2017 IEEE 3rd International Conference on Collaboration and Internet Computing

An Access Control Framework for Cloud-Enabled Wearable Internet of Things

Smriti Bhatt, Farhan Patwa and Ravi Sandhu
Institute for Cyber Security (ICS),
Center for Security and Privacy Enhanced Cloud Computing (C-SPECC), and
Department of Computer Science, University of Texas at San Antonio, San Antonio, Texas, USA
bhattsmriti1@gmail.com, farhan.patwa@utsa.edu and ravi.sandhu@utsa.edu

***Abstract*—Internet of Things (IoT) has become a pervasive and diverse concept in recent years. IoT applications and services have given rise to a number of sub-fields in the IoT space. Wearable technology, with its particular set of characteristics and application domains, has formed a rapidly growing sub-field of IoT, viz., Wearable Internet of Things (WIoT). While numerous wearable devices are available in the market today, security and privacy are key factors for wide adoption of WIoT. Wearable devices are resource constrained by nature with limited storage, power, and computation. A Cloud-Enabled IoT (CEIoT) architecture, a dominant paradigm currently shaping the industry and suggested by many researchers, needs to be adopted for WIoT. In this paper, we develop an access control framework for cloud-enabled WIoT (CEWIoT) based on the Access Control Oriented (ACO) architecture recently developed for CEIoT in general. We first enhance the ACO architecture from the perspective of WIoT by adding an Object Abstraction Layer, and then develop our framework based on interactions between different layers of this enhanced ACO architecture. We present a general classification and taxonomy of IoT devices, along with brief introduction to various application domains of IoT and WIoT. We then present a remote health and fitness monitoring use case to illustrate different access control aspects of our framework and outline its possible enforcement in a commercial CEIoT platform, viz., AWS IoT. Finally, we discuss the objectives of our access control framework and relevant open problems.**

***Keywords*-Internet of Things; IoT Devices; Wearable Devices; WIoT; Cloud-Enabled; Access Control;**

I. Introduction

Internet of Things (IoT) has given rise to a new wave of technology innovation. IoT is a very broad term in today's context which includes various enabling technologies: machine-to-machine (M2M) technologies, Internet, networking, communication protocols, cloud and mobile computing, and big data analytics [1]. A recent IoT architecture shaping the industry today is the combination of Cloud and IoT, with major cloud services providers offering IoT services and applications on top of their existing cloud services [2]. The integration of Cloud and IoT has also been suggested and studied in the academic literature [3]–[5]. Some of the common terms used for this architecture are: *cloud-based IoT, cloud-assisted IoT* or *cloud-enabled IoT* [6]. Here, we adopt the term Cloud-Enabled IoT (CEIoT).

The CEIoT architecture has gained much popularity in industry and academia. Most of the work is focused on either specific applications and technologies of IoT, or state-of-art surveys. Here, we focus on access control aspects, mainly authorization, of the CEIoT architecture. Securing the cloud-enabled IoT architecture involves security in two vast arenas—*Cloud* and *IoT*. A proper characterization of access control in the CEIoT architecture is necessary for its wide adoption and continued success.

Many different layered IoT architectures has been proposed in the literature [1], [7]–[10]. In particular, an access control oriented (ACO) architecture for cloud-enabled IoT is proposed in [6]. The ACO architecture has four layers: *object layer, virtual object layer, cloud services layer,* and *applications layer*. Each of these layers encapsulate different entities, associated data, and their access control requirements in the CEIoT framework.

Wearable Internet of Things (WIoT) is an emerging sub-field of IoT. Numerous wearable devices to track and gather data on vital aspects of human lives are available. Wireless Sensor Networks (WSNs) and Wireless Body Area Networks (WBANs) are few of the enabling technologies of WIoT together with Internet and smart phones. Despite various devices and applications being studied and developed for WIoT, an access control framework for WIoT is still missing.

In this paper, we present an access control (AC) framework for CEIoT in context of WIoT, that is Cloud-Enabled Wearable Internet of Things (CEWIoT), based on the enhanced ACO architecture with an additional layer, *Object Abstraction Layer*. Our framework addresses various authorization requirements of and between each layer and their associated data and components, and is divided into three categories of access control models: *Object, Virtual Object,* and *Cloud*. We also discuss the main access control models which are appropriate or specifically designed for the above categories. We then develop a Remote Health and Fitness Monitoring (RHFM) use case consistent with our framework and discuss its possible enforcement. The objectives and relevant research problems associated with our framework are also discussed.

The major contributions of this paper are outlined below.

- We present a general categorization of IoT devices that will allow researchers to realize different sub-fields of IoT and approach relevant security issues in those fields.
- We enhance the ACO architecture for CEWIoT by adding an *Object Abstraction Layer* in order to clearly identify different types of objects (specifically, edge and gateway devices) in the architecture.

0-7695-6303-1/17/31.00 ©2017 IEEE
DOI 10.1109/CIC.2017.00050

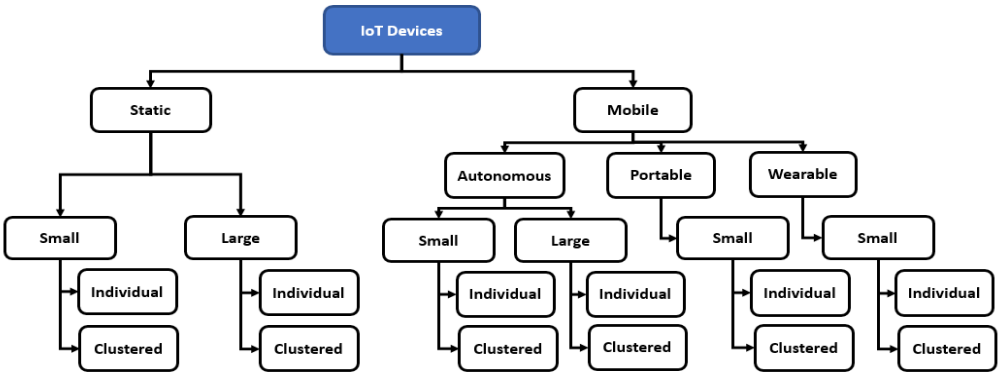

Figure 1: A General Classification of IoT Devices

- In context of this enhanced ACO architecture, we develop an access control framework with a set of models dealing with access and authorization requirements in and between layers of the architecture.
- We develop a use case depicting interactions between ACO layers with respect to our access control framework and discuss its possible enforcement in a commercial CEIoT platform, viz., AWS IoT [11].

The rest of the paper is organized as follows. We briefly discuss IoT devices and domains, and the ACO architecture in Section II. In Section III, we discuss WIoT devices and application domains, and present an enhanced ACO architecture for WIoT. We present our access control framework for CEWIoT in Section IV. Section V includes the details of our use case, and Section VI discusses the objectives and research problems associated with our framework. Finally, we conclude with future work in Section VII.

II. Background

In this section, we first present a classification of IoT devices based on three key characteristics, and discuss some IoT application domains. The classification and taxonomy of devices can be utilized to represent various IoT sub-fields. Second, we briefly review the Access Control Oriented (ACO) architecture developed for IoT.

A. IoT Devices

The impact of IoT is clearly visible in every aspect of human lives, such as smart homes, smart cities, offices, hospitals and businesses. With the disruptive trend of IoT, different types of smart devices are evolving in the market with "anything" and "everything" being connected to the Internet. This widening IoT paradigm and increasing number of connected things requires a proper categorization of IoT devices/things. This categorization provides a holistic view of different types of IoT devices in the market today, and can be extended as they evolve with time.

Figure 1 shows our classification and taxonomy of IoT things. In order to develop this classification, we consider three major characteristics: *mobility, size,* and *nature* of smart IoT things. They are defined as follows.

- **Mobility:** In IoT, the devices inherit the properties of their owners or of the entities to which they are attached. Mobility is one of the main characteristics that enables identifying the state of smart things and their capability of movement. We classify devices into two categories: **static** and **mobile**. Static things cannot move and are restricted to a specific location of installation, for example a smart surveillance camera on a building. Whereas, mobile things are capable of movement, and mobility can be achieved either independently *(e.g., autonomous cars)*, or dependently *(e.g., wearable smart watches)* through the device owners/carriers. Thus, they can be further classified into three categories: **autonomous** which are capable of moving independently, **portable** which can be carried around, and **wearable** which can be worn and attached to their owners.
- **Size:** IoT devices are of different sizes, from a small tiny sensor to big complex machinery. It is difficult to define definite metrics to categorize IoT things based on the size. However, for simplicity we consider two categories: **small** and **large**. For example, any device that can be easily carried by an individual is a small IoT device, such as small sensors or wearable devices. Thus, we consider only *small* category under *portable* and *wearable*.
- **Nature:** The third characteristic is the nature of things or devices. The nature of IoT devices depends on their architecture and functionality. Any thing that acts individually to perform a task is an **individual** IoT device, and a combination of multiple things that operates together to achieve a specific functionality is a **clustered** IoT device. As the name implies, individual things are made up of a single thing (e.g., a sensor sensing motion), and a clustered device is a combination of small sensors, such as wireless sensor networks (WSNs) or a smart car that has multiple sensors and actuators.

Other characteristics, such as technologies used, operating systems, network and communication protocols, can be considered for further enhancing our classification as required.

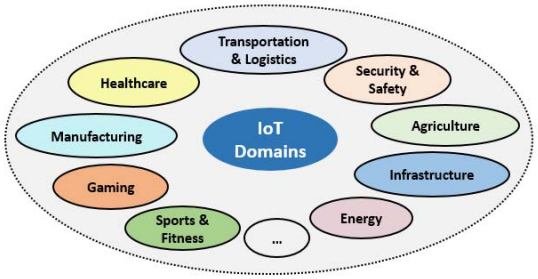

Figure 2: IoT Application Domains

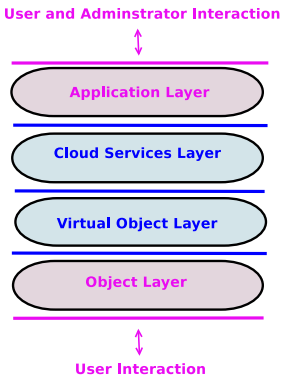

Figure 3: ACO Architecture for IoT [6]

There have been other efforts to classify IoT devices. In [12], IoT things are classified into three categories based on the technology areas—*i) attached devices* (e.g., RFID[1] tags and barcodes attached to things), *ii) sensing and actuating devices*, and *iii) embedded devices* that have embedded processors and storage. Another way of classifying IoT devices is based on communication capabilities resulting in two categories: *gateway devices* and *constrained devices*, where constrained devices are further classified into three classes: *Class 0, Class 1,* and *Class 2* based on their memory and processing capabilities [14]. In [15], the authors presented a classification of IoT devices for creating a security framework based on a comprehensive list of properties, such as power capability, real and non-real time, communication protocol, bandwidth and size. Most of these works focus on distinct technologies used while classifying IoT devices, and fall short in providing a general classification of IoT devices.

Based on various application domains, IoT has started to diverge into different IoT sub-fields, such as Vehicular IoT (VIoT), Medical IoT (MIoT), and Wearable IoT (WIoT). The objective of our IoT device categorization is to provide an overall general classification of heterogeneous IoT devices, and we believe that the above three characteristics are most suitable ones for this purpose. This categorization provides a basis to represent different IoT sub-fields, where distinct nodes in the tree can be combined to realize these sub-fields. For example, VIoT would be a combination of *autonomous, large,* and *clustered* IoT devices (sensors and actuators). Similarly, *wearable, small,* and *individual* or *clustered* device categorization can be realized as WIoT, as well as corresponds to MIoT to some extent. Therefore, this classification will enable IoT stakeholders, researchers, and businesses to focus on desired IoT sub-fields and associated security and privacy issues while developing innovative solutions.

B. IoT Application Domains

In recent years, numerous IoT services and applications are increasingly being deployed and explored practically in every domain, such as infrastructure, manufacturing, transportation, energy, as well as in critical domains like military and healthcare. In [7], four main IoT domains with a futuristic domain were presented along with their relevant scenarios. Since then IoT has influenced many other application domains as well, and is still expanding. Figure 2 presents some of the application domains being impacted by IoT today with possibility of many more to be added. Smart cities, smart homes, and utilities are specific IoT examples in the infrastructure domain. Smart cities with IoT have been extensively studied [16]–[19]. In transportation, RFID toll tags, smart traffic lights and traffic management with traffic flow data, parking with smart sensors, and mobile ticketing and travel are some IoT scenarios [7], [20]. Similarly, numerous IoT services and applications for health care have been proposed. A comprehensive survey by Islam et al. [21] discusses the state-of-art of IoT in health care, along with various medical IoT devices, services, applications, and use case scenarios.

Other domains like energy employ connected sensors for controlling and managing electricity usage, and other forms of energy, such as wind and solar for fulfilling the energy requirements of the planet efficiently. Meanwhile, retail and logistics are employing IoT for supply-chain management; moisture sensors are being used for watering plants and to improve crop yields; and IoT devices and sensors are utilized to improve efficiency and productivity in smart manufacturing [22]. Sports and fitness, security and safety, and gaming are some of the other emerging IoT domains, enabled by the wearable technology [23]. Besides these, the capabilities and benefits of IoT are being explored in many other domains, and soon enough will be realized in every aspect of our lives.

C. Access Control Oriented (ACO) Architecture for IoT

Many layered IoT architectures, with variations in different layers of the architecture, have been proposed in the literature [1], [3]–[5], [7], [20], [24]–[27]. A general IoT architecture comprises three basic layers: *an object layer, one or more middle layers,* and *an application layer* [1], [7]–[10]. Recently, an IoT architecture, consistent with above architectures, was proposed by Alshehri and Sandhu [6]. The motivation of their architecture is to integrate Cloud computing and its benefits in IoT, and incorporate the concept of virtual objects (VOs) [24]

[1]Radio Frequency Identification (RFID) allows automatic identification of things to which they are attached [13]

which are the digital representation of physical smart objects. The authors have designed a layered IoT architecture with a focus on aiding the development of access control models for CEIoT, and thus, named it as Access Control Oriented (ACO) architecture for CEIoT.

Figure 3 shows the ACO architecture for IoT. It has four layers: *object layer, virtual object layer, cloud services layer,* and *applications layer*. Besides these layers, the ACO architecture also includes two other entities—*users* and *administrators*. Users are individuals who directly or indirectly interact with the IoT framework and benefit from its capabilities, while administrators are responsible for managing IoT securely and efficiently. The four layers of the ACO architecture are described as follows [6].

1. **Object Layer:** This is the base layer of the ACO architecture where heterogenous IoT devices like sensors, actuators, embedded devices, etc. reside. Mostly these devices are constrained devices with limited power, memory, and storage. Users directly interact with this layer while using and controlling the physical objects. For example, user can manually turn off a device, such as a light or a pump. Different types of IoT devices discussed in our device categorization fit in this layer. These devices or objects mainly collect data and send it to other end points, such as other objects, virtual objects, gateways, and cloud for storage, computation and analysis. Object-to-object communication occurs within this layer and is achieved through various machine-to-machine (M2M) networking protocols and standards—Bluetooth, Zigbee, 6LoWPAN, ISA 100, WirelessHart/802.15.4, and LTE. Internet enables the communication and data exchange with other ACO layers through a set of protocols, such as HTTP, MQTT, and CoAP [1], [6].
2. **Virtual Object Layer:** In the ACO architecture, the authors promote the use of virtual objects (VOs), that is digital representation of physical IoT objects, and thus, introduce the virtual object layer to facilitate objects to applications interactions via VOs. VOs are capable of representing the current state of associated physical objects in the digital space when they are connected, and can also store a future state for those devices when they are offline. They provide a uniform interface for the physical objects to communicate with the upper ACO layers. In AWS IoT [11], virtual objects are used to represent real-world IoT devices in the cloud, and are known as *Thing Shadows* or *Device Shadows*. Other capability of this layer is to enable VO-to-VO communication, where the interaction is not restricted by the heterogeneous communication protocols utilized by their equivalent physical objects. The authors in [6] also discussed different types of VO to physical object association—*one(or less)-to-one, many-to-one, one-to-many,* and *many-to-many* associations [24].
3. **Cloud Services Layer:** This layer is the core of the CEIoT architecture. Many researchers have presented the Cloud as one of the most important enabling technologies for IoT [1], [3]–[5], [7], [27]. The cloud services layer particularly serves to host the storage, computation, and analysis services for the huge amount of data generated by billions of IoT devices. These resource constrained devices leverage the capabilities of the Cloud to perform desired functions. Users and business stakeholders can employ machine learning and data mining technologies to extract useful information from the IoT data that can be used in numerous ways to benefit customers. Besides this, cloud services layer is a suitable place to host an authentication and authorization service which manages secure communication and data access between IoT objects and applications. Different types of possible interactions, including communications and data access, in this layer are: *i) interactions between different cloud services inside one cloud (intra-cloud, cross-tenant, cross-account), ii) interactions between cloud services of different clouds (inter-clouds, multi-cloud),* and *iii) interactions between components of other layers (VO-to-Cloud, Cloud-to-Apps)*.
4. **Applications Layer:** This is the layer that delivers IoT services to end users through IoT applications and has been placed at the top of the ACO architecture. It acts as an interface for the users to remotely send commands and receive data and information from the objects. Users are also able to visualize the IoT data, which has been analyzed in the cloud services layer, through the applications. The applications also allow administrators and users to configure devices, and define access control polices for securing access to IoT resources and data.

Within each layer and among different layers of the ACO architecture, the access control requirements need to be addressed through appropriate access control models. Some of the suggested access control models in [6] for this purpose are role-based access control (RBAC) [28], [29], attribute-based access control (ABAC) [30], [31], and relationship-based access control (ReBAC) [32]. We will discuss about these models in context of our AC framework in Section IV.

III. Wearable Internet of Things (WIoT)

Wearable Internet of Things (WIoT) is a rapidly evolving sub-field of IoT which has some well-defined application domains. WIoT has already started to revolutionize the health care industry with numerous wearable devices and applications for monitoring vital body parameters, such as heart rate, pulse, temperature, blood pressure, blood sugar level, and other behavioral parameters [33]. Some of the examples of wearable devices, enabled by ubiquitous Internet and mobile technology, are smart watches (e.g., Apple watch), fitness and health tracking devices (e.g., Fitbit), wearable health monitoring sensors (e.g., smart glucometer), and wearable smart clothing and accessories (e.g., smart t-shirts, necklace, bands).

In the near future, WIoT will occupy one of largest market share among various IoT sub-fields. There has been significant research on wearable IoT devices and applications, mostly focusing on health care use cases. These studies are more

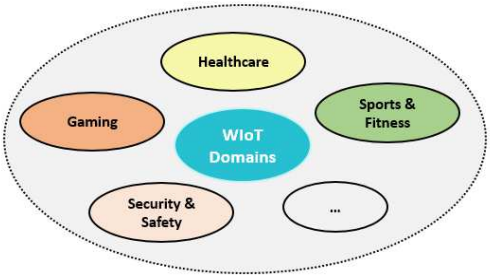

Figure 4: WIoT Application Domains

driven towards the benefits and implementation of a particular application scenario. Since the wearable devices are directly associated to the users and collect their physical and behavioral data, user privacy and data confidentiality and integrity are major issues impeding the success of WIoT. Currently, an IoT architecture for WIoT that focuses on its access control requirements is lacking. In this section, we discuss wearable devices and domains, and present an enhanced ACO architecture which incorporates devices, components, and authorizations relevant to WIoT.

A. Wearable Devices and Application Domains

Wearable devices are gaining popularity due to their lightweight nature and their capabilities of continuously tracking users for improving their quality of life. They are the building blocks of WIoT. A wearable IoT device is defined as one that collects user data, processes and analyzes the data based on some intelligence, and delivers useful insights to the users [34].

The wearable devices in today's world can be classified into three types: *In-Body, On-Body,* and *Around-Body*. **In-body** wearable devices are installed inside the human body, such as implantable devices (e.g., a Pacemaker). **On-body** wearable devices are those which can be worn on the body, such as wearable sensors, clothing and accessories, and other contact-based sensors. **Around-body** devices are the ones which are in close proximity of the users. Generally, they work together with prior two types of devices and gather data around users, such as user environment data, to perform defined functions. These devices on their own would not be considered wearable devices, and be more like general IoT devices.

Previously, we discussed IoT domains in general. Here we discuss WIoT domains— *health care, sports and fitness, security and safety,* and *gaming*. The domain space for WIoT is widening over time as we see innovative devices and applications. Figure 4 shows the WIoT application domains which are discussed below.

- **Health Care:** Health care is one of the largest application domain of wearable devices today. IoT has many applications ranging from remote patient monitoring to assistance for chronic disease patients and elderly population. Wearable technology is the backbone of IoT in health care domain. With numerous wearable sensors and devices, the health of patients can be monitored remotely which helps in managing hospital resources, and at the same time allows patients to live comfortably in their house. Wearable medical devices allow the patients to be more independent and be better aware of the benefits of a healthier lifestyle. Ambient assisted living is another scenario where WIoT is widely being used [35].
- **Sports and Fitness:** For athletes, it is very important to track their performance and improve their weaknesses to achieve desired goals. Wearable devices for tracking activity and different body parameters, such as smart watches and bands, heart rate and pulse monitors, and pedometers, are available in the market today. Social networking allows the collected data to be shared with other users. Fitness tracking bands are available and affordable, enabling users to track their fitness.
- **Security and Safety:** With numerous devices and platforms which a user needs to access, there is the possibility to incorporate user credentials in a wearable device. Nymi band [36] is one such wearable device that can be used as a multi-factor authentication device for the user who wears it to authenticate to different applications or services. Another important application domain is safety. There are smart phone applications to track locations of different things and people. This can be easily extended to wearable devices that would track your location for safety purpose. For example, if there is a natural disaster and your location needs to be traced for rescue operations. Similarly, such wearable devices are beneficial to the people going on long treks in dangerous places. Some of the wearable safety devices are discussed in [37].
- **Gaming:** Virtual reality is becoming more and more popular in the gaming industry. Wearable head mounted displays and other wearable devices will soon take over existing gaming devices.

WIoT has great potential in these domains but needs strong authentication and access control mechanisms to support it with billions of wearable devices and associated big data. A persistent problem in this domain is how to identify a user attached to a wearable device, since the device could be intentionally or accidentally given to an unauthorized user. Authentication based on biometric parameters is an effective solution in such scenarios. Besides, authorization is another critical issue that needs to addressed.

B. Enhanced ACO Architecture for WIoT

The wearable devices are usually resource constrained with limited computing, storage, and power. These devices communicate to a special device with comparatively better storage and computing power, known as *gateway devices*. These gateway devices abstract out the heterogeneity at the object level and facilitate pushing the data to a server or a cloud through the Internet. Due to large amount of data generated by WIoT, a Cloud-enabled architecture is essential to support WIoT. In this section, we extend the ACO architecture [6], discussed earlier, for IoT to incorporate components and communications of WIoT. We choose this architecture since it has been designed

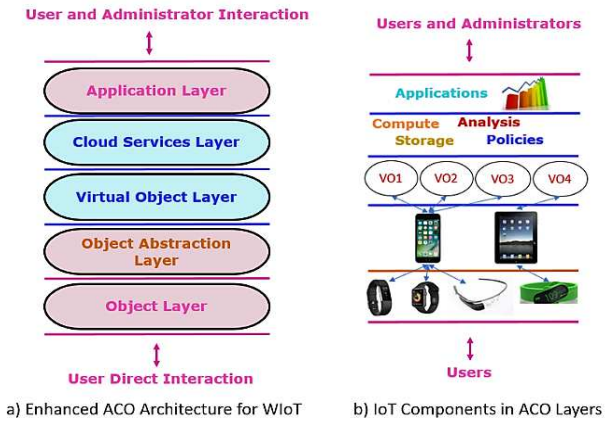

Figure 5: Enhanced ACO Architecture for WIoT

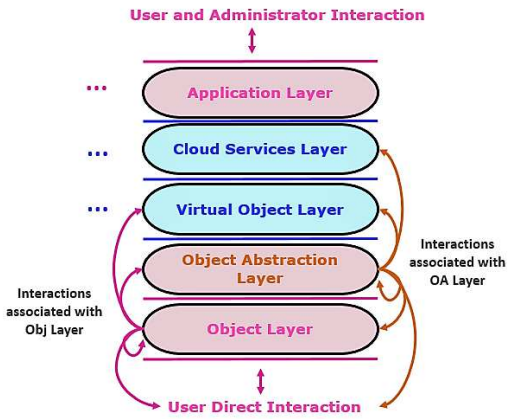

Figure 6: Interactions Between ACO Layers

from an access control perspective and supports the CEIoT framework. It has four layers: *object layer, virtual object layer, cloud services layer,* and *application layer*. In general, these layers encompass all the aspects of Cloud-Enabled IoT. However, due to the heterogeneity and resource constrained nature of wearable devices, there is a need for an abstraction layer which provides a gateway for the edge devices/things to communicate to the upper layers in the architecture. Therefore, we enhance the ACO architecture by introducing an **Object Abstraction (OA) Layer** in context of WIoT.

The enhanced ACO architecture for WIoT is shown in Figure 5(a). The OA layer is extended from the object layer and is comprised of gateway devices, such as smart phones. It has a unique task to facilitate object to VO communication abstracting all the heterogeneity (network and communication protocols) involved in the object layer. We assume as the edge devices become more sophisticated in the near future, the need of an abstraction layer may be reevaluated. In the rest of the paper, the ACO architecture refers to our enhanced ACO architecture, unless otherwise specified. In Figure 5(b), various components within each layer and their interactions are shown for a typical wearable IoT scenario with wearable edge devices, gateway devices, virtual objects, cloud services, and applications for monitoring and visualizing the IoT data.

IV. Access Control Framework For CEWIoT

Security and privacy in WIoT are primary factors that will enable its wide adoption and continued success at the consumer level. The key technologies to achieve the objective of security and privacy are access control mechanisms. In general, access control requires both authentication and authorization techniques, however, we scope our work here to the authorization mechanisms in a specific instance of IoT, the WIoT. As discussed earlier, the constrained wearable devices demand a cloud-enabled IoT (CEIoT) architecture. Therefore, we adapt CEIoT architecture in context of WIoT, that is Cloud-Enabled Wearable Internet of Things (CEWIoT).

In order to develop a comprehensive set of access control models for CEWIoT, we need an access control framework that captures different types of communications and data exchange within and among the five layers of the ACO architecture. The layers of the ACO architecture encapsulate various entities, such as users, edge objects, gateway objects, virtual objects, cloud services, applications, and administrators, and these entities further comprise of other sub-entities. A single access control model would not be sufficient to capture all the access control requirements of different layers (and their associated entities) in the ACO architecture. Hence, we develop an Access Control (AC) framework for controlling access and data exchange between several entities in CEWIoT.

A. Access Control (AC) Framework

In the academic literature, many access control models have been proposed for IoT. Ouaddah et al. [38] extensively discuss access control models developed for IoT. The diverse and dynamic nature of IoT requires a unified access control framework for grouping different types of IoT models focusing on distinct IoT components and their interactions.

Figure 6 shows the possible interactions associated with two of the ACO layers (Object and OA) explicitly, where other layers' interactions follow the same pattern (represented as dots), in the five layered ACO architecture for WIoT. Here, we assume each layer can interact with itself and its adjacent layers upto two levels in each direction (up and down). For instance, the interactions associated with the Object layer are: *i) with itself (Obj–Obj), ii) with users (Obj–Users), iii) with OA layer (Obj–OA),* and *iv) with VO layer (Obj–VO)*. There are numerous such interactions associated with each ACO layer where each one of them represents an authorization point in WIoT. The access control models addressing these authorization points are grouped into three categories of models: *i) Object Access Control, ii) Virtual Object Access Control,* and *iii) Cloud Access Control*, which comprises our Access Control (AC) framework for CEWIoT. The AC framework incorporating all the possible interactions in the ACO architecture for WIoT is shown in Figure 7.

There are two modes of interaction between any two layers of the enhanced ACO architecture, first *direct interaction (DI)*

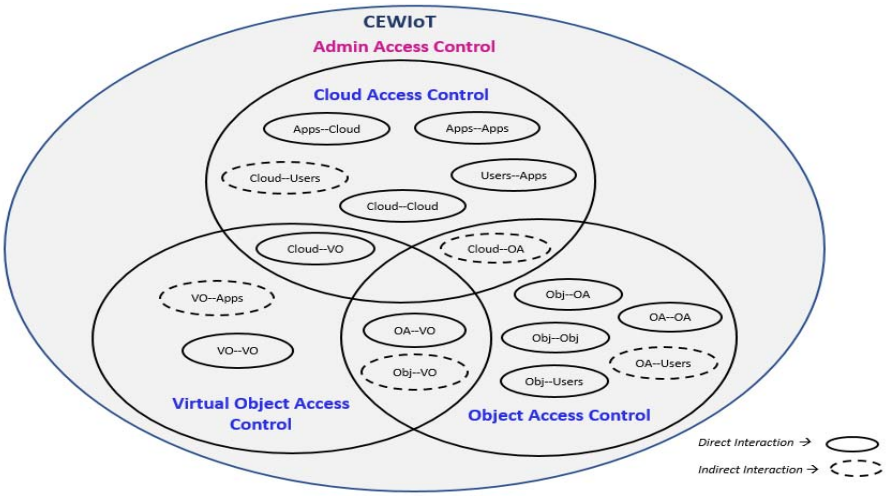

Figure 7: Access Control Framework Based on Interactions Between Different Layers of the ACO Architecture

and second *indirect interaction (IdI)*. For any layer, the DI implies interaction with itself and immediately adjacent layers; and IdI implies interaction with second level of adjacent layers at top and bottom of that layer. In the figure, DI are shown as solid ovals and IdI are shown as dashed ovals. There are some common interactions between any two category of models, such as *OA–VO*, and *Obj–VO* which belongs to both Object AC and Virtual Object AC models. This results into overlap between the AC categories in the framework. The outer administrative access control circle in the framework represents that admin access is relevant to the entire CEWIoT space, and administrative access control models can be designed for each one of the three AC categories. The interaction between layers of the ACO architecture is mediated by operational access control models, under configuration and control by administrators. The AC categories are discussed as follows.

- **Object Access Control Models:** This category of models includes the authorization at the Object layer and the Object Abstraction (OA) layer, as well as interactions with their adjacent layers (upto two level) in the ACO architecture. The edge IoT devices which are resource constrained reside at the Object layer, and gateway IoT devices that have sufficient resources for performing larger computation and storage functions reside in the OA layer. Access control models which focuses on communications, and data access and transfer within and outside these layers can be grouped into this category of models. The interactions covered in this category are: *Obj–Obj, Users–Obj, Obj–OA, Obj–VO, OA–OA, User–OA, OA–VO,* and *Cloud–OA*.
- **Virtual Object Access Control Models:** The access control models designed for virtual object (VO) communications among themselves (VO-to-VO), and for interactions with other layers can be grouped into the Virtual Object AC models. These models focus on interactions to and from the VOs, and encompass three direct interactions—*VO–VO, OA–VO, Cloud–VO*, and two indirect interactions—*VO–Apps* and *Obj–VO*.
- **Cloud Access Control Models:** The cloud services layer allows IoT to leverage its practically unlimited storage, computation, and analysis capabilities. It provides the flexibility and scalability needed for IoT [39]. The cloud is capable of hosting many IoT components. For example, AWS IoT hosts a device gateway, virtual objects, cloud services, and cloud applications. Thus, the access control models in this layer are more complex and may significantly overlap with above two categories. The interactions which need to be secured here are: *Cloud–VO, Cloud–OA, Apps–Cloud, Users–Cloud, Cloud-to-Cloud, Users-to-Apps,* and *Apps–Apps*. We include the applications layer interaction within this category of models, since applications mainly utilize the data stored and analyzed in the Cloud to provide IoT services to the users. Also, these applications are often Cloud applications with their application and database servers hosted in the Cloud.

Any access control model developed for CEWIoT can be easily mapped to one of the above three AC categories and may address authorization related to all the interactions (small circles inside a category) or a subset of the interactions relevant to that category. Our AC framework can be easily adapted for a general CEIoT architecture considering the original ACO architecture and relevant interactions.

B. Access Control Models

Here, we discuss appropriate access control models for our AC framework. Access control models in general can be divided into two types: *Operational*, and *Administrative* models, as shown in Figure 8. An operational access control model secures usage of resources and services in any application or system. It also controls access to the data in a system. Administrative access control models control the access of admin users on resources and entities, such as create,

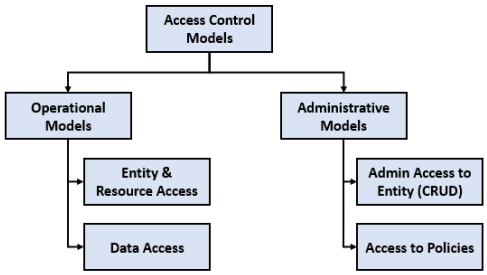

Figure 8: Types of Access Control Models

read, update, and delete, and manage access to policies. Also, typically in any system, only the admin users have authority to specify and update the access control policies. As per our framework, each of the three categories of AC models for CEWIoT includes respective operational and administrative models. Role-based access control (RBAC) has been widely utilized in developing both operational and administrative models for various systems and applications.

In [38], Ouaddah et al. have presented a qualitative and quantitative analysis of access control models for IoT. As per their analysis, Capability-based access control (CapBAC) have been employed quite often for addressing authorizations in IoT. Moreover, other access control models, such as RBAC and ABAC, have also been considered. Each one of these has its own advantages and disadvantages with respect to the IoT domain. The benefits of CapBAC are that it is user driven and supports delegation, however, it does not consider contextual or environmental information in the system. Whereas, ABAC employs contextual attributes (e.g., location, time, etc.), and user and subject attributes, and object attributes, but is often policy driven rather than user driven [38].

A Virtual Object AC model addressing VO–VO communication is developed by Alshehri and Sandhu in [40]. They developed operational and administrative access control models for controlling communications between virtual objects (VOs). For operational models, they utilized access control lists (ACLs), CapBAC, and ABAC, and for administrative models they used ACLs and RBAC. Their work aligns with our AC framework.

In [41], we recently developed an access control model for AWS Internet of Things, known as AWS-IoTAC. AWS IoT is a cloud-enabled IoT platform provided by one of the largest cloud service providers, Amazon Web Services (AWS) [42]. It controls the communications between several components, such as devices, virtual objects, cloud services, and applications based on the attributes and authorization policies defined for these entities in the Cloud. Our model was developed for a general CEIoT platform and is an instance of ABAC to some extent, with policy-based access control as its core. We also proposed some ABAC enhancements to our model for more fine-grained and flexible access control in AWS IoT. This model fits into the Cloud AC model category

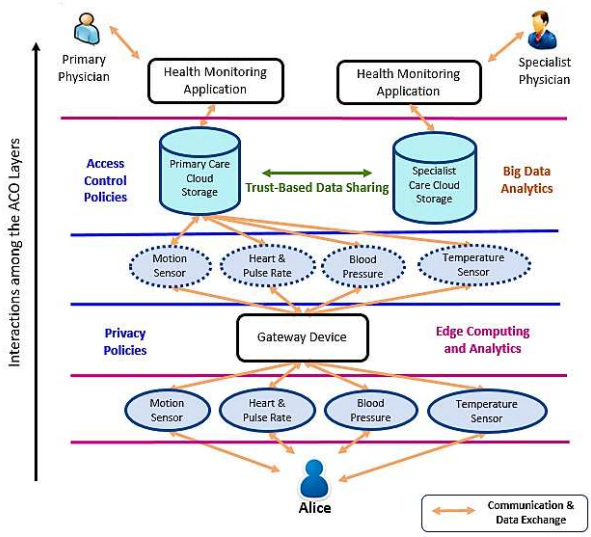

Figure 9: A Remote Health and Fitness Monitoring Example

of our framework and captures the interactions between cloud services and IoT entities.

We believe more fine-grained access control models for CEWIoT can be developed based on above models. However, they need to consider the unique characteristics and properties of WIoT. Some of the suitable models to support the properties of CEWIoT will be influenced by ABAC and ReBAC, together with combining benefits of other models, such as CapBAC. ABAC models are capable of incorporating the attributes of the users of wearable devices and relevant contextual attributes, such as location of the users. Similarly, ReBAC models will be used to capture the relationship of users and objects in context of wearable things.

For developing administrative models, RBAC provides great flexibility and administrative capabilities. ABAC is another suitable model for controlling admin authorization and functions. An administrative model for hierarchical attribute-based model (HGABAC) [43] is developed in [44]. Influenced by such models, administrative models for operational WIoT models can be developed. These are some of our initial insights, however, more concrete access control models for CEWIoT require further research.

V. Use Case

A. Remote Health and Fitness Monitoring Example

For the use case, we consider a remote health and fitness monitoring (RHFM) example as shown in Figure 9, within the ACO architecture for CEWIoT. In this example, we discuss the access control points along the ACO layers and how they map to the three categories of models in our AC framework. *Alice* has a problem of high blood pressure, and uses wearable technology to monitor her health and overall fitness. At the Object layer, there are four wearable devices—*a motion sensor, a heart rate and pulse sensor, a blood pressure sensor,* and *a temperature sensor*, which Alice uses to measure relevant body

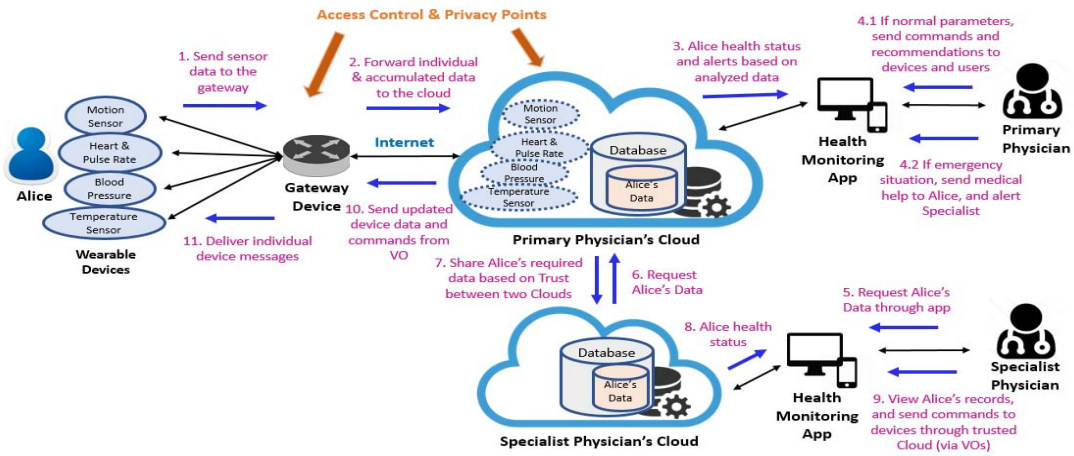

Figure 10: A Sequential View of RHFM Example

parameters. These devices communicate to a gateway device (Alice's smartphone) at OA layer, that allows interaction with the upper layers of the architecture. OA layer provides an initial access control point where user-centric privacy policies can be deployed. It could also be used as an edge computing and analysis platform for WIoT. For each wearable device, we assume a corresponding VO (*one-to-one association)* at the VO layer. VO layer facilitates seamless communication between applications and physical devices, and addresses several IoT issues, such as identification, scalability, heterogeneity, security and privacy [40].

The huge amount of IoT data collected by these devices is stored and analyzed at the cloud services layer. There are two data storage in the cloud, one for Alice's Primary physician and second for her Specialist physician. All the data is by default stored at her Primary physician's data storage. The data is securely shared with the Specialist physician only when the need arises, for example when the Specialist or Alice request it to be shared, or in some emergency situation. Data security and privacy should be maintained based on trust established between the two physicians with user consent. Access control and privacy policies for any access control model, designed for either secure communications or data security and privacy, can be defined at the Cloud services layer as an Authorization service. The Cloud with ample resources also enables Big Data Analytics in WIoT. The analyzed data is then utilized by the Health Monitoring applications to show meaningful results to the physicians, at the Application layer.

The interactions within and among different layers need to be authorized. For example, the edge wearable devices associated with a particular user must communicate to an authorized gateway device. Similarly, the gateway device must uniquely identify and authenticate the edge devices and allow authorized communication and data exchange with respective virtual objects. The access control models which would address such authorizations at the Object layer and OA layer and among their adjacent layers are Object AC models. In our use case, we assume that the wearable devices do not communicate with each other, however, a possible scenario of communication between physical objects is WSNs, where each node can talk to every other node in the network. Correspondingly, appropriate models addressing authorizations associated with VOs need to be developed. The Virtual Object AC models, as in [40], control access to virtual objects and relevant topics/channels in a publish/subscribe model. The Cloud AC models comprise models designed for controlling access to and from cloud services and resources, as well as any access control model developed for securing data in the cloud, and for enabling secure collaboration and data sharing between tenants, accounts, or clouds.

Figure 10 depicts a sequential representation of the use case. Alice uses four wearable devices—*a motion sensor, a heart rate and pulse sensor, a blood pressure sensor,* and *a temperature sensor*. The devices authenticate and communicate to a gateway device, which sends the collected data to their corresponding VOs instantiated in the Primary physician's Cloud. This data is then stored in the database, and analysis is performed on it in the Cloud. The health monitoring application provides useful insights to the Primary physician based on Alice's data analytics results. If everything is normal, Primary physician sends commands and recommendations to Alice by sending messages to the devices through the VOs. Whereas, in case of an emergency situation, immediate medical help is sent to Alice, and an alert (e.g., email) is sent to the Specialist physician based on some predefined rules. Alice's data and analytics results are shared with the Specialist physician's cloud as required based on established trust and access control policies. The Specialist physician can also send commands to the edge devices, and schedule a visit for Alice and inform her through the application by sending updates to the device VOs in Primary physician's cloud. The gateway device ensures the delivery of messages sent by physicians to physical edge devices. In this scenario, there is no direct interaction between physicians or applications. The setup and configuration of the

use case would be done by a number of administrators (cloud admin, health care admins, etc.) and the user (Alice).

B. Proposed Enforcement in AWS IoT

Based on our previous work [41], we propose an enforcement of above use case in the AWS IoT platform utilizing its services and functionalities. Previously, we implemented a smart-home use case in AWS IoT, along with setting up configurations and authorization policies for VOs, physical devices, and cloud services. In AWS IoT, a *Thing* for each wearable device needs to be created, which is its equivalent VO and has a *Thing Shadow* that provides a set of topics for clients (devices, apps) to publish/subscribe messages. For each device, a valid certificate registered in AWS IoT should be created and copied onto the physical devices. This is a complicated task since the devices need to be compliant with the AWS IoT protocols and standards. AWS IoT has its own device gateway which enables secure authentication and communication with edge devices. The idea of employing privacy-preserving policies defined by users or administrators at the gateway level requires further investigation, since device gateway is embedded in the platform and cannot be accessed by the cloud users, probably due to security reasons. The IoT data generated can be stored in a *DynamoDB* database, and desired computation and analysis be performed utilizing AWS *Lambda function*. Based on the assumption that physicians use the AWS cloud, the application server for health monitoring applications would be hosted in the Cloud. However, in case of a collaborative data sharing scenario, appropriate cross-tenant or cross-account access control models for WIoT are currently missing in a cloud-enabled IoT architecture.

VI. Objectives of AC Framework and Research Problems

In this section, we discuss the objectives of our AC framework for CEWIoT and relevant open research problems.

A. **User-Based Device Authentication:** Wearable devices have peculiar characteristics of being closely related to their owners (who actually wear them, and whose information they are collecting). Therefore, physical security is of great importance, and also device authentication mechanisms based on user biometrics are necessary, such as fingerprint and heart rate. This ensures that even if a wearable device is lost or stolen, an attacker would not be able to comprise the data security and integrity. Such techniques for wearable devices are already being investigated [36], as well as need further research.

B. **User-Centric Data Security and Privacy:** Wearable devices are attached to the users and collect very sensitive data and information that would compromise user privacy, if it falls into an attacker's hand. Therefore, security practices involving the users are necessary for preserving data privacy and security in WIoT. We believe that the users whose data is being collected should be involved in the authorization process, not at each and every step but at least at some initial point of the process. A recent study conducted on fitness tracker devices depicts threat to user personal data due to vulnerabilities in the devices and provides guidelines for better security [45].

C. **Edge Computing in WIoT:** Gateway device at OA layer is an ideal place to provide edge computing capabilities for constrained edge devices. One of the proposed mechanism of applying edge computing is cloudlets [46], which can be employed on the device gateways, such as a laptop or a small server machine at home. Edge computing is necessary in wearable devices due to their low bandwidth and low latency requirements which directly affects their usability. Edge computing in wearable cognitive assistance scenarios is discussed in [47]. For secure edge computing in WIoT, access control models for such scenarios demand significant research.

D. **Multi-Cloud Architecture:** With more than 25 billion connected IoT devices by 2020 [48], the need for a multi-cloud architecture is inevitable to support IoT. A collaborative data sharing scenario in Cloud is considered in our use case, yet appropriate Trust-based access control models for cross-tenant, cross-account, and multi-cloud architectures are still lacking in context of WIoT.

VII. Conclusion

The main objective of this paper is to develop a conceptual AC framework for cloud-enabled wearable IoT (CEWIoT). A flexible approach is necessary for securing the IoT space, and our framework would act as a guideline for researchers in developing fine-grained access control models for specific interactions and authorization in CEWIoT. It will play a vital role in the development of a family of AC models, focusing on particular scenarios, for the WIoT domain. Moving forward towards the goal of formalizing IoT concepts and terminologies, we presented a classification of IoT devices and discussed various application domains of IoT and WIoT. We also discussed suitable access control models, along with a WIoT use case and its possible implementation in the AWS IoT platform. In the future work, we plan to develop access control models focusing on some of the interactions in the three AC categories of our framework, especially Cloud Access Control models.

Acknowledgment

This research is partially supported by NSF CREST Grant HRD-1736209, NSF Grants CNS-1111925, CNS-1423481, CNS-1538418, and DoD ARL Grant W911NF-15-1-0518.

References

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[2] "Here's How the Internet of Things (IoT) Will Change Workplaces," http://www.insight.com/en_US/learn/content/2017/02072017-heres-how-the-internet-of-things-iot-will-change-workplaces.html, accessed: 2017-06-10.

[3] A. Botta, W. de Donato, V. Persico, and A. Pescapé, "Integration of Cloud Computing and Internet of Things: A Survey," *Future Generation Computer Systems*, vol. 56, pp. 684–700, 2016.

[4] P. Parwekar, "From Internet of Things Towards Cloud of Things," in *IEEE International Conference on Computer and Communication Technology (ICCCT)*, 2011, pp. 329–333.

[5] B. P. Rao, P. Saluia, N. Sharma, A. Mittal, and S. V. Sharma, "Cloud Computing for Internet of Things & Sensing Based Applications," in *IEEE International Conf. on Sensing Tech. (ICST)*, 2012, pp. 374–380.

[6] A. Alshehri and R. Sandhu, "Access Control Models for Cloud-Enabled Internet of Things: A Proposed Architecture and Research Agenda," in *IEEE International Conference on Collaboration and Internet Computing (CIC)*, 2016, pp. 530–538.

[7] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A Survey," *Computer networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[8] Z. Yang, Y. Yue, Y. Yang, Y. Peng, X. Wang, and W. Liu, "Study and Application on The Architecture and Key Technologies for IoT," in *International Conference on Multimedia Technology (ICMT)*. IEEE, 2011, pp. 747–751.

[9] P. Porambage, M. Ylianttila, C. Schmitt, P. Kumar, A. Gurtov, and A. V. Vasilakos, "The Quest for Privacy in The Internet of Things," *IEEE Cloud Computing*, vol. 3, no. 2, pp. 36–45, 2016.

[10] M. Wu, T.-J. Lu, F.-Y. Ling, J. Sun, and H.-Y. Du, "Research on The Architecture of Internet of Things," in *3rd International Conference on Advanced Computer Theory and Engineering (ICACTE)*, vol. 5. IEEE, 2010, pp. V5–484.

[11] "AWS IoT Platform," http://docs.aws.amazon.com/iot/latest/developerguide/what-is-aws-iot.html, accessed: 2017-01-08.

[12] K. Kotis and A. Katasonov, "An IoT-Ontology for The Representation of Interconnected, Clustered and Aligned Smart Entities," *Technical report, VTT Technical Research Center, Finland*, 2012.

[13] E. Welbourne, L. Battle, G. Cole, K. Gould, K. Rector, S. Raymer, M. Balazinska, and G. Borriello, "Building The Internet of Things Using RFID: The RFID Ecosystem Experience," *IEEE Internet computing*, vol. 13, no. 3, 2009.

[14] "IoT Device Categories Class 0,1,2," http://www.cisoplatform.com/profiles/blogs/classification-of-iot-devices, accessed: 2017-08-10.

[15] V. Jincy and S. Sundararajan, "Classification Mechanism for IoT Devices Towards Creating A Security Framework," in *Intelligent Distributed Computing*. Springer, 2015, pp. 265–277.

[16] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for Smart Cities," *IEEE Internet of Things journal*, vol. 1, no. 1, pp. 22–32, 2014.

[17] H. Schaffers, N. Komninos, M. Pallot, B. Trousse, M. Nilsson, and A. Oliveira, "Smart Cities and The Future Internet: Towards Cooperation Frameworks for Open Innovation," *The future internet*, pp. 431–446, 2011.

[18] P. Vlacheas, R. Giaffreda, V. Stavroulaki, D. Kelaidonis, V. Foteinos, G. Poulios, P. Demestichas, A. Somov, A. R. Biswas, and K. Moessner, "Enabling Smart Cities Through a Cognitive Management Framework for The Internet of Things," *IEEE communications magazine*, vol. 51, no. 6, pp. 102–111, 2013.

[19] G. Suciu, A. Vulpe, S. Halunga, O. Fratu, G. Todoran, and V. Suciu, "Smart Cities Built on Resilient Cloud Computing and Secure Internet of Things," in *19th International Conference on Control Systems and Computer Science (CSCS)*. IEEE, 2013, pp. 513–518.

[20] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions," *Future generation computer systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[21] S. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K.-S. Kwak, "The Internet of Things for Health Care: A Comprehensive Survey," *IEEE Access*, vol. 3, pp. 678–708, 2015.

[22] "How The Internet of Things is Revolutionizing Manufacturing," http://www.businessinsider.com/internet-of-things-in-manufacturing-2016-10, accessed: 2017-08-04.

[23] "Wearable Technologies," https://www.wearable-technologies.com/innovation-worldcup/categories/, accessed: 2017-08-15.

[24] M. Nitti, V. Pilloni, G. Colistra, and L. Atzori, "The Virtual Object as A Major Element of The Internet of Things: A Survey," *IEEE Comm. Surveys & Tutorials*, vol. 18, no. 2, pp. 1228–1240, 2016.

[25] L. Da Xu, W. He, and S. Li, "Internet of Things in Industries: A Survey," *IEEE Trans. on Indust. Informatics*, vol. 10, no. 4, pp. 2233–2243, 2014.

[26] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges," in *10th International Conference on Frontiers of Information Technology (FIT)*. IEEE, 2012, pp. 257–260.

[27] R. Roman, J. Zhou, and J. Lopez, "On The Features and Challenges of Security and Privacy in Distributed Internet of Things," *Computer Networks*, vol. 57, no. 10, pp. 2266–2279, 2013.

[28] R. Sandhu, E. J. Coyne, H. Feinstein, and C. Youman, "Role-Based Access Control Models," *IEEE Computer*, vol. 29, no. 2, pp. 38–47, 1996.

[29] D. F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn, and R. Chandramouli, "Proposed NIST Standard for Role-Based Access Control," *ACM Transactions on Information and System Security (TISSEC)*, vol. 4, no. 3, pp. 224–274, 2001.

[30] X. Jin, R. Krishnan, and R. Sandhu, "A Unified Attribute-Based Access Control Model Covering DAC, MAC and RBAC," in *IFIP Annual Conf. on Data and App. Security and Privacy*. Springer, 2012, pp. 41–55.

[31] V. C. Hu, D. Ferraiolo, R. Kuhn, A. Schnitzer, K. Sandlin, R. Miller, and K. Scarfone, "Guide to Attribute Based Access Control (ABAC) Definition and Considerations," *NIST Special Publication 800-162*, 2014.

[32] Y. Cheng, J. Park, and R. Sandhu, "Relationship-Based Access Control for Online Social Networks: Beyond User-to-User Relationships," in *International Confernece on Privacy, Security, Risk and Trust (PASSAT) and International Confernece on Social Computing (SocialCom)*. IEEE, 2012, pp. 646–655.

[33] S. Hiremath, G. Yang, and K. Mankodiya, "Wearable Internet of Things: Concept, Architectural Components and Promises for Person-Centered Healthcare," in *EAI 4th International Conference on Wireless Mobile Comm. and Healthcare (Mobihealth)*. IEEE, 2014, pp. 304–307.

[34] "The Challenges of Wearable Electronics ," http://www1.futureelectronics.com/Mailing/etechs/TEConnectivity/etechALERT_TE_ConsumerWearables/Images/WearablesWhitePaper_TE.pdf, accessed: 2017-08-08.

[35] A. Dohr, R. Modre-Opsrian, M. Drobics, D. Hayn, and G. Schreier, "The Internet of Things for Ambient Assisted Living," in *2010 Seventh International Conference on Information Technology: New Generations (ITNG)*. IEEE, 2010, pp. 804–809.

[36] "Nymi Band," https://nymi.com/, accessed: 2017-01-08.

[37] "Top 6 Wearable Safety Devices," https://blog.cammy.com/top-wearable-safety-devices, accessed: 2017-01-08.

[38] A. Ouaddah, H. Mousannif, A. A. Elkalam, and A. A. Ouahman, "Access Control in The Internet of Things: Big Challenges and New Opportunities," *Computer Networks*, vol. 112, pp. 237–262, 2017.

[39] P. Sethi and S. R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications," *J. of Electrical and Computer Engineering*, vol. 2017.

[40] A. Alshehri and R. Sandhu, "Access Control Models for Virtual Object Communication in Cloud-Enabled IoT," in *18th International Conference on Information Reuse and Integration (IRI)*. IEEE, 2017.

[41] S. Bhatt, F. Patwa, and R. Sandhu, "Access Control Model for AWS Internet of Things," in *International Conference on Network and System Security*. Springer, 2017, pp. 721–736.

[42] "Amazon Web Services (AWS)," https://aws.amazon.com/, accessed: 2016-12-10.

[43] D. Servos and S. L. Osborn, "HGABAC: Towards A Formal Model of Hierarchical Attribute-Based Access Control," in *International Symposium on Foundations and Practice of Security*. Springer, 2014, pp. 187–204.

[44] M. Gupta and R. Sandhu, "The {GURA_G} Administrative Model for User and Group Attribute Assignment," in *International Conference on Network and System Security*. Springer, 2016, pp. 318–332.

[45] "Fitness Trackers Could Benefit from Better Security," http://www.ed.ac.uk/news/2017/fitness-trackers-could-benefit-from-better-securit, accessed: 2017-09-15.

[46] M. Satyanarayanan, P. Bahl, R. Caceres, and N. Davies, "The Case for VM-Based Cloudlets in Mobile Computing," *IEEE pervasive Computing*, vol. 8, no. 4, 2009.

[47] M. Satyanarayanan, "The Emergence of Edge Computing," *Computer*, vol. 50, no. 1, pp. 30–39, 2017.

[48] "Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020," http://www.gartner.com/newsroom/id/2636073, accessed: 2017-07-02.