ISSN 2250-3153

Home Automation: Access Control for IoT Devices

Rahul Godha*, Sneh Prateek, Nikhita Kataria**

* Cisco Systems, Bangalore, India
** Akamai Technologies, Bangalore, India

Abstract- This paper introduces access control for home automation devices for Internet of Things (IoTs), which offers capabilities to identify and connect many physical sensors into a unified secure system. As a part of IoTs, serious concerns are raised over access of personal and global information pertaining to devices and individual privacy. This research talks about how different devices can be applied different access polices on it.

Index Terms- Access Control, Internet of Things (IoT), Security, Threats.

1. INTRODUCTION

The Internet of Things can be described as connecting everyday objects like mobile phones, smart watches, electronic tablets, sensors and actuators to the Internet where the devices are intelligently linked together enabling various ways to communicate between things and peoples, and between things themselves. With the rapid development of Internet and communications technology, our lives are gradually led into a virtual dimension of augmented reality. People can chat, work, talk and interact via connected objects. However, human beings live in a real world, human activities cannot be fully implemented through the services in the virtual worlds.

Building IoTs has advanced significantly in the last couple of years since it has added a new dimension to the world of communication technologies. According to[2], it is expected that the number of devices connected to the Internet will increase from 100.4 million in 2011 to 2.1 billion by the year 2021, growing at a rate of 36% per year. In the year 2011, 80% machine to machine (M2M) connections were made over mobile networks such as 2G and 3G and it is predicted that by 2021, this ratio will increase to 93% since the cost related with M2M over mobile networks are generally cheaper than fixed networks.

Based on a large number of low-cost sensors and wireless communication, the sensor network technology brings new demands to the communication technology. It can change the way we live, work and play. Apart from benefits of IoTs, there are several security and privacy concerns that needs to be addressed to build a private and secure home.

This journal consists of 6 general sections. These are:
1) Abstract
2) Introduction
3) Security and Privacy Concerns in IoT,
4) Authentication Mechanism
5) Proposed Solution and Research
6) Conclusions

2. SECURITY AND PRIVACY CONCERNS IN IOT

The rapid expansion of connected devices, as the Internet of Things, introduces new opportunities for enabling new services and merging new technologies with modern life.
The Smart Home is being rapidly deployed by service providers. Services such as home monitoring (camera), home automation (control over home appliances, home access, etc.), and home security (connected alarm system) enable user control over a wide range of services by means of end-user devices.
Furthermore, home appliances are being connected to the Internet for software updates, malfunction reports, and so forth.
These transformations have introduced a wide variety of new risks. The potential for malicious activities ranges from mischief to crime and malicious hacking. Hacking into cameras, violating privacy, and accessing content (pictures and movies) are some of the security threats introduced by the new era of connected homes.

These violations of accessing the content of our home automated devices can led to many dangerous outcomes. The third party sensor can gather and monitor our private data which can lead to burglary or any other form of troubles. Therefore, these unauthorized access needs to be checked.

In the world of computer networks we have various protocols like 802.1X, PAP, PEAP, EAP and many but these protocols require much high CPU processing capability as well as much memory. So, we need a light weight mechanism that can easily authenticate the microcontrollers or our home automation device sensors.

2.1 HOME AUTOMATION AND CYBERCRIME

Connectivity over the internet or a network; energy conservation; security and various home applications remain driving factors or communication. All these requirement in terms of bandwidth, cost and installation. The development of Internet connected technologies that are implementing IP solutions at home to harness energy while staying away from security threats.

Several standard protocols like IEEE 802.15.4 that can enable cost effective communication between the devices with low latency and cheap installation costs. There are many industrialized based protocols that are also available. Therefore,

with each new protocol represents a new area for possible security flaws.

3. AUTHENTICATION MECHANISM

As of today, IoT faces many challenges to authenticate the devices sensors that join the network. As the hardware ID for the sensors can be forged. Therefore, there are not many ways are to authenticate the device sensors or home automation devices. We have industry adopted standard security protocols like X10, Z-Wave or ZigBee that can provide encryptions mechanisms but proper ways to authentication devices still needs much research.

As referred from the [3] many security mechanisms have been proposed based on private key cryptographic primitives due to fast computation and energy efficiency. Scalability problem and memory requirement to store keys makes it inefficient for heterogeneous devices in IoT. Currently IoT do not address all authentication requirements like mutual authentication, Replay attack resistant, DOS, MITM as well as light weight solutions.

A Simpler Solution for authentication of all the sensors is to maintain a minimal database in the centralized server through which all home sensors are connected. A centralized server can be any sensor or object or a router in our home through which all other home sensors gets Internet or our private network access. This centralized server should be single point of network contact for all the home sensors. A database can be a file or hash of all the connected devices.

4. PROPOSED SOLUTION

The proposed solution concentrates on controlling the access for the devices or objects that are connecting in home network. Irrespective of the authentication mechanism used, it focus on how much access should a device must get. Some home sensors can have access to a particular Server 1 while other sensor can have access to server 2 but not to server 1 [From Fig 1]. This access control can vary from sensor to sensor. There can also be sensors that cannot get any Internet access.

A. Tagging Mechanism for access control

The devices that are given access to the networks should be assigned a particular tag by the centralized router. The tag determines the access level to the device or sensor into our private network. For example, the devices that are given the highest level of privileges can be granted Read/Write and Publication access while the device with least privilege can only share his data to centralized router or server. It is depicted in the form of table as:

Access Level	Access Code(in bits)	Device Privileges
7	111	Read, write and complete Internet access
6	110	Read, Write and publication to limited server(s) access
5	101	Read, Write & 1 server access
4	100	Read and Write access
3	011	Read access
2	010	No network access (Device can only share its info)
1	001	No access to network
0	000	Not allowed in network

Table 1

*The Read/Write or publication access are with respect to centralized server.

The tags will be kept private within the centralized and it should not be shared with any other devices. The other devices that are connected to the centralized router/server or sensor will be unaware of anything called the tags or the number. It is a mechanism that only centralized authority will know that which connected device should be given what access.

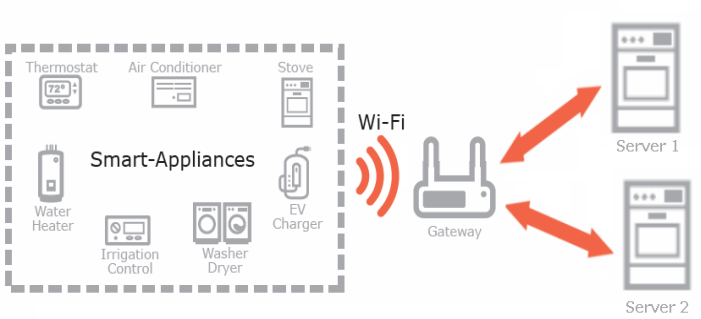

Figure: 1

B. Tag Assignment

As described in Authentication mechanism section that a hash is maintained at the centralized server. The tag will be maintained in the hash. Each connected device in our private home network should be assigned a corresponding TAG. The TAG assignment should be done by an authentication mechanism (if in future any available) or the owner of the home that have access to centralized server. As currently we lack the authentication methods like 802.1X, EAP in IoT world. I have to leverage this task on the centralized server.

If any new sensor or device that tries to connect to our home network will be assigned a default tag value of **"2"**. Its access code will be "**010"**, which defines no network access. The centralized server will read the data that it shares but it cannot publish any of its data to the Internet.

C. Selective Publication

This mechanism also provides a selective publication mechanism. There are some sensors that send its data to some remote server that analyzes and present it graphical form. So that sensor can be provided with access to that one particular server. It can also be illustrated as in following figure:

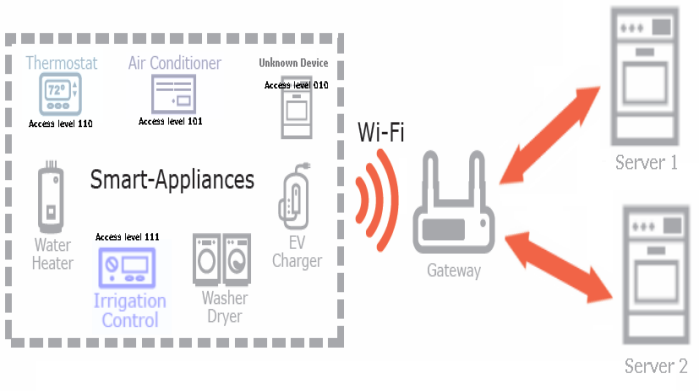

Figure: 2

As shown in the Figure 2 Irrigation Control has been assigned maximum access level 111 by the Gateway. Therefore, it is capable to access complete Internet while Thermostat has been assigned with Access level 110, it can be given access to both Server 1 & 2. The following table describes more on selective Access.

Home Sensor	Access Level	Selective Publication
Irrigation Control	111	Access to R/W and Complete Internet Access
Thermostat	110	Access to R/W and to both Servers 1 & 2.
Air Conditioner	101	Access to R/W and Server 1only
Unknown Device	010	Gateway can read its data, but it won't be allowed any n/w access.

Table 2

D. Implementation

This intelligence is with Gateway or centralized server that maintains the Access level Codes to each connected sensor. The authorized user that has access to centralized server and mentions which servers a particular sensor can access. A file or database will be maintained in centralized server which will look like the below mentioned table:

Device	Access Level	Access	Accessible IP(s)
Irrigation Control	111	All	
Thermostat	110	-	IPs of Server 1 & 2
Air Conditioner	101	-	IP of Server 1.
Unknown Device	010	-	-

Table 3

List of accessible IPs can be maintained in form of linked lists. A sample algorithm that can be followed is mentioned as:

Steps in the algorithm:

1) Received a request from a particular sensor for destination IP.
Let say sensor name is SensorX that requests for IP address be IPX.
2) Determine its access level by reading from the hash or file.
3) Based on the access level, perform the following task:

3.1) If access_level == 7
return TRUE; // Allow this access.

3.2) if access_level >= 5 and access_level < 7
For the Device SensorX
AccessibleIPs = get the list of accessible IPs for SensorX;
Compare IPX with each AccessibleIPs
If Match found
return TRUE; // as allow this access.
log a message.
else
return FALSE; // Block this access.
log a failure message.

3.3) If access_level == 4
No Internet/Network Access;
This device can log some data files in a particular directory in the server.

3.4) If access_level == 3
No Internet/Network access
This device can read some files in a particular directory in the server and can perform its own action based on that file commands. It cannot modify that file.

3.3) If access_level == 2
No Internet/Network access.
Gateway can read its shared data.

3.4) If access_level == 1
No access within the network.

3.5) If access_level < 1
Completely Blocked.

4) Log the necessary options and messages.
5) Process the next request.

This algorithm executes on the centralized server or router. That handles all the sensors request. The Sensors should be unaware of any such access codes or access levels.

5. CONCLUSION (TO BE FILLED AFTER REVIEW)

A conclusion section is not required. Although a conclusion

may review the main points of the paper, do not replicate the abstract as the conclusion. A conclusion might elaborate on the importance of the work or suggest applications and extensions.

APPENDIX

Appendixes, if needed, appear before the acknowledgment.

REFERENCES

[1] Identity Authentication and Capability Based Access Control (IACAC) for the Internet of Things.

[2] S. Hilton. (2012, 14 January). Progression from M2M to the Internet of Things: an introductory blog. Available: http://blog.bosch-si.com/progression-from-m2m-to-internet-of-things-an-introductory-blog/.

AUTHORS

First Author – Rahul Godha, Software Developer Engineer, Cisco Systems, Bangalore, rgodha123@gmail.com
Mobile No.: +91 9901106720

Second Author – Sneh Prateek, Software Developer Engineer, Akamai Tech, Bangalore, snehsm.007@gmail.com

Co-Author- Nikhita Kataria, Software Developer Engineer, Cisco Systems, Bangalore.