Authorizations in Cloud-Based Internet of Things: Current Trends and Use Cases

Smriti Bhatt[1], Lo'ai A. Tawalbeh[1] (IEEE Senior Member), Pankaj Chhetri[2], Paras Bhatt[3]
[1]Department of Computing and Cyber Security,
Texas A&M University-San Antonio, TX, 78224, USA
[2]Department of Electrical and Computer Engineering,
[3]Department of Computer Science,
Prairie View A&M University, Prairie View, TX, 77446, USA
Email: sbhatt@tamusa.edu, Ltawalbeh@tamusa.edu, pachhetri@pvamu.edu, paras.bhatta18@gmail.com

***Abstract*—With the advancement of the Internet and technology, the Internet of Things (IoT) has gained significant momentum in recent years. There is rapid growth in the number of smart IoT devices and IoT applications. These devices and applications primarily gather, store, and share user data. However, the IoT devices have limited resources, such as storage, power, and computation. Cloud Computing enables IoT to leverage its unlimited capabilities, such as storage, computation, and analytics. Today, Cloud and IoT have become parallels and move together to form a Cloud-Enabled IoT architecture. This diverse and dynamic Cloud-IoT architecture, where IoT devices connect and disconnect on the fly and share data for analysis and computation with the Cloud raises many security and privacy concerns and broadens the attack surface. For example, in a government organization with high security and data privacy risk, there has to be a secure access control mechanism in place to ensure authorized access to data and resources. In this paper, we discuss the state-of-art of authorization mechanisms in Cloud-Enabled IoT architecture. We present two use cases – A Smart Home use case, and A Smart University Parking use case, to discuss various access control and authorization requirements in Cloud-Based IoT. We then propose an Attribute-Based Access Control (ABAC), a flexible access control approach, to address these access control requirements in the Cloud-Based IoT architecture, mainly in the context of presented use cases.**

Keywords-Authorization; Access Control; Attributes; Internet of Things; Attribute-Based Approach;

I. INTRODUCTION

The recent trends in communication and Internet industry brought to the users end many technology-enabled services such as: paying invoices, flights reservations, socializing with others, location determination, Online shopping, and healthcare services [1]. Moreover, the Internet of Things (IoT) has become a part of people's life which provides convenience in their day-to-day task. Many IoT devices, applications, and platforms are being introduced in the commercial industry. Most of these platforms are provided by different vendors and service providers which have their customized standards and mechanisms [2]. However, IoT devices are resource constraint and leverage the Cloud Computing capabilities for storage, computation, and analysis [3]. There are various Cloud Enabled IoT applications that include: Smart Home, Internet of Vehicles (IoV), Sports and fitness, and Healthcare applications [4]. Mostly, the IoT applications are running on mobile devics with huge amount of data being stored in the Cloud. Mobile Cloud Computing (MCC) is helpful especially in providing Edge computing in IoT where real-time processing is necessary, and the results are needed in the shortest amount of time possible [5].

With the uncontrolled growth of IoT devices, applications, and platforms there is critical security and privacy risk to IoT data continuously generated, consumed, and disseminated within this broad and dynamic Cloud-Based or Cloud-Enabled IoT architecture. However, there is a lack of a unified mechanism to address specific access and authorization issues in IoT. A secure authorization mechanism ensures only authorized entities (users, devices, etc.) can get access to data and resources, and at the same time defends against unauthorized access requests. Security and privacy of data and information is the primary concern in IoT. A promising approach to address security and privacy concerns in IoT is to develop secure access control and authorization mechanisms. Currently, the access control models for IoT have been developed based on few popular models in the industry, such as Role-based Access Control (RBAC) [6, 7] and Capability-Based Access Control (CapBAC) [8]. A flexible access control model that has recently gained significant attention in academia is Attribute-Based Access Control (ABAC) [9, 10] where permissions are determined based on attributes (properties) of users (or subjects) and objects. Despite the development of numerous access control models for IoT, there is no consensus on a standard formal access control model or a uniform authorization mechanism for Cloud-Based IoT. A diverse range of industry players in the IoT space makes it even more challenging to develop a standard or unified access control/authorization model.

In this paper, we investigate the current state-of-art of authorization mechanisms and discuss some of the relevant security risks and vulnerabilities in the context of Cloud-Enabled IoT architectures. We specifically discuss the access control and authorization challenges involved in achieving a fully secured Cloud-IoT platform. One of the predominant challenges is to develop a flexible and fine-grained access control model for IoT to prevent unauthorized access to IoT

data and devices. To address this challenge, we propose an Attribute-Based Access Control (ABAC) model to secure a Cloud-Based IoT architecture. We present two Cloud-Based IoT use cases – *A Smart Home*, and *A Smart University Parking System,* and discuss access control and authorization requirements in these two IoT domains. We illustrate the use cases from an ABAC perspective and identify attributes for its components to demonstrate the applicability of ABAC model in Cloud-Enabled IoT. For example, in a smart home, there are several devices, such as a smart light and a light sensor, and these devices and the home users can have a set of attributes defined which identify the authorizations for each of these entities. A detailed description and analysis of the use cases are presented in Section III.

The rest of the paper is organized as follows. In Section II, we present a brief background on Cloud and Mobile Cloud computing and IoT architectures. In Section III, we discuss some of the existing access control models and the ABAC model for Cloud-Enabled IoT and present two Cloud-Enabled IoT use cases – A Smart Home and A Smart University system. Section VI discusses IoT data security challenges and possible future directions. Finally, in Section V we conclude this paper.

II. BACKGROUND

In this section, we briefly discuss relevant background on Cloud/Mobile Cloud Computing and IoT architectures. The evolution of IoT converges from the development of wireless technologies, micro-controllers and micro-electromechanical systems (MEMS), machine-to-machine technologies, and the Internet. IPv6 is another factor to support the evolution of IoT with large Internet addressing space [11]. With advancements in IPv6, billions of smart object can be uniquely identified in the virtual space. IoT is continuously evolving with "anything" and "everything" being connected to the Internet. IoT things are becoming smarter with the support of technologies like Cloud Computing, Mobile Computing, Artificial Intelligence (AI), Big Data Analytics, and Machine learning. According to the Gartner hype cycle for emerging technologies, as of July of 2017, the IoT platforms are towards the peak and are expected to reach the plateau within the next two to five years [12]. Moreover, the number of connected devices is growing exponentially and has been estimated to reach more than 20 billion devices by 2020 [13].

Besides the classical cloud computing models presented in the literature, there are more efficient architectures that were proposed to enhance the performance of Cloud/Mobile Cloud Computing environments. A revision of the concept of Mobile cloud computing, its characteristics, and applications was presented in [14]. The work in [15] presented a survey for the current approaches and trends in cloud computing and Mobile Cloud Computing based on the different parameters including performance and delay.

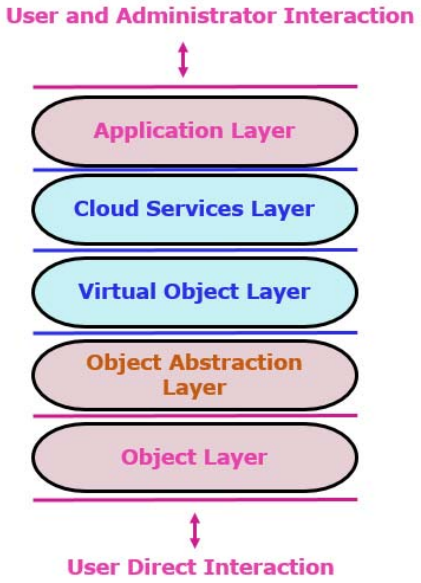

Figure 1. Enhanced ACO Architecture for Cloud-Enabled IoT [2]

One main challenge facing the cloud computing research is the costly implementation of the cloud environments. The work in [16] presents an overview of the simulation tools used to simulate the cloud and mobile cloud environments stating the advantages and disadvantages of each one. The authors in [17] presented techniques to mitigate the insider threats in Fog computing and cloud computing. The authors in [18] proposed a trust delegation mobile cloud computing model to secure the user's data. Moreover, the main challenge of securing the data during transmission and especially over mobile networks (wireless) was addressed in [19]. Other work proposed the implementaitons of secure crypto algorithms in hardware to provide the sutiable level of data encryption accoridng to the sensitivity of these data being processed and transmitted. For more detials the reader is referred to [20, 21].

In the literature, the developments in IoT has been maintained based on several IoT architectures. A basic IoT architecture is generally comprised of three layers: *i) object or perception layer* where the devices and physical objects are present, ii) one or more *middleware layer(s)* where virtual objects (digital counterpart of physical objects) and Service-Oriented Architecture (SOA) management services and Cloud services are present, and iii) *an application layer* which is the top layer of the architecture and comprises users and administrators who can directly access the IoT applications [22]. An Access Control Oriented (ACO) architecture for Cloud-Enabled IoT with four layers has been presented in [22].

Figure 1 shows the Enhanced ACO (EACO) architecture. The Object layer comprises physical IoT devices with which the users interact directly. These devices collect data from users and surrounding environments and move the data forward to subsequent upper layers in the architecture. The *Object Abstraction* layer provides an abstraction between the heterogeneous physical devices and their respective virtual objects. This layer acts as the first access control point for

physical IoT devices and provides an authorization and privacy interface between the object layer and other layers in EACO. It comprises gateway devices, which have better storage and computation resources than physical IoT devices, such as sensors and actuators. The *Virtual Object* layer consists of virtual objects, which are digital representations of physical objects. The *Cloud Services* layer includes all the cloud services (e.g., compute, storage, and network services) which store data and perform data analytics. Access control and authorization policies are defined in the cloud services and are enforced at different layers. The fourth layer, *Application* layer provides meaningful insights to the users with the help of IoT data analytics and visualization techniques. Other similar layered IoT architectures have been presented in [23, 24].

III. ABAC IN CLOUD-ENABLED IOT

In this section, we first discuss some of the previously published and current access control models for IoT. We then present two Cloud-Enabled IoT use cases and discuss their access control and authorization requirements. In addition, we depict the attribute-based access control approach to address the access control requirements and secure the Cloud-Enabled IoT architecture.

A. Access Control Models for Internet of Things (IoT)

Currently, Cloud-Enabled IoT platforms employ some customized form of access control models, i.e., RBAC model where permissions (read, write, publish, subscribe, etc.) are defined based on predefined *roles* which can be assigned to different entities, such as users and IoT devices. However, the role-based approach by itself is inadequate to address the dynamic requirements of Cloud-Based IoT. In today's commercial Cloud-Based IoT platforms, the authorization mechanisms are based on some customized role-based approach where access control policies are coupled with cryptographic certificates (e.g., X.509 certificates) and keys, which are in turn, associated with specific IoT things/entities. A formal access control model for AWS IoT platform, a real-world Cloud-based IoT architecture, has been developed in [25]. This model is known as AWS-IoTAC and is developed based on an extended from AWS Cloud Access Control (AWSAC) [26] model. The authors also proposed some Attribute-based access control (ABAC) enhancements for the AWS-IoTAC model for more fine-grained access control policies for IoT.

Besides, there are several other access control models, which have been developed by different researchers in academia. In a comprehensive survey by Ouaddah et al. [27], the authors have presented a detailed analysis of several access control models for IoT. IoT access control models are mainly based on CapBAC models [28, 29] and Role-based access control (RBAC). An RBAC model for IoT has been proposed in [30] and a combination of two access control model – RBAC and ABAC, known as ARBHAC model is proposed by Sun et al. in [31]. This model utilizes attributes of users to assign roles to the users instead of determining authorizations for users on objects. Similarly, some of the other hybrid models combining RBAC and ABAC, and ABAC with groups and group attributes have been developed in [32, 33].

B. Use Cases

- ***A Smart Home Use Case***

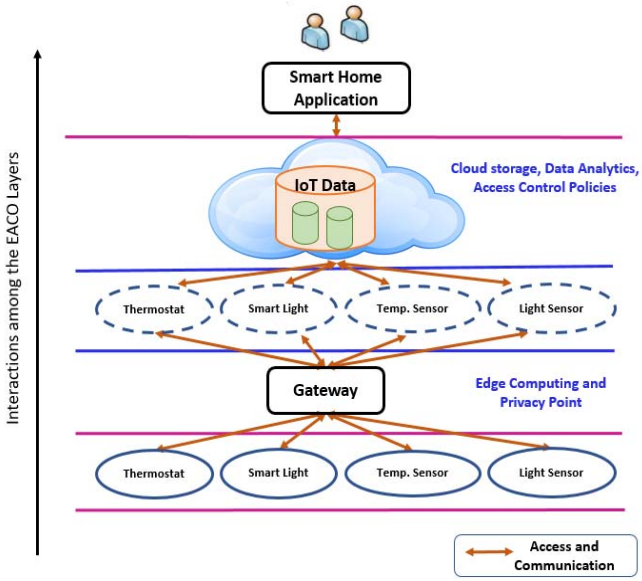

Figure 2. A Smart Home in EACO Layers

In Figure 2, a Smart home use case is represented within the EACO architecture. Each layer of the architecture represents different components of the use case. In the object layer, there are physical devices – *a thermostat, a smart light, a light sensor*, and *a temperature sensor*. In the object abstraction layer, there is a *gateway*, which authenticates the devices and enables communication with other layers in the architecture. It acts as the access control and privacy point for the devices and data and provides Edge computing capabilities. The virtual objects for each object (IoT device) are present in the virtual object layer represented as dashed circles. The data is stored in the Cloud services layer which also hosts the authorization policies and enables data analytics. IoT applications utilize the data collected from IoT devices and present it to the users to provide meaningful insights and predictive analysis. The arrows between these layers represent accesses and communications between these layers. These IoT devices need to communicate securely with each other to perform their tasks. With so many access points, such as physical devices and gateway, an attacker can break into the IoT network through some weak security-enabled device or a device with weak access control and authorization policy. Therefore, there is a need for a flexible access control approach, which can ensure security and privacy of users and IoT devices and resources in Cloud-Enabled IoT architecture.

In this use case, for secure authorization ABAC approach can be applied where different entities are assigned attributes and based on the attributes specific authorizations on these entities are allowed or denied. An attribute is a name and value pair, where the name is attribute name which can hold a set of

values defined in its range of values. In general, a simple example of attributes is the *age* of the user and the *location* of a device or a user. In ABAC, IoT devices, services, and applications have their own set of attributes with specific values. These attributes can hold different types of values, such as *age* will hold numbers and *location* will hold a set of strings. Then, the authorization can be assigned based on these attributes for different users and devices. For example, if the user is requesting access to a device, then the attributes of the user and the device need to comply with the defined authorization policy to allow access to the device. An example policy would be if the user requesting access to a device is the *owner* of the device and the *location* of the user is at home, then this user would be allowed access to the device to do some operation, such as turn on/turn off. Generally, in ABAC, an access control policy needs to be defined for specific authorizations. These authorization policies are defined as predicate logic expressions and if the expression is evaluated to be true, then the access will be granted, otherwise, denied. Similarly, devices can request access to other devices for sending or receiving messages.

In Figure 2, the IoT devices can have a set of attributes, such as *typeOfDevice* whose range of values is {Sensor, Actuator}, *ownerOfDevice* whose range of values is residents in the home, and *manufacturer* which represents the manufacturer of the device. Similarly, the home users can have attributes, such as *houseRole* which has values {Owner, Spouse, Child, Guest}, and *location* of the user. For a thermostat, the *typeOfDevice* = {Actuator}, *ownerOfDevice* = {Owner, Spouse}, and *manufacturer* = {NEST}, and for a smart light *typeOfDevice* = {Actuator}, *ownerOfDevice* = {Owner, Spouse, Child}, and *manufacturer* = {NEST}. Whereas, the light sensor has *typeOfDevice* = {Sensor}, *ownerOfDevice* = {Owner, Spouse, Child}, and *manufacturer* = {NEST}, and Temp. sensor has *typeOfDevice* = {Sensor}, *ownerOfDevice* = {Owner, Spouse, Child}, and *manufacturer* = {NEST}. Further, we can design more detailed attributes where it identifies the *typeOfSensor* with a range of values {light, temp}. A hierarchical relationship between attributes can also exist based on the nature of the use case. A detailed hierarchical relationship between attributes is presented in [32]. Similarly, the users in a Smart home, such as the Owner, Spouse, Child, and Guest would get their values assigned based on their roles and location. Typically, an administrator who also specifies a set of attribute-based access control policies using users and devices attributes defines the attributes and their range of values. In a Smart home scenario, the administrator who sets the policy would be the owner of the house or the spouse of the owner. Besides users and devices attributes, there are other contextual attributes, which could be considered in access control decisions. One example is *timeOfDay* which represents at what time of the day the access is requested and is authorized based on the policy involving this attribute. In ABAC, unlike any other access control model such as RBAC or CapBAC, the attributes determine the authorizations for different users (or subjects) on the objects. This provides a flexible access control and fine-grained authorization mechanism based on ABAC authorization policies for the dynamic Cloud-Based IoT architecture.

- ***A Smart University System***

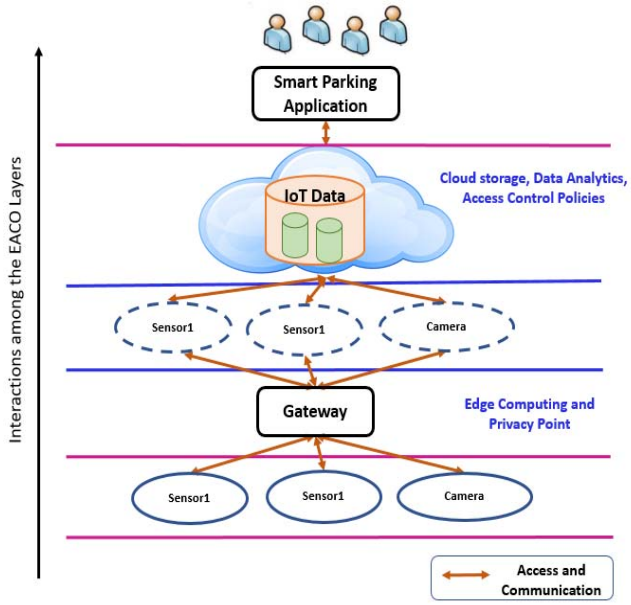

Figure 3. A Smart University Parking System in EACO Layers

Now, we present another Cloud-based IoT use case, i.e., *A Smart University parking system* adapted from [33][34] where a set of IoT sensors gather parking availability data and send it to the Cloud. The Cloud services then process the data and perform data analytics to provide information to the users through applications, for example, a smartphone application. If the parking is available, then the users are notified and will be to obtain information on available parking spots in various parking lots. This smart parking system eventually saves a lot of time for the university users, such as faculty, staff, and students, which is instead wasted, for finding an available parking spot.

In Figure 3, a smart university parking system is presented in the context of the EACO architecture. In the object layer, there are two sensors – *Sensor1* and *Sensor2,* and a C*amera*. In a real scenario, there would be numerous sensors and cameras to track numerous cars and parking spots. These sensors would gather data on the availability of the parking spots and the cameras monitor the flow of traffic in the parking lots during the day. The data is sent through the gateway and the virtual objects to the Cloud where computation and analytics are performed to provide meaningful insights and predictive analytics to the users on peak parking hours. The data is presented to the users through IoT applications where users can set preferences for the required information [35][36].

Similar to the previous use case, the sensors and cameras can have a set of attributes assigned by the administrator, such as *typeOfDevice, manufacturer.* The *ownerOfDevice* attribute

does not fit in this scenario though since the owner would be the university that owns the parking space. Therefore, depending on the use case the set of attributes change for IoT devices and other entities as well.

For instance, in this use case, the user roles are different, such as student, faculty, staff, and visitor and based on these roles the information about the available parking spots will change since there are specific spots only for students or only for faculty. At the same time, ABAC authorization policies also change. For example, a visitor should not be allowed to park in the parking spots reserved for the faculty. These use cases present the applicability and effectiveness of the attribute-based access control and authorization mechanism in a real-world Cloud-Enabled IoT architecture. In this research, we discuss and present the conceptual use cases on how ABAC can be applied in Cloud-Based IoT platforms. For the practical implementation of these use cases, we plan to utilize the AWS Cloud-IoT platform and extend our work into concrete prototypes by designing detailed use case components and defining their attributes and ABAC authorization policies.

IV. Discussion and Future Research Directions

In this paper, we discussed authorizations in Cloud-Based IoT environment involving smart IoT devices, users, and Cloud services and applications. However, there is a huge amount of data continuously being generated and shared by these IoT devices. In some of the IoT domains, security and privacy of data is the primary concern. For instance, in a Smart healthcare use case, where user data and information is highly privacy-sensitive, the Cloud-Based IoT architecture raises critical data security and privacy issues. In this architecture, the data is hosted in the Cloud, which comprises data from individual devices, data aggregated from different sources, and metadata related to IoT entities [22]. With these different types of IoT data, there are various data security and privacy issues, which need to be addressed with further research in the Cloud-Based/Cloud-Enabled IoT architecture.

Figure 4, presents three main IoT data security and privacy challenges, i.e., *Data Security, Data Ownership,* and *Data Privacy and Sharing,* which are discussed below.

- **Data Security:** In the Cloud-Enabled IoT architecture, it is critical to secure user data and devices data. Data access control models need to be developed for securing static data stored at different points, physical devices, gateway, and Cloud, as well as data in motion flowing between different components in the architecture.
- **Data Ownership:** Another critical aspect of IoT data is data ownership. Who actually owns the data? Users, devices, or Cloud service providers, or IoT applications. To address the data ownership concern, it is important to identify different sources and consumers of IoT data, which will then allow to define the data ownership relation between IoT entities and data.

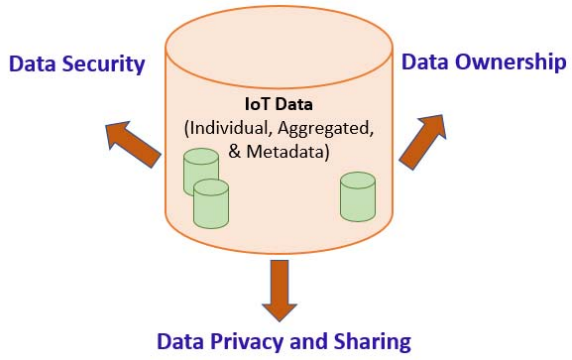

Figure 4. IoT Data Security and Privacy Challenges

- **Data Privacy and Sharing:**
  The IoT data is gathered from several physical devices, such as sensors or wearable devices. This data is then shared among several entities physical devices, gateway, and multiple Cloud services. Data privacy is an inevitable challenge to be addressed in IoT for its continued success in the ever-growing connected world.

These are some of the possible future research directions for IoT data security and privacy in Cloud-Based IoT architecture.

V. Conclusion

In this paper, we presented the authorization mechanisms in two Cloud-Enabled IoT use cases and depicted that ABAC provides a secure and dynamic authorization mechanism for Cloud-Enabled IoT architecture. On the other hand, current authorization mechanisms are based on role-based or policy-based approach where policies are assigned to users, resources, and devices. These roles and policies once defined and assigned to specific entities are difficult to manage and may result in numerous roles and policies which arises the problem of role-explosion and policy-explosion. Therefore, ABAC is a promising approach to address access control and authorization requirements in a dynamic Cloud-Enabled IoT environment. In future work, we plan to implement our use cases in a real-world Cloud-IoT platform and also investigate future directions discussed above to develop data access control and authorization models.

Acknowldgment: This research is supported by Texas A&M University-San Antonio through Research Council Grants.

References

[1] Lo'ai, A. Tawalbeh, and Waseem Bakhader. "A Mobile Cloud System for Different Useful Applications." In *4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, pp. 295-298. IEEE, 2016.

[2] Bhatt, Smriti, Farhan Patwa, and Ravi Sandhu. "An Access Control Framework for Cloud-Enabled Wearable Internet of Things." In *3rd IEEE International Conference on Collaboration and Internet Computing (CIC), 2017*, pp. 328-338. IEEE, 2017.

[3] Huang, Dijiang, and Huijun Wu. "Mobile Cloud Computing: Foundations and Service Models". Morgan Kaufmann, 2017.

[4] Lo'ai, A. Tawalbeh, Waseem Bakhader, Rashid Mehmood, and Houbing Song. "Cloudlet-based mobile cloud computing for

healthcare applications." In 2016 IEEE Global Communications Conference (GLOBECOM), pp. 1-6. IEEE, 2016.

[5] Ibrahim, Shadi, Hai Jin, Bin Cheng, Haijun Cao, Song Wu, and Li Qi. "Cloudlet: Towards Mapreduce Implementation on Virtual Machines." In *Proceedings of the 18th ACM International Symposium on High Performance Distributed Computing*, pp. 65-66. ACM, 2009.

[6] 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.

[7] Ferraiolo, David F., Ravi Sandhu, Serban Gavrila, D. Richard Kuhn, and Ramaswamy Chandramouli. "Proposed NIST Standard for Role-Based Access Control." *ACM Transactions on Information and System Security (TISSEC)* 4, no. 3 (2001): 224-274.

[8] Hernández-Ramos, José L., Antonio J. Jara, Leandro Marin, and Antonio F. Skarmeta. "Distributed Capability-Based Access Control for the Internet of Things." *Journal of Internet Services and Information Security (JISIS)* 3, no. 3/4 (2013): 1-16.

[9] Jin, Xin, Ram Krishnan, and Ravi Sandhu. "A Unified Attribute-Based Access Control Model Covering DAC, MAC and RBAC." In *IFIP Annual Conference on Data and Applications Security and Privacy*, pp. 41-55. Springer, Berlin, Heidelberg, 2012.

[10] Hu, Vincent C., David Ferraiolo, Rick Kuhn, Arthur R. Friedman, Alan J. Lang, Margaret M. Cogdell, Adam Schnitzer, Kenneth Sandlin, Robert Miller, and Karen Scarfone. "Guide to Attribute Based Access Control (ABAC) Definition and Considerations (draft)." *NIST Special Publication*800, no. 162 (2013).

[11] "Internet of Things (IoT)." http://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT. Accessed 10/12/2017.

[12] "Top Trends in the Gartner Hype Cycle for Emerging Technologies, 2017." Accessed 10/15/2017.

[13] "Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015." https://www.gartner.com/newsroom/id/3165317. Accessed 10/12/2017.

[14] Tawalbeh, Lo'ai, Norah Alassaf, Waseem Bakheder, and Alaa Tawalbeh. "Resilience mobile cloud computing: features, applications and challenges." In 2015 Fifth International Conference on e-Learning (econf), pp. 280-284. IEEE, 2015..

[15] Fernando, Niroshinie, Seng W. Loke, and Wenny Rahayu. "Mobile Cloud Computing: A Survey." *Future Generation Computer Systems* 29, no. 1 (2013): 84-106.

[16] Bahwaireth, Khadijah, Elhadi Benkhelifa, Yaser Jararweh, and Mohammad A. Tawalbeh. "Experimental Comparison of Simulation Tools for Efficient Cloud and Mobile Cloud Computing Applications." *EURASIP Journal on Information Security* 2016, no. 1 (2016): 15.

[17] Stolfo, Salvatore J., Malek Ben Salem, and Angelos D. Keromytis. "Fog computing: Mitigating insider data theft attacks in the cloud." In 2012 IEEE symposium on security and privacy workshops, pp. 125-128. IEEE, 2012.

[18] Tawalbeh, Lo'ai A., Fadi Ababneh, Yaser Jararweh, and Fahd AlDosari. "Trust delegation-based secure mobile cloud computing framework." International Journal of Information and Computer Security 9, no. 1-2 (2017): 36-48.

[19] Moh'd, Abidalrahman, Nauman Aslam, Hosein Marzi, and L. A. Tawalbeh. "Hardware implementations of secure hashing functions on FPGAs for WSNs." In Proceedings of the 3rd international conference on the applications of digital information and web technologies (ICADIWT). 2010.

[20] Tawalbeh, Lo'ai, Alexandre Tenca, Song Park, and Cetin Koc. "An efficient hardware architecture of a scalable elliptic curve crypto-processor over GF (2 n)." In Advanced Signal Processing Algorithms, Architectures, and Implementations XV, vol. 5910, p. 59100Q. International Society for Optics and Photonics, 2005

[21] Mohammad, Abidalrahman, and Adnan Abdul-Aziz Gutub. "Efficient FPGA implementation of a programmable architecture for GF (p) elliptic curve crypto computations. " Journal of Signal Processing Systems 59, no. 3 (2010): 233-244.

[22] Alshehri, Asma, and Ravi Sandhu. "Access Control Models for Cloud-Enabled Internet of Things: A Proposed Architecture and Research Agenda." In *2016 IEEE 2nd International Conference on Collaboration and Internet Computing (CIC)*, pp. 530-538. IEEE, 2016.

[23] Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The Internet of Things: A Survey." *Computer Networks* 54, no. 15 (2010): 2787-2805.

[24] Gubbi, Jayavardhana, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions." *Future Generation Computer Systems* 29, no. 7 (2013): 1645-1660.

[25] Bhatt, Smriti, Farhan Patwa, and Ravi Sandhu. "Access Control Model for AWS Internet of Things." In *International Conference on Network and System Security*, pp. 721-736. Springer, Cham, 2017.

[26] Zhang, Yun, Farhan Patwa, and Ravi Sandhu. "Community-Based Secure Information and Resource Sharing in AWS Public Cloud." In *IEEE Conference on Collaboration and Internet Computing (CIC)*, 2015, pp. 46-53., 2015.

[27] Ouaddah, Aafaf, Hajar Mousannif, Anas Abou Elkalam, and Abdellah Ait Ouahman. "Access Control in the Internet of Things: Big Challenges and New Opportunities." *Computer Networks* 112 (2017): 237-262.

[28] Gusmeroli, Sergio, Salvatore Piccione, and Domenico Rotondi. "A Capability-Based Security Approach to Manage Access Control in the Internet of Things." *Mathematical and Computer Modelling* 58, no. 5 (2013): 1189-1205.

[29] Mahalle, Parikshit N., Bayu Anggorojati, Neeli Rashmi Prasad, and Ramjee Prasad. "Identity Establishment and Capability Based Access Control (IECAC) Scheme for Internet of Things." In *15th International Symposium on Wireless Personal Multimedia Communications (WPMC),* 2012, pp. 187-191. IEEE, 2012.

[30] Liu, Jing, Yang Xiao, and CL Philip Chen. "Authentication and Access Control in the Internet of Things." In *32nd International Conference on Distributed Computing Systems Workshops (ICDCSW)*, pp. 588-592. IEEE, 2012.

[31] Kaiwen, Sun, and Yin Lihua. "Attribute-Role-Based Hybrid Access Control in the Internet of Things." In *Asia-Pacific Web Conference*, pp. 333-343. Springer, Cham, 2014.

[32] Bhatt, Smriti, Farhan Patwa, and Ravi Sandhu. "ABAC with Group Attributes and Attribute Hierarchies Utilizing the Policy Machine." In *Proceedings of the 2nd ACM Workshop on Attribute-Based Access Control*, pp. 17-28. ACM, 2017.

[33] Bhatt, Smriti, Farhan Patwa, and Ravi Sandhu. "An Attribute-Based Access Control Extension for OpenStack and its Enforcement Utilizing the Policy Machine." In *2nd International Conference on Collaboration and Internet Computing (CIC)*, pp. 37-45. IEEE, 2016.

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

[35] Pankaj Chhetri, Cajetan M. Akujuobi, Matthew N. O. Sadiku, Smriti Bhatt, Paras Bhatt, "Wavelet Applications to the Internet of Things: A Smart Parking System." *In Journal of Scientific and Engineering Research*, 2018, 5(11):80-89.

[36] Aloqaily, Moayad, Safa Otoum, Ismaeel Al Ridhawi, and Yaser Jararweh. "An intrusion detection system for connected vehicles in smart cities." Ad Hoc Networks (2019).