactions on Information and System Security (TISSEC)* 4, 3 (2001), 224–274.
[28] Maanak Gupta and Ravi Sandhu. 2016. The \mathrm {GURA_G} GURAG Administrative Model for User and Group Attribute Assignment. In *International Conference on Network and System Security*. Springer, 318–332.
[29] Vincent C Hu, David Ferraiolo, Rick Kuhn, Adam Schnitzer, Kenneth Sandlin, Robert Miller, and Karen Scarfone. 2014. Guide to attribute based access control (ABAC) definition and considerations. *NIST Special Publication 800-162* (2014).
[30] Xin Jin, Ram Krishnan, and Ravi Sandhu. 2012. A unified attribute-based access control model covering DAC, MAC and RBAC. In *IFIP Annual Conference on Data and Applications Security and Privacy*. Springer, 41–55.
[31] Rafiullah Khan, Sarmad Ullah Khan, Rifaqat Zaheer, and Shahid Khan. 2012. Future internet: the internet of things architecture, possible applications and key challenges. In *Frontiers of Information Technology (FIT), 2012 10th International Conference on*. IEEE, 257–260.
[32] Bo Lang, Ian Foster, Frank Siebenlist, Rachana Ananthakrishnan, and Tim Freeman. 2009. A flexible attribute based access control method for grid computing. *Journal of Grid Computing* 7, 2 (2009), 169–180.
[33] Parikshit N Mahalle, Bayu Anggorojati, Neeli Rashmi Prasad, and Ramjee Prasad. 2012. Identity Establishment and Capability Based Access Control (IECAC) Scheme for Internet of Things. In *15th Symposium on Wireless Personal Multimedia Communications (WPMC)*. IEEE, 187–191.
[34] Jiwan Ninglekhu and Ram Krishnan. 2017. AARBAC: Attribute-based administration of role-based access control. In *Collaboration and Internet Computing (CIC), 2017 IEEE 3rd International Conference on*. IEEE, 126–135.
[35] Jiwan Ninglekhu and Ram Krishnan. 2017. Attribute based administration of role based access control: A detail description. *arXiv preprint arXiv:1706.03171* (2017).
[36] Michele Nitti, Virginia Pilloni, Giuseppe Colistra, and Luigi Atzori. 2016. The virtual object as a major element of the internet of things: a survey. *IEEE Communications Surveys & Tutorials* 18, 2 (2016), 1228–1240.
[37] Aafaf Ouaddah, Hajar Mousannif, Anas Abou Elkalam, and Abdellah Ait Ouahman. 2017. Access Control in The Internet of Things: Big Challenges and New Opportunities. *Computer Networks* 112 (2017), 237–262.
[38] Pritee Parwekar. 2011. From internet of things towards cloud of things. In *Computer and Communication Technology (ICCCT), 2011 2nd International Conference on*. IEEE, 329–333.
[39] Pawani Porambage, Mika Ylianttila, Corinna Schmitt, Pardeep Kumar, Andrei Gurtov, and Athanasios V Vasilakos. 2016. The quest for privacy in the internet of things. *IEEE Cloud Computing* 3, 2 (2016), 36–45.
[40] Fausto Rabitti, Elisa Bertino, Won Kim, and Darrell Woelk. 1991. A model of authorization for next-generation database systems. *ACM Transactions on Database Systems (TODS)* 16, 1 (1991), 88–131.
[41] BB Prahlada Rao, Paval Saluia, Neetu Sharma, Ankit Mittal, and Shivay Veer Sharma. 2012. Cloud computing for Internet of Things & sensing based applications. In *Sensing Technology (ICST), 2012 Sixth International Conference on*. IEEE, 374–380.
[42] Ravi Sandhu, Edward J Coyne, Hal Feinstein, and Charles Youman. 1996. Role-Based Access Control Models. *IEEE Computer* 29, 2 (1996), 38–47.
[43] Mahadev Satyanarayanan, Paramvir Bahl, Ramón Caceres, and Nigel Davies. 2009. The Case for VM-Based Cloudlets in Mobile Computing. *IEEE pervasive Computing* 8, 4 (2009).
[44] Daniel Servos and Sylvia L Osborn. 2014. HGABAC: Towards a formal model of hierarchical attribute-based access control. In *International Symposium on Foundations and Practice of Security*. Springer, 187–204.
[45] Hai-bo Shen and Fan Hong. 2006. An attribute-based access control model for web services. In *2006 Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT06)*. IEEE, 74–79.
[46] Bo Tang, Hongjuan Kang, Jingwen Fan, Qi Li, and Ravi Sandhu. 2019. Iot passport: a blockchain-based trust framework for collaborative internet-of-things. In *Proceedings of the 24th ACM Symposium on Access Control Models and Technologies*. 83–92.
[47] Yuan Tian, Nan Zhang, Yueh-Hsun Lin, XiaoFeng Wang, Blase Ur, Xianzheng Guo, and Patrick Tague. 2017. Smartauth: User-centered authorization for the internet of things. In *26th {USENIX} Security Symposium ({USENIX} Security 17)*. 361–378.
[48] Ronghua Xu, Yu Chen, Erik Blasch, and Genshe Chen. 2018. Blendcac: A smart contract enabled decentralized capability-based access control mechanism for the iot. *Computers* 7, 3 (2018), 39.
[49] Zhihong Yang, Yingzhao Yue, Yu Yang, Yufeng Peng, Xiaobo Wang, and Wenji Liu. 2011. Study and application on the architecture and key technologies for IOT. In *2011 International Conference on Multimedia Technology*. IEEE, 747–751.
[50] Ning Ye, Yan Zhu, Ru-chuan Wang, Reza Malekian, and Qiao-min Lin. 2014. An efficient authentication and access control scheme for perception layer of Internet of Things. (2014).
[51] Eric Yuan and Jin Tong. 2005. Attributed based access control (ABAC) for web services. In *IEEE International Conference on Web Services (ICWS05)*. IEEE.