Internet of Things (IOT) Based Access Control

Neeraj Kaushik
Department of Electronics and Communication Engineering
Faculty of Engineering, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India

ABSTRACT: The Internet of Things (IoT) is the extension of the internet to the real world where all objects collect information and communicate with their environments without human interference or with nothing. Unauthorized users gain access to users property is one of the bigger challenge nowadays. Therefore providing protection and privacy and access to user's property is the main focus of this paper. They collect and pass important, privately held data from various users. That puts security and privacy problems at the forefront: the ability to handle millions of people's digital identities and billions of devices is key to success. Since most of the information in the IoT setting can be personal or confidential information, there is a need to maintain anonymity and limit access to information. This article will concentrate on mechanisms for access control and authentication, as well as supporting the algorithms for cryptography in restricted devices.

KEYWORDS: IoT; Access Control; Cryptography; Security; Smart Object; Internet; Access.

INTRODUCTION

In the last few years, IoT has been one of the 21st century's most important innovations. Now that everyday objects — kitchen appliances, vehicles, thermostats, baby monitors — can be linked to the internet through embedded devices, seamless communication between people, processes, and stuff is possible [1]. With minimal human interference, physical objects can communicate and collect data through low-cost computing, the cloud, big data, analytics, and mobile technologies. Digital systems can capture, track and change any interaction between the connected things in this hyper connected world. The real world is facing the digital world-and they are cooperating [2].

While the concept of IoT has been in existence for a long time, it has become practical through a series of recent developments in a variety of different technologies.

- Connect to cheap, low-power sensor technology. The inexpensive and reliable sensors allow more manufacturers to use IoT technology.
- Connecting. A host of Internet network protocols have made it easy for efficient data transmission to link sensors to the cloud and to other "things."
- Plateforms in cloud computing. The growth in cloud platform availability enables companies as well as customers to access the resources they need to scale up without necessarily needing to handle it all.
- Learning by software and analytics. Businesses can gain information faster and easier with advancements in machine learning and analytics, along with access to diverse and large volumes of data stored in the cloud. The advent of these allied technologies continues to move IoT's limits, and IoT's data often feeds those technologies.
- Artificial Conversational Intelligence (AI). Advances in neural networks have introduced natural-language processing (NLP) to IoT devices (such as Alexa, Cortana, and Siri's automated personal assistants) and made them appealing, accessible, and feasible for home usage.

IoT and cloud computing integration would not only improve the performance and security aspects of the current application scenario but would also allow the creation of creative future applications. Smart cards are portable hardware, used to store user's hidden information. These are used in various applications including personal identification to ensure consumer integrity, online banking, education, and much more. They provide remote access control, accessibility support and with the ability to update several functionalities. This can be used to integrate with other technologies, such as the Single Sign-On (SSO) system, access control policies, etc., to exploit multiple cloud-based services and safe communication between users and devices in the distributed network environment [3].

But, for users to access cloud-based services and data, they need to go through the network and communication system that is vulnerable to a variety of malicious attacks like eavesdropping, man-in-the-middle (MITM) attacks, replay attacks, forgery, Denial of Service (DoS). Users are also vulnerable to attacks by masquerading and tracing identities. Therefore, end machines used to access these services are resource limited and are not adequately capable of enforcing the protection protocols by themselves. To mitigate these attacks and ensure privacy of the identity of the user, it is important to build a lightweight authentication system with efficient computations to allow access to multiple services with identical credentials. We propose in this paper a smart card authentication system using identity-based access control mechanism to gain access to multiple distributed cloud services in a resource-bound IoT environment. SSO definition is used to allow access to several Cloud services without the need to hold separate passwords for each. Nowadays there are a multitude of models of access control that are applied to various Internet of Things scenarios where protection is required. Below is a brief overview of the most common models that are deployed in these scenarios.

In the Compulsory Access Control (MAC) model-1, the system administrator gives permissions to the object that is subject to access. The model assigns subjects and artifacts to security labels, and it is independent of user operations, only the administrator can change object security labels. MAC models are difficult and expensive to introduce and maintain, their use is typically restricted to military applications and thus MAC models are not used as an access control system. Users retain access to resources in the Discretionary Access Control (DAC) models2, which can grant permissions to their resources by being included in the Access Control Lists (ACL). Each entry in the access control list gives permissions for users (or groups of subjects) to access resources. Objects usually store the permissions. Unlike in MAC, where permissions are given by the administrator in predefined rules, in DAC, permissions are given by users who decide the access rights to the resources that belong to them. Present UNIX, FreeBSD, and Windows operating systems implement the DAC.

In addition, users are delegated to positions in the Role-Based Access Control (RBAC) model3, and the security policies grant roles rather than users privileges. Since the functions are connected to the users. RBAC allows the development of permissions and inheritance hierarchies. However, given the administrative problems of large structures where memberships make administration potentially inefficient, RBAC does have some problems. Traditional models of access control such as MAC, DAC and RBAC do not accept additional parameters such as resource information and complex information (such as time, location). The Attribute-Based Access Control (ABAC) model4 was proposed to provide a more versatile framework, in which authorization decisions are based on attributes that the user must prove (e.g.: age, place, positions, etc.). One of ABAC's key benefits is that requesters do not need to be identified a priori by targets, offering a higher degree of open system versatility compared to RBAC models [4].

The Authorization-Based Access Control (ZBAC) five model uses credentials for authorization, which are provided along with a request to make a decision on access control. Unlike ABAC and RBAC systems, in which the user submits an authentication with the request for service, the user submits an authorization with the request in ZBAC systems. IoT situations place major constraints on privacy and access control, with conventional approaches to access management solutions not planned with these aspects.

LITERATURE REVIEW

In this paper we are proposing a new IoT access control architecture based on the block chain technology. Our first contribution is to provide a standard of reference for our proposed architecture within the IoT definition of Objectives, Requirements, Design and Mechanism. We also implement Fair Access as a completely decentralized pseudonymous and privacy system preserving authorization management that enables users to own and monitor their data. We use and adapt the block chain to integrate our concept into a decentralized Access Control Manager. In comparison to financial bitcoin transactions, Fair Access implements new types of transactions which are used to request, receive, delegate and cancel accesses [1]. This paper offers a detailed state-of-the-art analysis of various IoT access control solutions in the Goals, Models, Design, and Mechanisms (OM-AM) way.

An overview of the protection and privacy specifications is being performed for the most dominant IoT technology areas, including Personal and Home, Government and services, and Enterprise and business. It discusses the pros and cons of conventional models and protocols, as well as recent access control models from an IoT perspective [2]. This paper promotes the concept of Sustainable and Linked Communities SCC which emerges from the smart cities concept. The SCC is intended to tackle synergistically the needs of remembrance of the past (preservation and revitalization), the needs of living in the present (livability), and the needs of future planning (accessibility). Consequently, SCC's mission is to improve a community's livability, sustainability, revitalisation, and attainability. The goal of creating a community's SCC is to live in the present, prepare for the future and remember the past [3].

The Internet of Things (IoT) is characterized by heterogeneous technologies that are compatible with the delivery of creative services in diverse fields of operation. Satisfying the protection and privacy criteria plays a critical role in this situation. These specifications include data protection and authentication, IoT network access control, user and stuff privacy and trust, and enforcement of security and privacy policies. Because of the various requirements and communication stacks involved, conventional security countermeasures cannot be applied directly to the IoT technologies [4]. This paper provides a thorough overview of evolving and developing technology with a emphasis on 5 G mobile networks to facilitate the rapid growth of traffic and enable IoT. Also posed in developing an effective context-aware congestion management system are the challenges and open research directions relevant to the deployment of massive to critical IoT applications [5]. Within this paper, we discuss a number of common and groundbreaking IoT solutions within terms of context-aware perspectives on technology. More specifically, we are testing these IoT approaches using a framework we have developed around well-known context-aware theories of computing. This survey is intended to serve as a guideline and conceptual structure for the creation and study of context-aware products in the IoT paradigm. It also offers a comprehensive review of current on the marketplace IoT products and identifies a range of potentially important directions and developments in study [6]. This study explores the key developments in IoT access control and provides detailed analyzes of current IoT-specific authorizations systems.

Guided by the needs of representative IoT applications and key IoT specifications, we are raising the main specifications that IoT authorization frameworks should meet along with their evaluation criteria. Such standards and specifications form a basic foundation for our study of literature. Based on this report, we define the key open issues in the field of IoT access control and draw guidelines for potential investigations [7]. This paper discusses a crucial problem of access control within the Internet of Things (IoT). In particular, we are proposing a smart contract-based architecture, consisting of multiple access control contracts (ACCs), one judge contract (JC), and one register contract (RC), to achieve centralized and trustworthy access control for IoT systems. Every ACC provides one access control method for a subject-object pair and, by testing the subject's actions, implements both static access right validation based on predefined policies and dynamic access right validation.

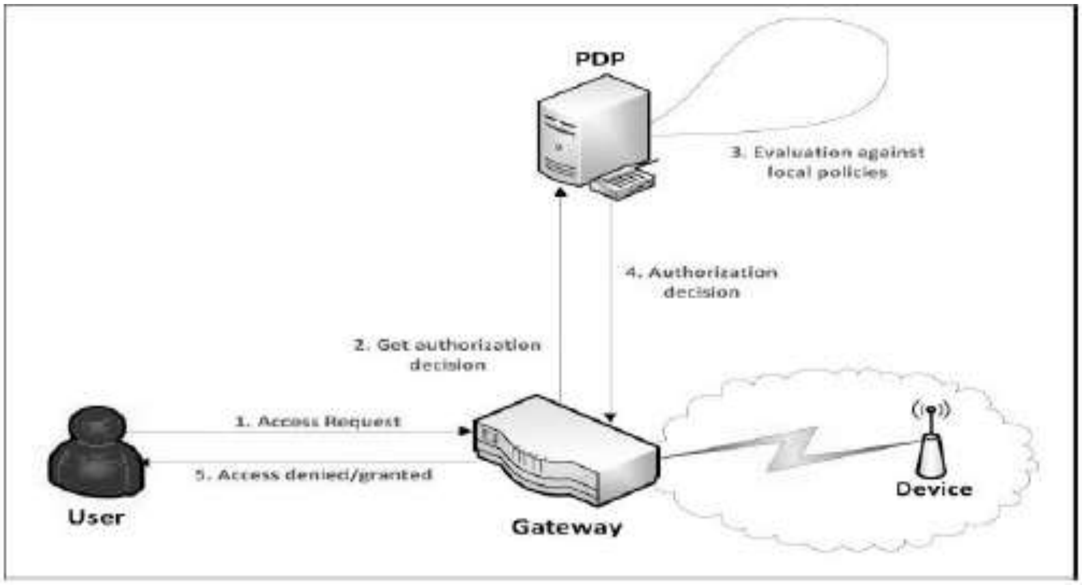
PDP
3. Evaluation against local policies
4. Authorization decision
2. Get authorization decision
1. Access Request
5. Access denied/granted
User
Gateway
Device

FIGURE. 1. Centralized approach.

METHODOLOGY

Centralized approach

All access control logic is outsourced in a centralized approach into a single agency responsible for handling access requests based on their authorization policies. As information providers the end tools play a minimal role. This centralized approach does not take into account resource constraints, since the principle of access control is situated within an organization without resource constraints. This method is conveyed via a scenario where a server receives a request from the mobile user who wishes to access the end computer, thereby creating a token containing the permission or refusal and sending it to the mobile user. The method, however, has major problems. Next, in decisions on access control, the end-device is not taken into account. Second, the access control logic is housed in one agency, and any failure may jeopardize the entire system as it is a single fault point.

Hybrid approach

End-devices are not passive actors, they participate in decisions on access control as shown in Figure 2. In this method, a server receives a request from the mobile user who wishes to access the end device, analyses the contextual information received by the end device and then decides to allow or deny access, so it produces a token containing the permission or rejection and sends it to the mobile user. This strategy also has a problem with the capacity of the end-devices to take contextual knowledge into account at the exact time of decision taking. Consequently, the information loses its significance in the authorization decision process [8].

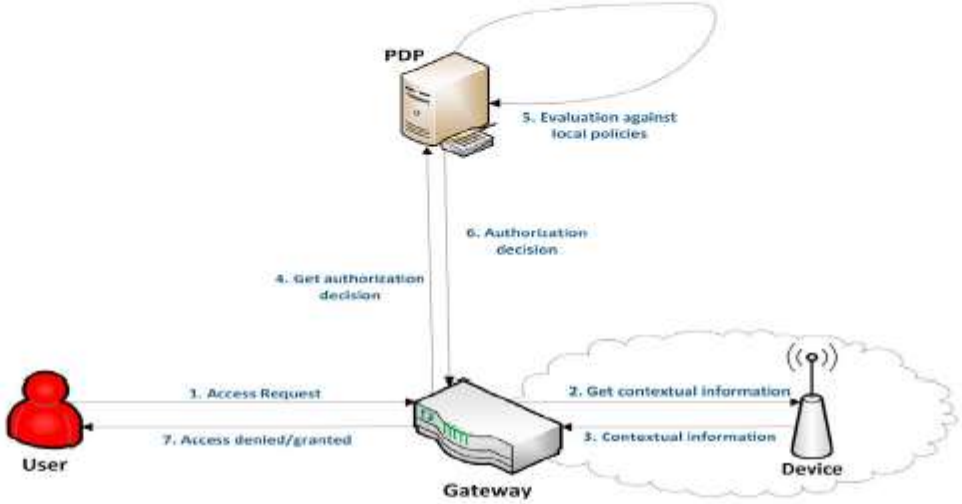
PDP
5. Evaluation against local policies
6. Authorization decision
4. Get authorization decision
1. Access Request
7. Access denied/granted
User
Gateway
2. Get contextual information
3. Contextual information
Device

FIGURE. 2. Hybrid approach.

Distributed approach

The end-device in the distributed architectures6 is a smart thing that allows process to be accessed and information to be sent to other services and devices. The apps will take decisions on authorizations without the need for central authorities. This approach offers interesting features, and is more suitable for IoT's scenarios and architectures [9].

CAPACITY-BASED ACCESS CONTROL ARCHITECTURE

Also in the presence of devices with resource constraints, DCapBAC was postulated as a feasible method to deploy on IoT scenarios. The core concept of this approach is the ability definition that was originally defined by9 as "card, ticket, or core that enables the owner to access an individual or object in a computer system." Typically this token is composed by a collection of rights given to the person that owns the token. In CapBAC, an entity that wants to access some information from another entity demands that the request be submitted along with a token. Thus, the person receiving the capacity already knows the permissions that were given to the requester when the request is to be processed. It simplifies the authorization process and is an essential feature not needed in situations with resource-constrained devices and complex access control policies.

Process

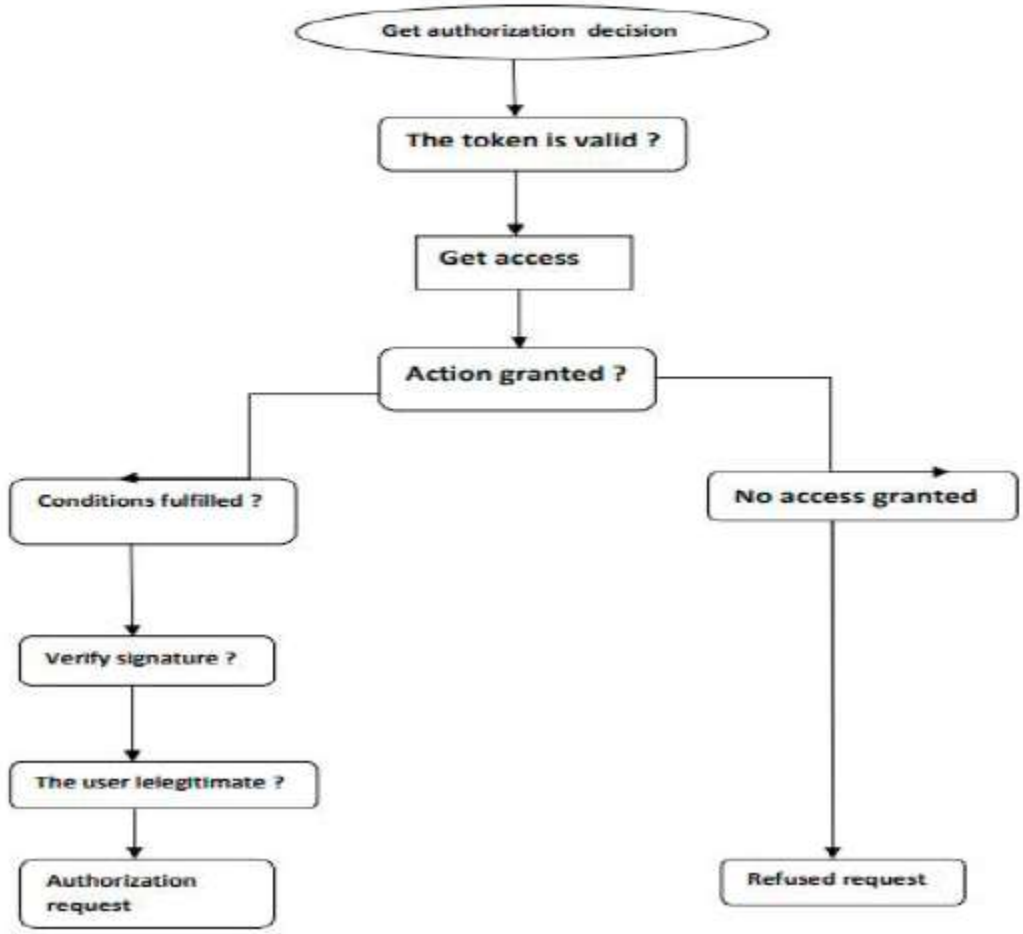

FIGURE 3: Process flow

CONCLUSION

This article dealt with the CapBAC model proposed as a feasible solution to IoT scenarios7 and is supported by restricted tools. This approach is based on the capability principle set out in6,8. This token contains the rights which the person that owns the token would be given. To be accepted in a real world, this token must be tamper-proof and unmistakably marked. In addition, a cryptographic system must be in place that is supported even by the restricted tools. In IoT environments and emerging technology health is a challenge. This design takes into consideration the constraints of smart objects in terms of storage, energy usage and time for execution.

REFERENCES

[1] A. Ouaddah, H. Mousannif, A. Abou Elkalam, and A. Ait Ouahman, “Access control in the Internet of Things: Big challenges and new opportunities,” *Computer Networks*. 2017, doi: 10.1016/j.comnet.2016.11.007.

[2] A. Ouaddah, A. Abou Elkalam, and A. Ait Ouahman, “FairAccess: a new Blockchain-based access control framework for the Internet of Things,” *Secur. Commun. Networks*, 2016, doi: 10.1002/sec.1748.

[3] Y. Sun, H. Song, A. J. Jara, and R. Bie, “Internet of Things and Big Data Analytics for Smart and Connected Communities,” *IEEE Access*, 2016, doi: 10.1109/ACCESS.2016.2529723.

[4] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, “Security, privacy and trust in

Internet of things: The road ahead," *Computer Networks*. 2015, doi: 10.1016/j.comnet.2014.11.008.

[5] G. A. Akpakwu, B. J. Silva, G. P. Hancke, and A. M. Abu-Mahfouz, "A Survey on 5G Networks for the Internet of Things: Communication Technologies and Challenges," *IEEE Access*. 2017, doi: 10.1109/ACCESS.2017.2779844.

[6] C. Perera, C. H. Liu, S. Jayawardena, and M. Chen, "A Survey on Internet of Things from Industrial Market Perspective," *IEEE Access*, 2015, doi: 10.1109/ACCESS.2015.2389854.

[7] M. W. Condry and C. B. Nelson, "Using Smart Edge IoT Devices for Safer, Rapid Response with Industry IoT Control Operations," *Proc. IEEE*, 2016, doi: 10.1109/JPROC.2015.2513672.

[8] V. C. Hu, D. R. Kuhn, and D. F. Ferraiolo, "Attribute-based access control," *Computer (Long. Beach. Calif).*, 2015, doi: 10.1109/MC.2015.33.

[9] D. Di Francesco Maesa, P. Mori, and L. Ricci, "Blockchain based access control," 2017, doi: 10.1007/978-3-319-59665-5_15.