ISSN 2395-1621

Security: Smart Homes Using Internet of Things (IOT)

#1Rugved Amrutkar, #2Sanket Vikharankar, #3Lochan Ahire

1rugved.a6195@gmail.com
2vikharankar.sanket@gmail.com
3lochanahire@gmail.com

#123Dept. of Computer Engineering, Smt. Kashibai Navale College of Engineering, Pune-41, India

ABSTRACT

Internet of Things (IoT) enables a set of devices to share and communicate information over the internet. IoT requires security solutions to secure the communication with confidentiality, integrity and authentication services so as to protect the data from intrusions and disruptions. Smart homes are homes with technologically advanced systems enabling task automation, easier communication and higher security. In order to secure data communication in smart homes, MQTT protocol can be used.MQTT (Message Queue Telemetry Transport) is a light weight protocol which is best suited for unreliable networks. It enables large network of small devices that needs to be controlled and monitored from back-end server on the internet.People are used to automated things in day to day life to a large extent. Increasing demand of smart devices which automate things and reduces human intervention, motivated us to merge smart homes with smart devices and build a secure home.

Keywords: IoT, MQTT, NodeMCU.

ARTICLE INFO

Article History

Received :6th April 2016

Received in revised form :

8th April 2016

Accepted : 10th April 2016

Published online :

13th April 2016

I. INTRODUCTION

Smart Homes are homes with technologically advanced systems enabling task automation, easier communication and higher security. This system proposes basic idea of controlling and monitoring home appliances through smart phones from remote places. Smart devices communicate with each other by passing data which deals with private information of user. As this data is passed through network, security issues may arise. Existing protocols like HTTP, CoAP which were previously used in smart homes proved to be less reliable considering security of data. Intruder can make changes in original data which may result in some fatal problems.

To overcome this issue, we are using MQTT protocol which requires low bandwidth, less resources and provides assurance of data transmission among the smart devices. After using MQTT, data transmission will become more reliable and prominent in source usage as well as high scalability objective is achieved.

The idea of smart home is gaining importance in the present context due to their ability to automate home environments with great effectiveness. Smart systems are defined ass miniaturized devices that incorporate functions of sensing, actuation and control. They are capable of describing and analyzing a situation, and taking decisions based on the available data in a predictive or adaptive manner, thereby performing smart actions. The control of such appliances and devices at home environment is a complex matter due to two important reasons. Firstly, the control expected out of such automation applications is far more compact compared to the control provided by traditional control systems. Secondly, in such applications there is always the human element that comes to force, where in the people accommodating the homes expects to occupy a comfortable, healthy, secure, economy and convenient space. Home networking is the core to the implementation of an automation system for a smart home.

II. RELATED WORK

There are other protocols which were used before MQTT but they are not as sufficient as MQTT protocol.

A.HTTP

The **Hypertext Transfer Protocol** (**HTTP**) is an application protocol for distributed, collaborative, hypermedia information systems.[1] HTTP is the foundation of data communication for the World Wide Web.

Hypertext is structured text that uses logical links (hyperlinks) between nodes containing text. HTTP is the protocol to exchange or transfer hypertext.

Compared with HTTP, MQTT features faster response and throughput, and lower battery and bandwidth usage, making it well suited to use for home automation.

B.CoAP

The Constrained Application Protocol (CoAP) is a specialized web transfer protocol for use with constrained nodes and constrained networks in the Internet of Things.

The protocol is designed for machine-to-machine (M2M) applications such as smart energy and building automation.

Assuming that we are using a resource constrained device we want to use the most efficient method. In simple cases, for example when you only want to retrieve information from a resource constrained network, CoAP is a good choice.

However, on the other side of the spectrum, if the network of devices (Sensors, Controllers and Actuators all mixed together) need to stay up to date on what everything else is doing, sending messages to many becomes costly. It is cheaper for a device to send one message to a server which is not resource constrained, which can then spend inexpensive energy in forwarding this message. Furthermore, MQTT has the advantage of overcoming firewalls.

III.PROTOCOL OVERVIEW

The integral part of the home automation implementation is the MQTT client. The MQTT client is implemented on the Atmega 328 microcontroller as a software code. Some basic concepts on MQTT and messaging middleware is as follows

A. Middleware

Middleware is defined as the software which provides a messaging fabric to link applications and systems together. The alternative to not using a middleware system is that the application writer has to deal with the mechanics of getting messages from A to B, dealing with connection failures, network outages, duplicate messages etc . The use of middleware helps the application writer to communicate messages from one system to another system in remote locations. The IBM Web sphere MQ is one such messaging middleware that allows collaborating applications to intercommunicate via a central hub, known as a Message Broker. Therefore data producers can produce desired set of data and just set up a MQTT publish to the Broker. On the other hand a Subscriber can subscribe to the published topic and extract data for actuation or remote monitoring.

B. MQTT

MQTT (MQ Telemetry Transport) is one of the protocols supported by the IBM Message Broker products as a communicating data to and from the Broker. The protocol was designed specifically for remote telemetry applications, with three specific design goals: (1) It should offer a once-and-once-only assured delivery mode to enable a message to be reliably transferred all the way from a remote sensor to a back-end application.(2) The protocol should be as lightweight as possible across the "wire" (or other communication medium) most remote telemetry is done over low bandwidth, high cost networks, and so minimizing the overhead of each message is highly desirable. (3) The protocol should be very easy to implement on embedded devices such as sensors and gateways.

MQTT offers three quality news services: "at most once" news release is completely dependent on the underlying TCP/IP network; Lost or duplicated messages will occur; "at least once" ensures that the message arrived, but the message repetition may occur; "only once" ensures that messages arrive once.

C. BROKERS

Many industry initiatives have been integral in the development of MQTT and its applications in Internet Of Things. Companies like IBM, Eclipse and forums like OASIS have been integral in resource development for MQTT and its prototyping for practical applications. Various Broker or servers have been developed and released for Public Domain usage for application development on MQTT. Some of the projects are PAHO, MOSQUITTO by Eclipse, messaging middleware like Web Sphere MQ and servers like m2m.eclipse.org and test.mosquitto.org have gained huge fame.

Overall Design

Publishing/Subscribing Message Model. The design is based on publishing/subscribing messaging model .In this model, the publisher and subscriber are both clients, the message Destination is called theme. By connecting to the message broker they transfer data across the network. Publishers send a specific topic of messages to message broker, subscribers subscribe specific news topics to the message broker, and the connection between the subscriber and publishers managed by the message broker. When the message broker receives the published messages, it delivers the message to subscriber. Publishing/subscribing messaging model allows multiple providers to publish messages to the same topic. It also allows multiple users to subscribe messages with a subject. Then the message broker will broadcast to different subscribers.

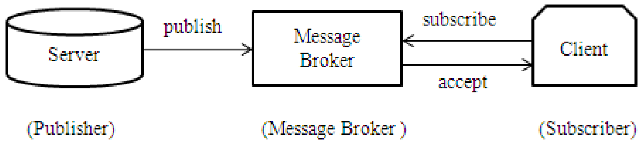


Fig. 1 Overall Architecture Diagram

As a message broker, it completes message routing function, receiving the message sent by the server, and then forwarded. Subscribers subscribe to the interesting topics, to submit information to the Message Broker, and to maintain a persistent connection. If publisher check into a new message, this message will be released by topic category. Depending on the topic, the Message Agent receives the message as well as the client's subscription, and releases this news to the corresponding phone.

IV. HARDWARE

NODEMCU-

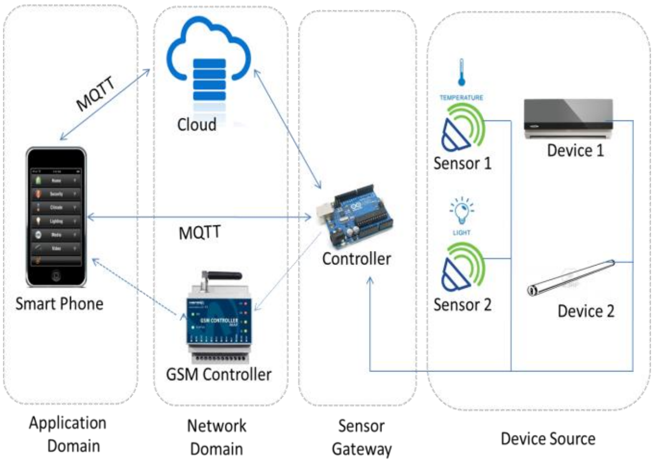
NodeMCU is an open source IoT platform. It uses the Lua scripting language. It is based on the eLua project, and built on the ESP8266 SDK 1.4. It uses many open source projects, such as lua-cjson and spiffs. It includes firmware which runs on the ESP8266 Wi-Fi SoC, and hardware which is based on the ESP-12 module.

NodeMCU was created shortly after the ESP8266 came out. On December 30, 2013, Espressif systems began production of the ESP8266.[9] The ESP8266 is a Wi-Fi SoC integrated with a Tensilica Xtensa LX106 core, widely used in IoT applications. NodeMCU started on 13 Oct 2014, when Hong committed the first file of nodemcu-firmware to GitHub. Two months later, the project expanded to include an open-hardware platform when developer Huang R committed the gerber file of an ESP8266 board, named devkit 1.0.

enabling NodeMCU to easily drive LCD, Screen, OLED, even VGA displays.

V. SYSTEM ARCHITECTURE

Home automation system architecture is a combination of three major domains, they are Application Domain, Network Domain and Device Domain. These domains are connected in sequence for reliable and secured data transmission in between end-user and Devices. Device Domain consists of home appliances like tube-light, AC, fan door etc. from which information is sensed by sensors and they are passed to controller. Controller is a device which plays a major role as a Gateway for this system. When sensor passes the data to controller, it recognizes and manipulates it to user understandable form. As Sensor can't interact with the smart phone device directly, controller is used as an interface. Controller passes the data to smartphone directly if proper internet connectivity is available. If due to some reason network is not available the information is stored at cloud for temporary purpose and then redirected to smart phone as soon as network is available. Cloud is acting as a database or server which is a part of Network Domain. User will receive information about current status of appliances and acknowledgement is passed as a response to the controller and accordingly the state of device will get changed. MQTT protocol is used for data transmission from appliances to user. When internet connection is not available GSM controller can be used to send the messages to user. But it is not efficient and secured way of data transmission. Hence internet based approach is used in this project.



.

VI. CONCLUSION

The emerging idea of Internet of Things (IoT) is rapidly finding its path in modern life aiming to improve our lie by connecting smart devices , technologies and applications. But there are several issues dealing with security is data security. The main feature that differentiate IoT security issues from traditional once are heterogeneous and large scale objects and networks. Data security issues leads to Data Authentication, Data Integrity, Privacy, etc. By using MQTT protocol, Data Authentication and Privacy issue is solved partially.

MQTT is a lightweight, low bandwidth, transmission efficient protocol, it helps the data to pass without any intrusions and disruptions. It controls the devices by sending commands and acknowledgements for successful execution of tasks.

VII. FUTURE SCOPE

The proposed paper is a basic prototype of the applications of using MQTT protocol for home automation applications. The paper can be extended to full fledged systems capable of interconnection of hundreds of sensors and many actuators. This approach requires efficient design of Brokers or Servers to meet the needs of the application.

- MQTT can be used as part of a large sensor network capable of monitoring floods, volcanic eruptions and earthquakes achievable through the deployment of application specific sensors in disaster prone areas.

- Servers or Brokers specific to application can be developed to improve the communication efficiency and thereby improve system performance.
- GSM kit can be used to make the controlling and monitoring home appliances offline using local SMS service.

ACKNOWLEDGEMENT

It gives us great pleasure in presenting the preliminary project report on
'SECURITY: SMART HOMES USING INTERNET OF THINGS (IoT)'.

We would like to take this opportunity to thank my internal guide **Prof. RAGHIB NASRI** for giving me all the help and guidance we needed. We are really grateful to them for their kind support. Their valuable suggestions were very helpful.

We are also grateful to **Prof.Dr.P.N.MAHALLE**, Head of Computer Engineering Department, Smt. Kashibai Navale College of Engineering, Pune-41 for his indispensable support, suggestions.

REFERENCES

[1] Ullas B S1, Anush S1, Roopa J2, Govinda Raju M2" Machine to Machine Communication for Smart Systems using MQTT" March 2014

[2] Bandyopadhyay, S.; Bhattacharyya, A., "Lightweight Internet protocols for web enablement of sensors using constrained gateway devices," Computing, Networking and Communications (ICNC), 2013 International Conference on , vol., no., pp.334,340, 28-31 Jan. 2013.

[3] Somayya Madakam, Ramaswamy R." Smart Homes(Conceptual Views)" 2014 2nd International Symposium on Computational and Business Intelligence

[4] F. Kausar, E. A. Eisa, I. Bakhsh, "Intelligent Home Monitoring Using RSSI in Wireless Sensor Networks" International Journal of Computer Networks & Communications, vol. 4, pp. 33-46, 2012.

[5] Colitti, Walter, Kris Steenhaut, and Niccolò De Caro. "Integrating wireless sensor networks with the web." Extending the Internet to Low power and Lossy Networks (IP+ SN 2011) (2011).