Convergent Access Control to Enable Secure Smart Communities

Smriti Bhatt*, Ravi Sandhu†
*Dept. of Computing and Cyber Security, Texas A & M University-San Antonio, San Antonio, Texas 78224, USA
†Institute for Cyber Security and Dept. of Computer Science, Univ. of Texas at San Antonio, Texas 78249, USA
*sbhatt@tamusa.edu, †ravi.sandhu@utsa.edu

***Abstract*—With current technological advancements in IoT, Artificial Intelligence, and networking (e.g., 5G/6G) technologies, we are swiftly moving towards enabling future connected smart communities. We envision a smart community (SC) as an interconnected ecosystem ranging from a small region to a global scale enabled by IoT devices and key technologies for the betterment of its citizens, businesses, and organizations. A critical aspect for enabling such future smart communities is developing a secure and privacy-preserving access control (AC) framework to defend against malicious actors in the system. Traditionally, access control principles have been formulated based on the access control requirements of an enterprise, an application or a system. Smart communities are an evolving and dynamic concept that includes a range of interdisciplinary components. Thus it is appropriate to reevaluate current access control principles for such a diverse and dynamic ecosystem. In this paper, we first discuss access control requirements and then present access control principles for future smart communities. We envision a convergent access control approach towards enabling future smart communities where different access control models synergistically converge at both policy and enforcement layers. Therefore, we propose a Convergent Access Control (CAC) framework that can address the access control requirements of dynamic application domains such as in future smart communities. The main goal of this paper is to present the vision and need for the CAC framework and initiate discussion on the future research agenda.**

***Index Terms*—Internet of Things, Smart Communities, Access Control Principles, Convergent Access Control**

I. Introduction

In today's connected world, everything and anything around us is being connected to the Internet [1]. With Internet of Things (IoT) devices and applications, and supporting technologies, such as cloud and edge computing, Artificial Intelligence (AI), Machine Learning and data analytics, we envision future connected smart communities (SC) where the users will be connected to the Internet along with their smart devices that utilize smart infrastructures, such as offices, buildings, homes, and hospitals. The concept of smart cities has received significant attention in both academia and industry recently, whereby smart communities are sometimes considered as inclusive with smart cities. Our vision of the smart communities expand beyond cities and nations to create a global connected ecosystem ranging across geographically distributed regions. Such smart communities consist of multiple small connected communities that require a highly collaborative and interdisciplinary ecosystem including IoT, networking, AI, and distributed computing, and personnel such as researchers and subject experts with different skills, knowledge, and expertise. The goal of enabling these smart communities is to improve the quality of life by developing applications for various components of the communities, including efficient energy consumption, smart street and traffic lights, smart public transportation, electric vehicle charging stations, and a smart crime detection and prevention system [2], [3].

One of the key aspects of deploying and sustaining such future connected smart communities is to ensure user data security and privacy by developing a secure access control framework. In this paper, we mainly focus on access control requirements and principles within the context of smart communities. Smart communities are largely distributed and dynamic in nature with specific characteristics, which makes it difficult and insufficient to apply traditional access control principles and models in this context. Therefore, we first discuss the access control requirements for smart communities (SC) with respect to their characteristics, and then define access control principles for SC. While general access control principles have already been defined, here we present access control principles for a constantly growing and evolving domain, i.e., smart communities. These principles are inspired by access control principles defined for next generation role-based access control [4], [5] in [6]. We also utilize the Policy, Enforcement, and Implementation (PEI) framework [7] to identify and map the access control principles at policy layer.

Next, we discuss the need for a convergent access control approach for addressing the access control requirements of future smart communities. In academic literature, several access control models, such as Discretionary Access Control (DAC) [8], [9], Mandatory (or Lattice-Based) Access Control (MAC) [10], Role-Based Access Control (RBAC), and Attribute-Based Access Control (ABAC) [11], [12], have been developed. While these models are abstract enough to be applied in diverse application domains, customized access control models adapted from these have been developed for specific application domains, such as web services, cloud computing, IoT, and online social networks [13]–[20]. With specific IoT application domains, there are several other subdomains [1] that have their application specific access control requirements, and thus, we need more customized access control models. For example, within IoT, several access control models for smart home and smart cars have been developed where the underlying models are one of the above access control models, i.e., RBAC or ABAC. Motivated by these scenarios, we believe that a single access control model, for instance either RBAC or ABAC, is not sufficient to address all the access control requirements of dynamic application domains as in the case of future smart communities. Hence, we envision and propose a Convergent Access Control (CAC)

978-1-7281-8543-9/20/$31.00 ©2020 IEEE
DOI 10.1109/TPS-ISA50397.2020.00029

framework which converges features and characteristics of different access control models, be it DAC, MAC, RBAC, ABAC, or others, together to address dynamic and changing access control requirements of any domain. For developing the CAC framework, it is essential to understand the difference between developing and formalizing access control models at policy layer and enforcing and deploying these models at enforcement layer of the PEI framework. This convergent approach towards access control incorporates various challenges and demands further research.

Figure 1 shows different aspects of access control in the context of future smart communities. The main contributions of this paper are outlined as follows.

- We first present the essential requirements of access control models in the context of smart communities along with their characteristics.
- We then define the access control principles for smart communities based on existing access control principles for next generation RBAC.
- Finally, we propose a Convergent Access Control (CAC) framework that converges different access control models and their features. We argue it is essential to establish convergence across several access control models and utilize the desired access control model features for enabling secure, safe, and sustainable connected smart communities in the future.

The rest of the paper is organized as follows. Section 2 discusses smart communities, PEI framework, and existing access control principles. Section 3 presents essential requirements for access control models and access control principles for future smart communities respectively. Section 4 presents a smart community use case and proposes the Convergent Access Control (CAC) framework. It also discusses the need for such a framework in the context of smart communities with the help of the use case scenario. Section 5 discusses various challenges and future research directions to enable the CAC framework in the context of smart communities. Finally, Section 6 concludes the paper.

II. Background

In this section, we define our vision of smart communities and provide brief background on the PEI framework and access control principles.

A. Smart Communities

Smart Communities (SCs) are emerging today with the convergence of IoT, Cyber-Physical Systems (CPS), cloud and edge computing, and intelligent applications based on AI and ML (Machine Learning) technologies. SCs are composed of physical devices, objects, and users where all of these entities are more-or-less always connected and interacting with each other [3]. We envision SCs as an interconnected region that leverages the smart use of technologies to benefit its citizens, businesses and organizations in various sectors including economic growth, social benefits, and environmental sustainability. A smart community can also be defined as a collection of connected human-cyber-physical systems enabled by IoT, cloud and edge computing technologies and services. One of the main objectives of developing future connected smart communities is to establish sustainable societies that improves human well being, safety, and security. With such a rapidly evolving connected ecosystem, there are several security and privacy threats including new attack surfaces being exposed to the attackers everyday, e.g., in [21], authors show that there are GPS security vulnerabilities in unmanned ground vehicles (UGVs) and are susceptible to spoofing attacks.

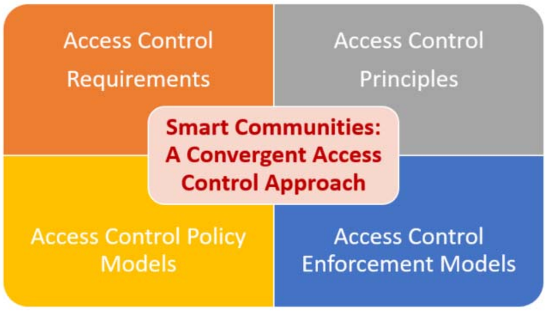
Access Control Requirements
Access Control Principles
Smart Communities: A Convergent Access Control Approach
Access Control Policy Models
Access Control Enforcement Models

Fig. 1. Access Control Aspects in Future Smart Communities

Smart communities have gained significant traction in the research community. Blockchain applications, challenges, and opportunities for smart communities were discussed in [22]. Another Blockchain application for SCs was proposed in [23] where a contract-based energy blockchain was used for secure electric vehicles charging in smart communities. Smart communities are enabled through connected sensors and smart devices that can collect large amount of data (user, system, and environment data). This large amount of data can be stored and analyzed using AI and ML technologies and algorithms on cloud platforms. Some of the popular cloud providers that have introduced their own IoT services are Amazon Web Services (AWS) [24], Azure [25], Google Cloud Platform (GCP) [26], and IBM Cloud [27].

To enable future smart connected ecosystem, an essential component is active collaborations between these large cloud providers and academic researchers. These cloud platforms already use features from multiple access control models due to industry realization that a single access control model is insufficient to meet the rapidly emerging security and privacy needs of IoT and future connected smart communities. Initially, most of these cloud providers utilized some customized form Role-based access control (RBAC) model. But, with the advent of new IoT technology, they are already exploring other access control models, such as Policy-based access control (PBAC) and Attribute-based access control (ABAC). We believe this is right time to start research towards converging access control models and develop an enhanced convergent access control approach for addressing dynamic access control requirements.

Within the scope of smart communities there are several smart application domains, some of them are discussed as follows [2].

- **Smart Energy** – Today's houses are enabled through smart sensors and devices and smart energy meters. Energy providers are providing incentives to users for actively reducing energy consumption.
- **Smart Street Lighting** - Using IoT technology and sensor networks, cities and municipalities can control the timing and brightness of street lights, and provide safety by lighting up bike paths to improve public safety.
- **Public Transportation** – With smart technology, public bus networks can be managed based on data analysis gathering most common traffic flows, where traffic is monitored in real time by the City and information about current travel time on certain roads broadcasts to the users to find best routes available.
- **Smart Utilities** – It provides a mechanism to manage your utilities using connected sensors and smart devices. In a distributed energy network, IoT sensors can provide the city an energy system that has enough capacity to receive as well as redistribute electricity to and from multiple energy sources.
- **Autonomous Vehicles** – Every car manufacturer have started incorporating various sensors insides and outside cars and soon enough, we will have connected autonomous vehicles on the streets in future SCs. IoT and CPS technology need to be used for enabling secure smart vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications and interactions [28].
- **Smart Farming and Infrastructure** – Sensor technology is implemented in public parks, and parking spots. Smart cooperative farming [29] employs sensors, drones, and other smart devices for precision agriculture and manage irrigation systems, where real time data is transmitted to farmers for watering their fields based on soil moisture.

B. PEI Framework

The PEI framework from an application-centric security perspective was presented by Sandhu [7]. Figure 2 shows the PEI framework along with its layers and components. There are three layers, namely the Policy (P), Enforcement (E) and Implementation (I) layers. At each layer (except for objectives) there need to be formal models defined to express and analyze the security policies. The topmost objectives layer is a high level layer that is deliberately kept informal to depict system level goals. At this layer, manager or CEO level input and judgement can be specified. In general there are always major tradeoffs within competing security and functional needs of the system which should be articulated informally here. The bottom layer focuses on actual running code, where trusted computing technology can be incorporated. The three inner layers of PEI framework are intended to have a many to many relation which implies that a policy model at the P (policy) layer may have many different manifestations at the E (enforcement) layer. Conversely, the authors believe that an enforcement model at the E layer may be able to support many different models. For example, a suitably configurable attribute-based enforcement model at the enforcement layer can enforce distinct policy layer models such as Role-Based Access (RBAC) Control or Mandatory Access Control (MAC).

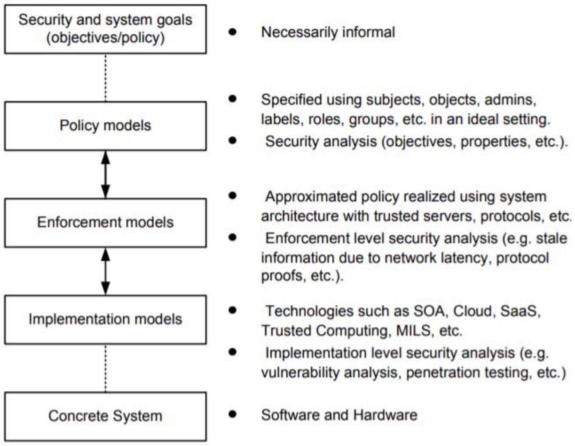
Security and system goals (objectives/policy)
Necessarily informal
Policy models
Specified using subjects, objects, admins, labels, roles, groups, etc. in an ideal setting.
Security analysis (objectives, properties, etc.).
Enforcement models
Approximated policy realized using system architecture with trusted servers, protocols, etc.
Enforcement level security analysis (e.g. stale information due to network latency, protocol proofs, etc.).
Implementation models
Technologies such as SOA, Cloud, SaaS, Trusted Computing, MILS, etc.
Implementation level security analysis (e.g. vulnerability analysis, penetration testing, etc.)
Concrete System
Software and Hardware

Fig. 2. The PEI Framework [7]

In this paper, we utilize the PEI framework to categorize and map the requirements and principles of access control in the context of future smart communities. Similarly, it is also important to identify and map these requirements and principles from an *operational* and *administrative* perspective. The will eventually help in developing a family of access control models for smart communities based on our proposed Convergent Access Control (CAC) framework.

C. Access Control Principles

Here, we discuss the ASCAA principles developed for next-generation role-based access control models by Sandhu et al. [6]. There were five access control principles defined for next generation access control in general including next-generation RBAC, summarized as ASCAA for Abstraction, Separation, Containment, Automation and Accountability.

- **Abstraction** – The abstraction principle refers to abstraction of permissions. In general, permissions and operations are system specific. For example operating systems typically support permissions such as read, write and execute. Database management system permissions could be select, delete, update, etc.
- **Separation** – Separation refers specifically to separation of administrative functions and operational functions. This is essential to manage access control policies for different types of users - admin and non-admin. It also allows to simplify the administration of access control models for the administrators by separating their functions with respect to the access control model being used.
- **Containment** – As presented in [6], the containment principle unifies the older principles of least privilege

and separation of duty, and further incorporates additional constraints and usage control elements. Least privilege has been a basic access control principle and is still widely engraved in basic security of any application domain. It defines that any actor entity (e.g., user or process) should have least privilege or minimum set of permissions essential to perform their jobs. While separation of duties enables restriction on who can do what since a user should not have all permissions to do all jobs. The concept of containment seeks to limit the damage that a user, or a set of users, can perpetrate either by deliberate malice or by victimization from malicious malware.

- **Automation** - Automation of access control administration is believed to be inevitable in next-generation access control. Due to increasing and evolving access control requirements, automatic privilege assignment and revocation is necessary to keep pace with growing requirements of cyberspace today.
- **Accountability** - The primary goal of accountability is to make a human user take responsibility for actions that the individual performs in a system. This can be achieved in a combination of three basic ways. Sensitive operations can be subjected to a more detailed level of auditing but unless the audit records are brought to some other user's attention the audit trail is useful only as a forensic tool. Detailed audit trails can trigger fraud detection systems to direct their attention to suspicious activity but ultimately some user has to be alerted.

These are the ASCAA principles and inspired by these access control principles, we will define access control principles for future smart communities which have different set of access control requirements as presented in the next section.

III. Access Control Principles for Future Smart Communities

In this section, we discuss the essential requirements of access control models and mechanisms for a dynamic and highly distributive architecture, i.e., connected smart communities. The smart communities (SC) are drastically different than other domains since it incorporates multiple application domains, components and technologies, along with different types of users (e.g., admins, actors who are performing actions, and even targets on which actions are being performed). Figure 3 presents our SC vision with modular features at base layer, integral components at second layer, and enabling infrastructure as top layer with multiple shared clouds across smaller communities connected to the main SC cloud. The modular features represent the basic features, such as physical devices, connected vehicles, drones, and access control policies, which comprises and can be utilized in forming any of the integral SC components such as connected workspaces, online learning, remote health, smart homes, and cooperative farms, and others (e.g., smart transportation). The top layer depicts key enabling technologies of SC including 5G, faster and wider coverage, and access control models and enforcement systems. Based on the modular features and integral components of SC as shown in the Figure 3, we believe that different types of access control features (e.g., attributes, roles, and realtionships) can be extracted from the modular view of smart communities to enable access control convergence in SC.

A. Essential Requirements for Access Control models for Smart Communities

In the context of this dynamic and highly distributive smart architecture, we now discuss the access control requirements of connected smart communities. These requirements of access control models are identified and defined based on the characteristics of smart communities. These requirements are mainly considered while designing new access control models and/or adopting existing access control models for SCs.

- **Dynamic Authorization** - In a highly dynamic architecture as SC, the access and authorizations are rapidly changing based on the components and the context where these components are being used within the smart communities. For example, in a remote health domain, the access requirements will change based on the type of users (e.g., doctors, nurses, patients, etc.) and the devices they use and their locations. The access control requirements for users and their devices in a smart hospital with numerous users would be different than a smart home requirements where the user is interacting with limited trusted users and its own devices in a more trusted environment. Thus, we need dynamic authorization capabilities that can change the authorizations based on the context. Access control policies need to be written in a way that they are able to dynamically adapt and assign privileges to users, devices, or applications.
- **Flexibility** - Since there are several components involved in SCs, flexibility in defining and updating access control policies for various entities and scenarios is an essential requirement. Attribute-Based Access Control (ABAC) has been widely referred as flexible access control since it allows to define fine-grained access control policies based on the attributes (and their values) of different entities.
- **Scalability** - In a large connected ecosystem, there are billions of connected users and devices that continuously communicate with each other. Smart communities range from small to large communities, therefore, access control mechanisms must be scale to incorporate authorizations associated with small or large number of devices, users, and other entities in SC.
- **Decentralization** - The next generation smart communities will be highly decentralized where any one entity or component would not be able to take all access control decisions unlike cloud-IoT platforms that we see today. Generally, cloud-enabled IoT platforms, such as Amazon Web Services (AWS) or Google Cloud Platform are still using a centralized architecture where all access control policies are defined in the cloud and enforced on different entities, such as devices, users, and applications [1]. In future smart communities, there will be multiple

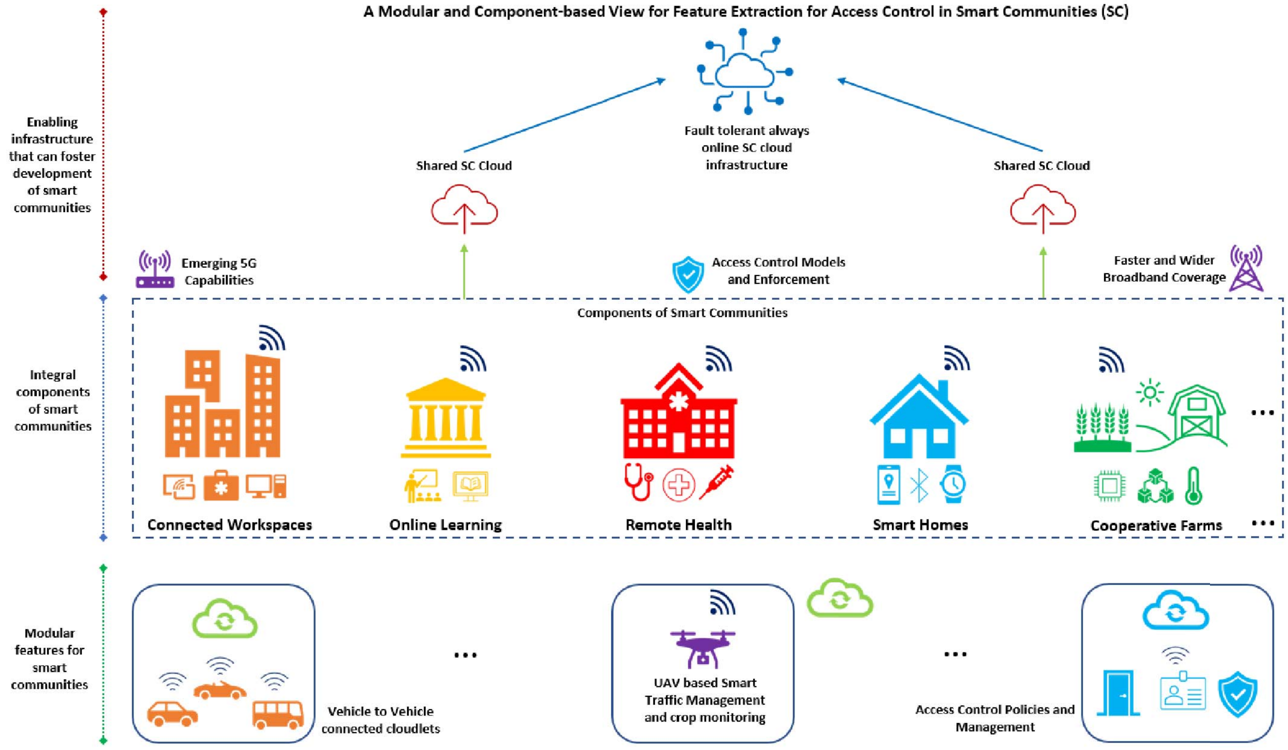
A Modular and Component-based View for Feature Extraction for Access Control in Smart Communities (SC)
Enabling infrastructure that can foster development of smart communities
Fault tolerant always online SC cloud infrastructure
Shared SC Cloud
Shared SC Cloud
Emerging 5G Capabilities
Access Control Models and Enforcement
Faster and Wider Broadband Coverage
Components of Smart Communities
Integral components of smart communities
Connected Workspaces
Online Learning
Remote Health
Smart Homes
Cooperative Farms
...
Modular features for smart communities
Vehicle to Vehicle connected cloudlets
UAV based Smart Traffic Management and crop monitoring
Access Control Policies and Management
...

Fig. 3. A Modular View of Smart Communities and its Components

clouds and edge cloudlets that will have a set of users and devices connected and interacting with them, thus, access control models and policies need to be defined and enforced in a decentralized manner so that access decisions can be made quickly.

- **Compliance** - We propose compliance as one of the access control model requirements since currently there is lack of access control standards associated with IoT. Developing new access control standards and models that are compliant with those standards is inevitable for the success and sustainability of smart communities in the future. Moreover, with a decentralized access control architecture, compliance across smart devices, multiple clouds, communication protocols, and networking infrastructure to work collaboratively together is crucial to securely develop and deploy large connected smart communities.
- **Light-Weight** - IoT and smart technologies comprise of devices and edge gateways which are generally resource-constraint. Thus, the access control models and mechanisms need to be light-weight in order to be enforced on such IoT devices, gateways, and edge cloudlets. This requirement is more focused on the enforcement of access control mapping to enforcement layer of the PEI framework.
- **Privacy-Preserving** - In addition to securing authorizations in any domain, preserving user data privacy is also one of the requirements for secure access control models. With a large amount of data continuously being collected and shared within and across modular features, multiple components, and enabling infrastructure of smart communities, as shown in Figure 3, there is a need for privacy-preserving access control mechanisms or models. A privacy-preserving access control model should enable user-centric privacy approach where the user owns their data and information and can make decisions on how to share it only when required.

The light-weight and compliance requirements are focused on the enforcement layer, whereas other requirements are applicable to both policy models and enforcement models.

B. Access Control Principles for Next-Generation Smart Communities

Here we propose new and revised access control principles for next-generation smart communities that are inspired by the ASCAA principles discussed in Section 2, and defined based on the essential requirements of access control presented above.

- **Abstraction** - This principle is adopted from the ASCAA principles as it is applicable in the context of future smart communities. In this vast connected ecosystem, there are various components that have their own features and different types of access or authorization associated with them. For instance, in Figure 3, there is remote health and

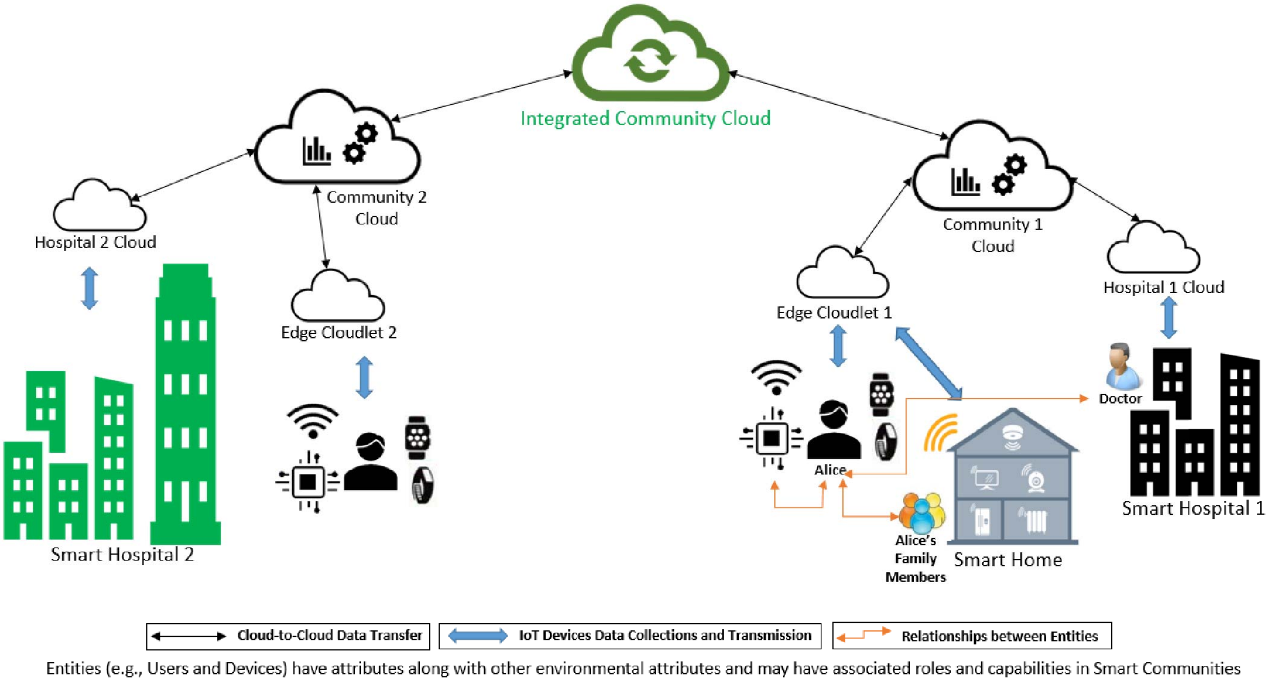
Integrated Community Cloud
Community 2 Cloud
Hospital 2 Cloud
Edge Cloudlet 2
Smart Hospital 2
Community 1 Cloud
Edge Cloudlet 1
Hospital 1 Cloud
Doctor
Alice
Alice's Family Members
Smart Home
Smart Hospital 1
Cloud-to-Cloud Data Transfer
IoT Devices Data Collections and Transmission
Relationships between Entities
Entities (e.g., Users and Devices) have attributes along with other environmental attributes and may have associated roles and capabilities in Smart Communities

Fig. 4. A Smart Community Use Case

a cooperative farm component with smart communities. However, access in each of these system domains is different with different types of entities and operations. To represent authorizations at high level in any of the smart communities, we need the abstraction principles to hide the implementation specific details. This principle directly aligns with the access control policy models at policy layer.

- **Dynamic Separation** - Dynamic Separation is revised from the ASCAA principles. In the context of smart communities, we define dynamic separation as the dynamic distinction between the operational access control and administrative access control mechanisms or models. Since there are many moving components in SCs, such as smart devices (e.g., connected autonomous cars, wearable devices, drones and uavs) and users who own and manage these devices, these users may behave as operational users or administrative users in different scenarios. For instance, a user using their wearable watch is an operational access control example, whereas the same user creating a virtual object or digital twin of that wearable device is an admin for the device at that point in time. Therefore, based on the context where devices, cloud services, and applications are being used in SCs, the access control models have to dynamically separate between the permissions available for that user or device.
- **Cooperation** - Smart communities are enabled by different connected components coming together as shown in Figure 3. There are various heterogeneous entities, devices, users, and their features in each component of SCs. To enable future SCs, we believe that various parties need to cooperate, collaborate, and work together based on pre-established or dynamic trust which demands cooperation among various access control mechanisms. The goal is to enable a secure access control architecture where one smart device in one component can access other devices in another component as needed. For example, devices connected to different shared cloud can communicate with each other without going to the always online cloud. This can also help preserve user data privacy by restricting the data within shared clouds with trusted parties and need not to share all data with the main cloud.
- **Delegation** - Delegation allows the users delegate permissions to other users and devices to act on their behalf. It is essential in a cooperative and fully autonomous environment where users will need to delegate their permissions to perform actions on their behalf based on preassigned trust on other users and devices.
- **Containment** - Containment incorporates basic access control principles, such as least privilege and need to know, and also the constraints specific to access control. It also adopted from ASCAA principles. While cooperation is an essential principle for collaborative SCs, it is also important to layout how the least privilege and constraint will be applied in SCs so that an attacker or malicious user cannot exploit the cooperation principle to cause harm to users, their data, and cooperative smart infrastructure, and launch cyber attacks.

- **Adaptability** - It is a new access control principle for rapidly evolving and growing smart communities. With new technological advancements in IoT, smart communities will change over time and so does its components, entities, and associated accesses and authorization. Thus, we propose an access control principle that accommodates and addresses any changes in the smart communities through this principle which allows to incorporate changes (add/remove entities, permissions, and access) in different components and entities, and their associated access and authorization.
- **Autonomous** - In the future SCs, the main goal is to have fully autonomous access control models that are once defined and implemented can be widely utilized. Similarly, autonomous access revocation works as well. This also aligns with the dynamic authorization principles.
- **Accountability** - This principle is essential to check and track who did what in a system. It is applicable in the context of the smart communities.

IV. Convergent Access Control Framework

A. A Smart Community Use Case

In order to discuss the need for a convergent access control framework for future connected smart communities, we present a use case scenario from the remote health component as shown in Figure 4. In this use case, there is a smart community with two sub-communities, community 1 and community 2 in different regions with these two sub-communities connected to the main community cloud. There is a user Alice who lives in smart community 1 in a smart home with her family members, and every user have their own wearable IoT devices. These IoT devices are connected to the edge cloudlets which eventually send data to the larger community 1 cloud. Smart hospital 1 has its own private cloud due to sensitive information being stored about the users. The unionized aggregate data which is not privacy-sensitive from the hospital cloud is sent to the community 1 cloud based on the requirements, which then is shared at the community cloud level. However, to ensure the users and their data are secured, access control and communication (data flow) policies in access control and communication control models, such as Attribute-Based Communication Control (ABCC) model [30] need to be defined that prohibit unauthorized access to users, their smart devices and data, edge cloudlets, and cloud services. Similar considerations apply to community 2.

This smart community comprises smart health and smart home domains that includes multiple users, things, objects, cloudlets, and cloud platforms. Users, devices, and objects are constantly in motion and connect to different networks, cloudlets, and cloud services based on the location and services needed to complete their tasks. In such a highly dynamic and distributed environment, access control and privacy requirements and features are continuously changing. Dynamic trust-based approaches including various access control features need to be considered in developing a secure access control framework for smart communities which also enables data privacy as an integral part of the access control model. In the above use case scenario, only one access control model (e.g., ABAC, RBAC, or ReBAC) would not be adequate. For example, users, devices, and objects can have attributes including environmental attributes, and also there can different types of relationships between users and their family members, relationships between users and devices (e.g., own a specific wearable IoT device) as shown in Figure 4. Moreover, roles can be assigned to users or devices based on the actions that they need to do, and also delegate access on other resources. Therefore, access control features from multiple access control models need to be combined and converged to address the access control needs of any application domains.

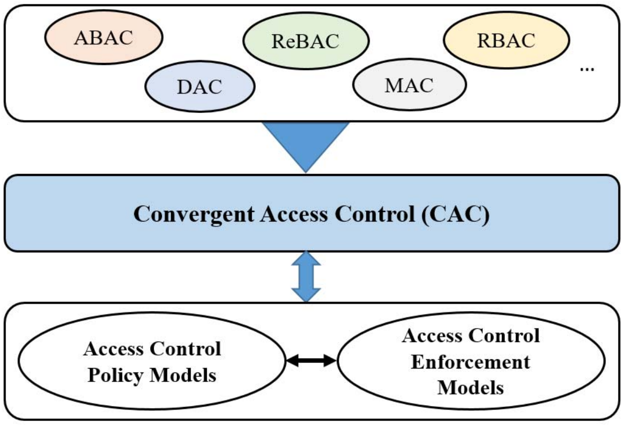
ABAC
ReBAC
RBAC
DAC
MAC
...
Convergent Access Control (CAC)
Access Control Policy Models
Access Control Enforcement Models

Fig. 5. The Convergent Access Control (CAC) Framework

Usually, different access control models for specific domains as IoT, Connected Vehicles, Wearable IoT, Cloud platforms are developed based on existing access control models, such as ABAC or RBAC. In order to capture all the entities, IoT applications, dynamic edge cloudlets, data communications, and cloud platforms and their access control aspects, we propose a convergent access control approach to converge the required access control features and develop a family of new access control models for specific application domains within the future smart communities.

B. Convergent Access Control for Smart Communities

With rapid advancements in IoT technologies and intelligent systems based on AI/ML, future smart connected communities, where users, smart devices and their digital twins (which are digital representations of physical devices), and applications across the world can communicate with each other, will soon become a reality. IoT comprises smart objects or things that are capable of autonomously gathering data and information from their surroundings and performing specific tasks. For example, a smart thermostat (e.g., Google NEST) can monitor your home temperature, while a smartwatch (e.g., Fitbit; Apple Watch) monitors your health and fitness. More recently, there has been a surge in IoT devices and IoT application developments that enable smart cities and smart communities.

These rapid developments in IoT space have created a climate that is ripe for studies devoted to rethinking and reevaluating current access control models. Moreover, by combining different promising access control models, for example, ABAC, RBAC, ReBAC, we can potentially develop a dynamic access control framework leveraging the benefits of different access control models.

Here, we propose a convergent access control (CAC) framework for addressing dynamic and new emerging access control requirements in future smart communities as discussed in Section 3. SCs include various application scenarios, for example, smart homes and neighborhoods, smart hospitals, smart universities, smart cities with smart infrastructure and utilities. Each of these above application scenarios have different types of entities (e.g., users, devices, and resources) with a set of attributes, and relationships between each other, along with different access control permissions associated with them. For example, in a smart home, the home owners have relationships with other users, such as spouse, and child, and each user can have their own attributes (e.g., age, location, etc.). Similarly, users and smart devices can have some relationships with each other (user-to-devices, devices-to-devices), and also devices can have a set of their attributes. All these features can be used towards determining authorizations in a smart home, for instance, a simple policy using attributes and relationships is as follows.

- *If a user is the home owner or have any relationship with the home owner, and age is greater than 18, and location is home, then allow access to a smart device in the home.*

This shows only one application scenario – smart home. There are several other application scenarios which would need to incorporate attributes, relationships, and probably other features, such as roles, capabilities, etc., from various access control models. Therefore, a convergence across existing access control models is needed to develop a family of next-generation access control models for future connected smart communities. Figure 5 shows our proposed convergent access control (CAC) conceptual framework.

Motivated by the smart healthcare use case in the context of smart communities, we propose a convergent access control (CAC) approach to address access control requirements in smart communities by converging promising access control models, such as ABAC, RBAC, and ReBAC to enhance security and privacy in distributed and dynamic application domains within smart communities. In such domains, both attributes of different entities, relationships between different entities, and other features must be captured to provide dynamic and fine-grained access control that can be adapted and enforced in a wide range of application domains, such as social IoT, smart home, smart communities with distributed cloud and edge computing, etc. The overarching goal of a convergent approach is to find a convergence between different access control models, and then develop a suitable access control policy model for an application domain, which can then be enforced through appropriate enforcement model. For example, at policy layer, attributes and relationships can together form an access control policy model for smart home. However, to enforce this model, we need an enforcement model for it which could be an RBAC enforcement model since it is a widely deployed model in most applications today. In this case, the attributes and relationships in policy model will be analyzed to determine equivalent roles for role-based enforcement model.

In this research, we envision and propose a convergent access control approach for address access control requirements of future smart communities. But, it is important to outline that developing a fully complete CAC framework needs significant research and work to find the best ways to combine different access control models based on the needs of the application domains, such as smart home, health, etc., and develop new access control models as per the requirements at policy layer and enforcement layer.

V. Discussion and Research Agenda

In this section, we present a discussion on the future research agenda for developing a convergence across different access control models and their capabilities for enabling secure smart communities. Here we discuss some specific research directions that need to be investigated to achieve our goal of developing the CAC framework.

- **Suitability of Access Control Models**: An interesting concept of evaluating the suitability of an access control model and system based on the application workload is discussed by Hinrichs et al. [31]. For developing most suitable and effective access control model for an application domain, further research on suitability analysis and evaluation of access control models and systems is needed. We envision suitability analysis as a part of the CAC framework to develop new access control models for specific applications and evaluate those models, especially in the context of various application domains within future smart communities.
- **Hybrid Access Control Models**: In literature, there is a trend to develop a new access control model for every new application domain based on some underlying access control model, such as ABAC, RBAC, CapBAC, or ReBAC. However, there is no consensus on how to develop these hybrid models that can be applied in real-world application domains. One of the objectives of CAC is to formalize the process of combining or converging different access control models.
- **AI-Enabled Strategies for Access Control**: Machine Learning models and AI strategies can be utilized to enhance access control models and develop more efficient and expressive access control models. There have already been some efforts on role-mining [32] for RBAC and attribute-mining for ABAC [33].
- **Access Control Evaluation Frameworks**: Evaluation of access control models have always been an interesting research question. Advanced access control evaluation

framework including qualitative and quantitative evaluation methods are still lacking and needs further research. These are some of the research directions presented here; however, ultimately significant research effort from multidisciplinary researchers and subject matter experts from different application domains, IoT security, secure CPS areas and researchers from access control models community is necessitous.

VI. Conclusion

In this paper, we presented the essential requirements of access control models in the context of future smart communities. We also presented new and revised some of the existing access control principles for enabling future connected communities. Towards enabling secure smart communities in the future, we propose a convergent access control approach towards addressing the authorization and privacy requirements in such communities. Our vision is to develop a Convergent Access Control (CAC) framework; however, significant research on different aspects of this framework is needed as we presented in the discussion and research agenda.

VII. Acknowledgments

This work is partially supported by NSF CREST Grant HRD1736209 and the Texas A&M System Chancellor Research Initiative (CRI) Grant.

References

[1] S. Bhatt, F. Patwa, and R. Sandhu, "An access control framework for cloud-enabled wearable Internet of Things," in *2017 IEEE 3rd International Conference on Collaboration and Internet Computing (CIC)*. IEEE, 2017, pp. 328–338.

[2] "Smart Community Services to Enable Better, Faster, Cheaper," https://sngroup.com/smart-city-services/.

[3] F. Xia and J. Ma, "Building smart communities with cyber-physical systems," in *Proceedings of 1st international symposium on From digital footprints to social and community intelligence*, 2011, pp. 1–6.

[4] 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.

[5] 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.

[6] R. Sandhu and V. Year, "The ASCAA principles for next-generation role-based access control," *Engineer*, vol. 1, p. E1, 2008.

[7] R. Sandhu, "The PEI framework for application-centric security," in *2009 5th International Conference on Collaborative Computing: Networking, Applications and Worksharing*. IEEE, 2009, pp. 1–5.

[8] R. Sandhu and Q. Munawer, "How to do discretionary access control using roles," in *Proceedings of the third ACM workshop on Role-based access control*, 1998, pp. 47–54.

[9] R. K. Thomas, R. S. Sandhu *et al.*, "Discretionary access control in object-oriented databases: Issues and research directions," in *Proc. 16th National Computer Security Conference*, 1993, pp. 63–74.

[10] R. S. Sandhu, "Lattice-based access control models," *Computer*, vol. 26, no. 11, pp. 9–19, 1993.

[11] 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.

[12] X. Jin, R. Krishnan, and R. Sandhu, "A unified attribute-based access control model covering DAC, MAC and RBAC," in *IFIP Annual Conference on Data and Applications Security and Privacy*. Springer, 2012, pp. 41–55.

[13] E. Yuan and J. Tong, "Attributed based access control (ABAC) for web services," in *IEEE International Conference on Web Services (ICWS'05)*. IEEE, 2005.

[14] B. Tang and R. Sandhu, "Extending OpenStack Access Control with Domain Trust," in *International Conference on Network and System Security*. Springer, 2014, pp. 54–69.

[15] S. Bhatt, F. Patwa, and R. Sandhu, "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, 2016, pp. 37–45.

[16] A. Alshehri and R. Sandhu, "Access Control Models for Virtual Object Communication in Cloud-Enabled IoT," in *International Conference on Information Reuse and Integration (IRI), IEEE*. IEEE, 2017, pp. 16–25.

[17] S. Bhatt, F. Patwa, and R. Sandhu, "ABAC with group attributes and attribute hierarchies utilizing the policy machine," in *Proceedings of the 2nd ACM Workshop on Attribute-Based Access Control*. ACM, 2017, pp. 17–28.

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

[19] M. Gupta, F. Patwa, and R. Sandhu, "An attribute-based access control model for secure big data processing in hadoop ecosystem," in *Proceedings of the Third ACM Workshop on Attribute-Based Access Control*. ACM, 2018, pp. 13–24.

[20] Y. Cheng, J. Park, and R. Sandhu, "Attribute-Aware Relationship-Based Access Control for Online Social Networks," in *IFIP Annual Conference on Data and Applications Security and Privacy*. Springer, 2014, pp. 292–306.

[21] D. He, S. Chan, Y. Qiao, and N. Guizani, "Imminent communication security for smart communities," *IEEE Communications Magazine*, vol. 56, no. 1, pp. 99–103, 2018.

[22] S. Aggarwal, R. Chaudhary, G. S. Aujla, N. Kumar, K.-K. R. Choo, and A. Y. Zomaya, "Blockchain for smart communities: Applications, challenges and opportunities," *Journal of Network and Computer Applications*, vol. 144, pp. 13–48, 2019.

[23] Z. Su, Y. Wang, Q. Xu, M. Fei, Y.-C. Tian, and N. Zhang, "A secure charging scheme for electric vehicles with smart communities in energy blockchain," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4601–4613, 2018.

[24] "AWS IoT Platform," http://docs.amazon.com/iot/, accessed: 2020-1-08.

[25] "Azure IoT," https://azure.microsoft.com/en-us/overview/iot/, accessed: 2020-08-15.

[26] "Google Internet of Things," https://cloud.google.com/solutions/iot-overview/, accessed: 2019-12-10.

[27] "IBM Cloud," https://www.ibm.com/cloud.

[28] M. Gupta, J. Benson, F. Patwa, and R. Sandhu, "Secure v2v and v2i communication in intelligent transportation using cloudlets," *arXiv preprint arXiv:2001.04041*, 2020.

[29] M. Gupta, M. Abdelsalam, S. Khorsandroo, and S. Mittal, "Security and privacy in smart farming: Challenges and opportunities," *IEEE Access*, vol. 8, pp. 34 564–34 584, 2020.

[30] S. Bhatt and R. Sandhu, "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*, 2020, pp. 203–212.

[31] T. L. Hinrichs, W. C. Garrison III, J. C. Mitchell, and A. J. Lee, "Application-sensitive access control evaluation: Logical foundations (extended version)," *University of Pittsburgh Department of Computer Science, Tech. Rep. TR-12-185*, 2011.

[32] J. Vaidya, V. Atluri, and Q. Guo, "The role mining problem: finding a minimal descriptive set of roles," in *Proceedings of the 12th ACM symposium on Access control models and technologies*, 2007, pp. 175–184.

[33] Z. Xu and S. D. Stoller, "Mining attribute-based access control policies from logs," in *IFIP Annual Conference on Data and Applications Security and Privacy*. Springer, 2014, pp. 276–291.