International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 3 | ISSN : 2456-3307

Access Control Framework for API Enabled Devices

Vandana C. P, Taffazul Imam, Shubham Dubey, Suman Thapa, Pradip Thapa

Department of Information Science Engineering, New Horizon College of Engineering, Bangalore, Karnataka, India

ABSTRACT

The recent advances in information and communication technologies brought about a novel paradigm, Internet of Things (IoT), in which a variety of devices in the physical world are connected to the Internet. The security cannot be disregarded from the employment of API-enabled devices because the impact of the security breach in these devices tends to be larger, as it directly affects the physical environment we live in. If an unauthorized user is able to access API-enabled devices in smart buildings, it may harm an occupant's life for instance by locking a door, turning off lights or air conditioners, which make occupants, lose their comfortable and so on. In this paper, an access control framework for API-enabled devices in smart buildings is implemented.

Keywords : Internet of Things, API, Authentication Manager and Access Control Manager, Access Control Manager, MICROCONTROLLER, IDE, XML, SOAP, RFID, AVR

I. INTRODUCTION

Devices are nowadays increasingly inter-connected to each other and to Internet. These devices are vulnerable to the attacks and the data theft. To accommodate the dynamic environment in smart building the security manager is deployed as a trusted third party in the system that acts as a perfect bodyguard against unauthorized users.To support scalability and efficiency the security manager is split into **Authentication Manager and Access Control Manager**.

II. WORKING

After a device received a request from users, the device is forced to ask Access Control Manager to evaluate the received request. The access control manager evaluates the request based on the access control policies, which are composed by the Administrator in advance. In order to investigate the feasibility of the proposed framework, we implemented the security framework in our smart building systems, which the device API has been implemented. Our analysis results indicate that our framework is adequate to enforce security for API-enabled devices in smart buildings. Experimental results showed that our framework is feasible to be practically used in smart buildings.

III. EXISTING SYSTEM

The existing system were not that advanced enough to provide extra security features we evaluated some limitations in existing system:-

LIMITATIONS

- Authentication process is not addressed.
- Access control process not properly addressed.
- Insufficient measures to provide security measures to api devices.
- Security, scalability, and performance of the proposed mechanism is not evaluated.
- Physical world like the heterogeneity of devices, dynamic environment not addressed

IV. PROPOSED SYSTEM

The previous works mainly focused on integrating context information to Access control model and managing access control on heterogeneous protocol

devices, whereas the addressing of enforcing security for API-enabled devices are still lacking.
The goal of our work is to provide an access control framework, which deals with the heterogeneity of devices and the dynamic environment in smart buildings.

To enforce security for API-enabled devices, security manager has two main functions:

1. To verify that a subject is the valid user of the system and
2. To assign an access permission of the resource,

To improve the efficiency of the system we split the security manager into two components, Authentication Manager, and Access Control Manager. Moreover, by splitting the security manager our framework supports the scalability of systems.

Authentication Manager

The main purpose of the authentication manager is to verify the user. Users send credentials information as a request parameter. After the user is verified, they are given the permissions. The permission may be guest, owner, admin.Different user have different rights and permissions. Access control of the devices are based on the permissions provide to the user by the authentication manager.

Access Control Manager

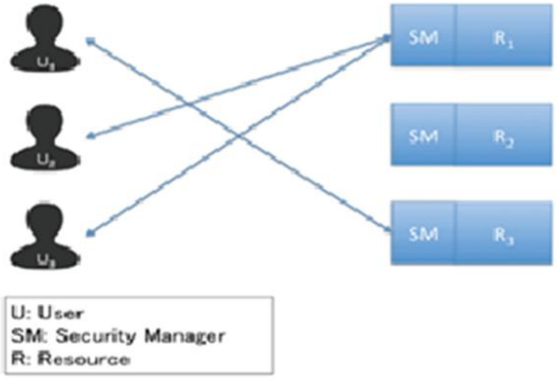
The main responsibility of access control manager is to handle the right of users and restrict access to resources. In the smart building with the large number of resources and users, we need an access control, which is able to deal with these complex conditions. Since the resources in smart building may not belong to one owner, we also need the authorization decision, which based on both attributes of resources and users.

In our system, user will request the access to the resources which will be authenticated by authentication manager and access is given by the access control manager based on the policies and restrict the access of the other resources.

FRAMEWORK FOR SECURITY

There are two kinds of conventional frameworks for enforcing security to resources:

In-situ Security Framework and Proxy Security Framework



FRAMEWORK FOR SECURITY

There are two kinds of conventional frameworks for enforcing security to resources:

In-situ Security Framework and Proxy Security Framework

The In-situ security framework is implemented by deploying a security manager in resource side. This approach has been popular in-home appliances by secured them with a password or a key. A user, which tends to access device, has to attach a key or a password. Each invocation from a user is evaluated by the security manager, which is implemented in the device.

And another is Proxy Security framework.

The proxy security framework is implemented by placing a security manager between user and resource. In this approach, the security manager accepts and checks every invocation that is requested by users. This kind of framework is widely used in web technology.

V. SYSTEM ANALYSIS AND REQUIREMENT

SOFTWARE USED

✓ ARDUINO IDE

The Arduino project provides the Arduino integrated development environment (IDE), which is a cross-platform application written in the programming language Java. It originated from the IDE for the languages Processing and Wiring. The Arduino IDE supports the languages C and C++ using special rules of code structuring. The Arduino IDE supplies a software library from the Wiring project, which provides many common input and output procedures.

✓ EMBEDDED C

Embedded C is a set of language extensions for the C Programming Language by the C Standards committee. Embedded C uses most of the syntax and semantics of standard C e.g., main () function, variable definition, datatype declaration, conditional statements (if, switch case), loops (while, for), functions, arrays and strings, structures and union, bit operations, macros,etc

✓ C# APPLICATION

C# (pronounced "C-sharp") is an object-oriented programming language from Microsoft that aims to combine the computing power of C++ with the programming ease of Visual Basics. C# is based on C++ and contains features similar to those of Java. C# is designed to work with Microsoft's .net platform. . C# simplifies programming through its use of Extensible Markup Language (XML) and Simple Object Access Protocol (SOAP) which allow access to a programming object or method without requiring the programmer to write additional code for each step

✓ ASP.NET FOR SERVER SIDE SCRIPTING

ASP.NET is an open-source server side web application framework designed for web development to produce dynamic web pages. It was developed by Microsoft to allow programmers to build dynamic web sites, web applications and web services. ASP.NET's successor is ASP.NET core. It is a re-implementation of ASP.NET as a modular web framework, together with other frameworks like Entity Framework.

HARDWARE

i. MICROCONTROLLER UNIT

The ATmega328P provides the following features: 32K bytes of In- System Programmable Flash with Read-While-Write capabilities. ATmega328P is a powerful microcontroller that provides a highly flexible and cost-effective solution to many embedded control applications. The ATmega328P AVR is supported with a full suite of program and system development tools including: C Compilers, Macro Assemblers, Program Debugger/Simulators, In-Circuit Emulators, and Evaluation kits.

ii. LCD DISPLAY

LCD (Liquid Crystal Display) screen is an electronic display module and found a wide range of applications. A 16x2 LCD display is very basic module and is very commonly used in various devices and circuits and also display,we can display two lines with maximum of 16 characters in one line.

iii. 4-CHANNEL RELAY UNIT

The board uses high quality relays, which can handle a maximum of 7A/240 V AC or 7A/24V DC. Each relay has all three connections - Common, Normally Open, Normally Closed brought out to 3 pin screw terminals which makes it easy to make and remove connections. The board has a power indication and a relay status LED to ease debugging. The board can accept inputs within a wide range of voltages from 4V to 12V.

iv. USB-to-TTL CABLE

Single-chip USB to Serial (RS232/RS422/RS485) asynchronous serial data transfer interface With Fully Compliant with USB Specification v2.0 (Full-Speed) Integrated USB 1.1 Transceiver and 5V to 3.3V Regulator provides good support for data transfer.

v. RFID READER

A Radio Frequency Identification Reader (RFID reader) is a device used to gather information from an RFID tag, which is used to track individual objects. Radio waves are used to transfer data from the tag to a reader. RFID is a technology similar in theory to bar codes.These RFID tag must be within the range of an RFID reader, which ranges from 3 to 300 feet, to be read.

vi. RFID TAGS

A radio-frequency identification system uses tags, or labels attached to the objects to be identified. Two-way

radio transmitter-receivers called interrogators or readers send a signal to the tag and read its response.

RFID tags can be either passive, active or battery-assisted passive. RFID tags contain at least two parts: an integrated circuit for storing and processing information, modulating and demodulating a radio-frequency (RF) signal, collecting DC power from the incident reader signal, and other specialized functions; and an antenna for receiving and transmitting the signal.

vii. 4 LOADS

Going through the effectiveness of the framework we implemented 4 loads i.e pair of bulb and pair of fan so that we would provide various access polices in these devices.

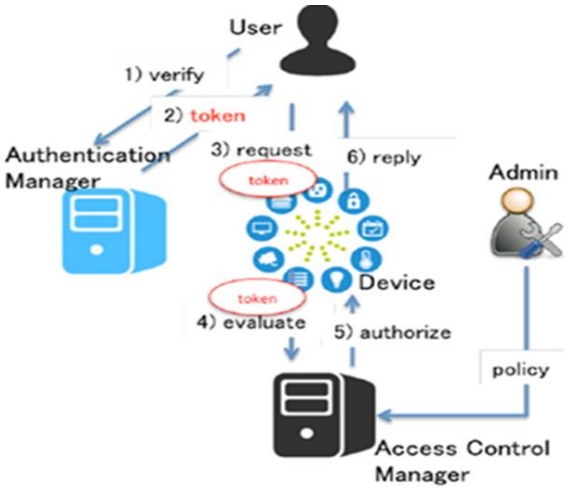
viii. TRANSFORMER UNIT

Transformer generally helps to regulate the voltage and since our device doesn't need that much of voltage or power supply we used step-down transformer so that we could reach our device requirements.

VI. SYSTEM ARCHITECTURE

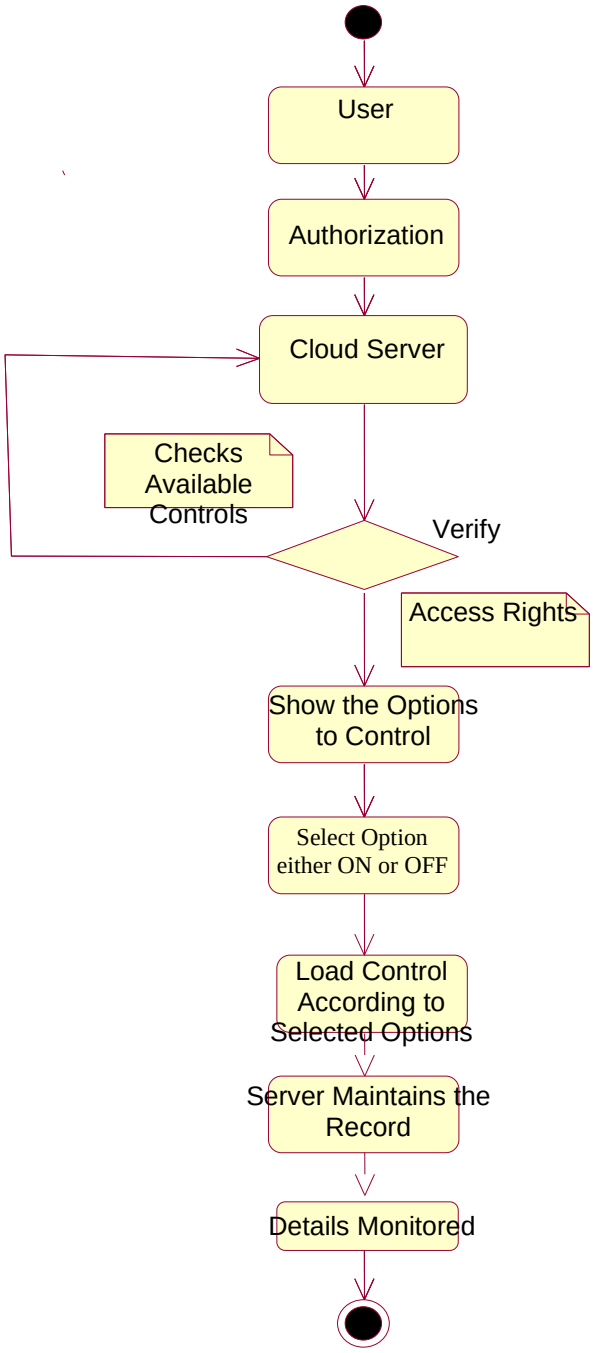
A system architecture or systems architecture is the conceptual model that defines the structure, behavior, and more views of a system. An architecture description is a formal description and representation of a system, organized in a way that supports reasoning about the structures and behaviors of the system.

A system architecture can comprise system components, the externally visible properties of those components, the relationships (e.g. the behavior) between them. It can provide a plan from which products can be procured, and systems developed, that will work together to implement the overall system. There have been efforts to formalize languages to describe system architecture, collectively these are called architecture description languages (ADLs).



ACTIVITY DIAGRAM

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. In the Unified Modeling Language, activity diagrams are intended to model both computational and organizational processes i.e. workflow.



TESTING

Testing is defined as the process of validating if the final system developed, meets the specified requirements or not. It involves the execution of software components in order to check if it responds correctly to the given inputs and performs functions within the expected time. The two-fundamental testing is component testing and system testing. Component testing tests the individual components in order to test the whole system to check the functional and non-functional requirements.

There are several testing steps involved before the product is given to the user acceptance test. They are:

- Unit testing
- Integration testing
- System testing
- User acceptance testing

We have successfully gone through these testing.

VII. CONCLUSION

After. we implemented the proposed framework in the real building environment. Through the analysis, we showed that the proposed framework is capable of enforcing security in smart environments. To evaluate the performance of the implementation, we also conducted several scenarios of experiments. From the measurement both client side and server side, the result showed that our proposed framework is feasible to be practically used in real smart buildings.

VIII. REFERENCES

[1]. Access Control Framework for API-Enabled Devices in Smart Buildings Syafril Bandara, Takeshi Yashiro, Noboru Koshizuka and Ken Sakamura

[2]. L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Computer networks, vol. 54, no. 15, pp. 2787–2805, 2010.

[3]. C. Lee, L. Zappaterra, K. Choi, and H.-A. Choi, "Securing smart home: Technologies, security challenges, and security requirements," in Communications and Network Security (CNS), 2014 IEEE Conference on. IEEE, 2014, pp. 67–72.

[4]. J. Al-Muhtadi, A. Ranganathan, R. Campbell, and M. D. Mickunas, "A flexible, privacy-preserving authentication framework for ubiquitous computing environments," in Distributed Computing Systems Workshops, 2002. Proceedings. 22nd International Conference on. IEEE, 2002, pp. 771–776.

[5]. H. Wang, Y. Zhang, and J. Cao, "Access control management for ubiquitous computing," Future Generation Computer Systems, vol. 24, no. 8, pp. 870–878, 2008.

[6]. K. Fysarakis, C. Konstantourakis, K. Rantos, C. Manifavas, and I. Papaefstathiou, "Wsacd-a usable access control framework for smart home devices," in Information Security Theory and Practice. Springer, 2015, pp. 120–133.

[7]. J. E. Kim, G. Boulos, J. Yackovich, T. Barth, C. Beckel, and D. Mosse, "Seamless integration of heterogeneous devices and access control in smart homes," in Intelligent Environments (IE), 2012 8th International Conference on. IEEE, 2012, pp. 206–213.

[8]. S. Cirani, M. Picone, P. Gonizzi, L. Veltri, and G. Ferrari, "Iot-oas: An oauth-based authorization service architecture for secure services in iot scenarios," Sensors Journal, IEEE, vol. 15, no. 2, pp. 1224–1234, 2015.

[9]. S. W. Oh and H. S. Kim, "Study on access permission control for the web of things," in Advanced Communication Technology (ICACT), 2015 17th International Conference on. IEEE, 2015, pp. 574–580.