DEVELOPMENT OF SECURE HOME AUTOMATION BASED ON HOMEKIT IOT PLATFORM

Sanjeev Singh Verma[1], D.Saranyaraj[2], Aditya Kumar Sinha[3]

[1]*PG Student, VLSI & ESD, Veltech Technical University, Chennai, Tamil Nadu, India*
[2]*Assistant Professor, Electronics & Communication Engineering, Veltech University, Chennai, Tamil Nadu, India*
[3]*Principal Technical Officer, C-DAC ACTS, Pune, Maharashtra, India*

ABSTRACT

The Internet is significantly developing and making different availability strategies. The Internet of Things (IoT) is one of those systems which change current Internet correspondence to Machine-to-Machine (M2M) premise. Subsequently, IoT can consistently interface this present reality and the internet by means of physical articles that implant with different sorts of canny sensors. An expansive number of Internet-associated machines will create and trade a tremendous measure of information that make day by day life more advantageous, settle on an intense choice and give helpful administrations. This paper not just depicts about the development and how imperative of IoT in day by day life, the non specific engineering, its most broadly utilized conventions, various conceivable applications additionally worry over security and protection issues in IoT, certifiable usage of IoT framework by utilizing Raspberry Pi and its future patterns. The IoT presumably gets to be a standout amongst the most well known systems administration ideas that can possibly bring out numerous advantages. We utilized Raspberry Pi as Server and iOS as Client. We built up a stack for connection to HomeKit Protocol utilizing abnormal state security and information encryption strategies. HomeKit is the name for Apple's Home Automation structure. HomeKit is a structure for speaking with and controlling associated home robotization embellishments that bolster Apple's HomeKit Accessory Protocol. HomeKit applications empower clients to find good embellishments and arrange them. Clients can likewise make activities to control embellishments, (for example, an indoor regulator or light), gather them together, and trigger them by utilizing Siri.

Keywords: *Internet of things (IoT), wireless sensor network, Apple HomeKit,Home Automation, Secure and Safe Network, Secure Remote Password (SRP) Protocol, Raspberry Pi Server.*

1. INTRODUCTION

In spite of the fact that quickly propelling advances, society is moving toward a "constantly associated" model. Wired and remote systems are all over the place, open benchmarks are characterized and took into account especially tending to methodology. Ideas connected with the "Future Internet" are being investigated , created and ceaselessly adjusted in day by day life.One new idea connected with the "Future Internet" is called "Web of Things" (IoT). The IoT turn into a dream where certifiable items are a piece of the web: each article is remarkably recognized, and open to the system, its position and status known , where numer-ous administrations and insight are added to viably grow an Internet, flawlessly joining between the digi-tal and physical world, inevitably influencing on individual and social environment. This paper introduces a diagram of the Internet of Things with security, bland engineering and conventions, applications, execution and its future patterns.

1.1 IoT Protocols

Protocol is the special set of rules and regulations that end point in a telecommunication connection use when they need to communicate to other end point which connected to the same/different network. In this subsection will briefly describe about the most frequently used protocols for Machine-to-Machine (M2M) communication.

1.1.1 MQTT (Message Queue Telemetry Transport): MQTT is a Client Server distributes or subscribes informing transport convention. It is light weight, open, straightforward and outlined in order to be anything but difficult to execute. The convention keeps running over TCP/IP or over other system convention that gave requested, lossless, bi-directional associations. The MQTT highlights include: utilization of the distribute/subscribe message design which gives one-to-numerous message appropriation, an informing transport that is rationalist to the substance of the payload, and this convention additionally has three characteristics of administration for message conveyance viz; "At most once", where messages are conveyed by best endeavors of working environment. The message misfortune can happen and this level could be utilized, Secondly, "At any rate once", where message are guaranteed to arrive however copy back rubs can happen. At last, "Precisely once", where message are guaranteed to arrive precisely once. This level could be utilized .This that bring about to radically lessen system activity. Promote more, the MQTT convention is not just minimized transport overhead and convention trade to decrease system activity additionally has a phenomenal component to tell invested individuals when an anomalous disengagement happen also.

1.1.2 CoAP (Constraint Application Protocol): CoAP is a particular web exchange convention for use with obliged hubs and compelled systems (e.g. low-control, lossy). The hubs regularly have 8-bit microcontroller with little measures of ROM and RAM, while obliged organize frequently have high parcel mistake rate and commonplace throughput is 10 kbps . This convention intended for Machine-to Machine (M2M) application, for example, savvy city and building computerization. CoAP gives a solicitation and reaction collaboration model between application end focuses, bolster work in revelation administrations and assets, and incorporates key ideas of the Web, for example, URIs and Internet media sorts. CoAP is intended to cordial interface with HTTP for joining with the Web while meeting particular prerequisites, for example, multicast support, low overhead and effortlessness for obliged situations.

1.1.3 Homekit : HomeKit speaks HomeKit Accessory Protocol (HAP), which keeps running on top of a BLE/Bluetooth Smart or a HTTP/TCP/IP stack. In the event that an extra does not bolster HAP straightforwardly a passage is required. HomeKit deals with the accumulation of embellishments in a characterized home, and how about we you communicate the administrations gave by those adornments utilizing iOS applications or Siri. HomeKit deals with frill/span revelation and arrangement, utilizing HAP to speak with those embellishment gadgets and entryways.

1.1.4 Secure remote password : The Secure Remote Password convention (SRP) is a cryptographically solid confirmation convention for secret word based, common verification over an unstable system association. Effective SRP validation requires both sides of the association with know about the client's secret word. Notwithstanding secret key confirmation, the SRP convention likewise performs a safe key trade amid the validation procedure. This key might be utilized to secure system activity by means of symmetric key encryption. SRP offers security and arrangement focal points over other test reaction conventions, for example, Kerberos and SSL, in that it doesn't require trusted key servers or declaration foundations. Rather, little check keys got from every client's secret key are put away and utilized by each SRP server application. SRP gives a close perfect answer for some applications requiring straightforward and secure secret word confirmation that does not depend on an outside base. Another great part of the SRP convention is that compromized confirmation keys are of little esteem to an assailant. Possesion of a check key does not permit a client to be mimicked and it can't be utilized to acquire the clients secret word with the exception of by method for a computationally infeasible lexicon assault. A compromized key would, be that as it may, permit an aggressor to mimic the server side of a SRP confirmed association. Thusly, care ought to be taken to forestall unapproved access to confirmation keys for applications in which the customer side depends on the server being bona fide.

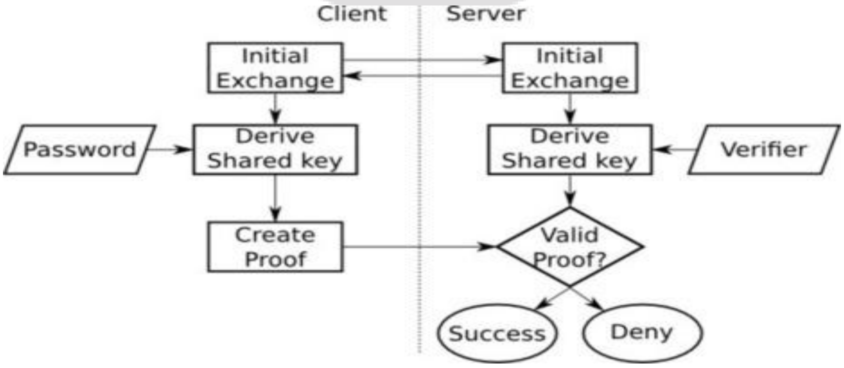


FIG 1. SRP IMPLEMENTATION

1.2 IOT Architecture

Today, Internet of Things(IoT) is utilized as a catchphrase by numerous sources. This expression envelops a system of arrangements by one means or another identified with the universe of intercommunicating shrewd articles. These arrangements indicate next to zero interoperability abilities as a rule they are created for particular difficulties at the top of the priority list, taking after particular necessities. Additionally, as the IoT umbrella covers very surprising application fields, it creates the impression that advancement cycles and innovations utilized fluctuate immensely. As an outcome simply vertical and segregated arrangements rise while just a more level methodology, where application storehouses share a typical specialized establishing and regular engineering standards, could in the long run lead to a full fledge Internet of Things. While entirely legitimate now, on the long run we trust that this circumstance is unsustainable. As in the systems administration field, where a few arrangements rose at its earliest stages to leave spot to a typical model, the TCP/IP convention suite, the rise of acommon reference model for the IoT space and the ID of reference designs can prompt a quicker, more engaged improvement and an exponential increment of IoT-related arrangements. These arrangements can give a vital point of interest to develop economies, as new plans of action can influence those mechanical arrangements giving space to monetary advancement.

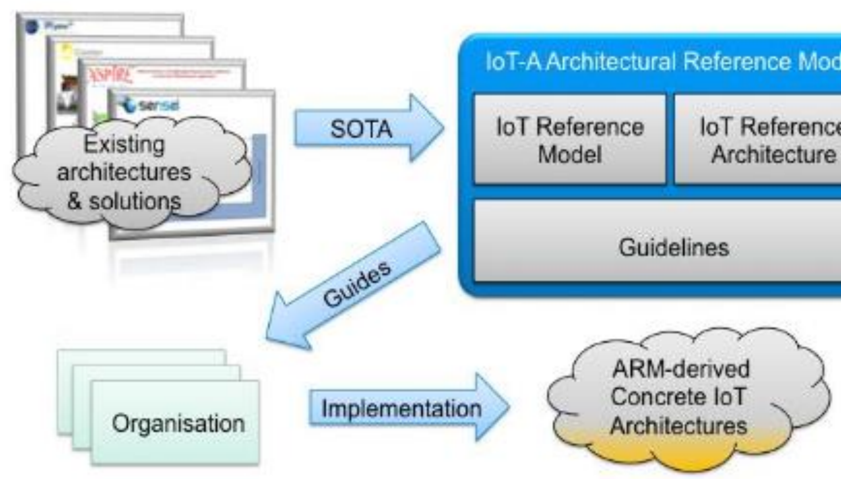

Existing architectures & solutions
SOTA
IoT-A Architectural Reference Model
IoT Reference Model
IoT Reference Architecture
Guidelines
Guides
Organisation
Implementation
ARM-derived Concrete IoT Architectures

FIG 2. IOT ARCHITECTURAL REFERENCE

2. RELATED WORK

2.1 MOTIVATION

To enhance way of life it is expected to change home ecological condition as indicated by the disposition of the habitants with no intrusion. Now and again physically incapacitate or impaired individuals are not capable move much from one place so for them it is extremely hard to get to customary household machines. For them it is vital to build up a framework which requires less human cooperation. We require vitality effective, adaptable framework which likewise distinguish the flaw in the gadgets consequently and inform the related specialist and client about the issue naturally. To give this offices in creating nations like India we require a much brilliant framework which give all the above offices in low cost and less vitality utilization.

2.2 LITERATURE SURVEY

Home Automation is only computerization of the home that is robotization of family unit action or housework. It can likewise incorporate brought together lighting control, machines, ventilation, warming and aerating and cooling (HV AC), security of entryways and doors. It serves to enhanced solace, comfort, security and vitality productivity. Home computerization is valuable for elderly and handicapped people groups to expand personal satisfaction so they turns out to be less subject to parental figures. Lately home robotization ubiquity has been expanding for the most part due to its effortlessness through cell phone network and higher reasonableness. In home computerization framework different electrical gadgets in a house cooperates with each other by utilization of the data innovation to expand vitality productivity and security. Despite the fact that there are a few issues with this framework like many-sided quality, high rivalry with different merchants, incongruent gauges and high cost which results to this home computerization framework is restricted to affluent or yearning clients as it were. A significant number of the home robotization frameworks that are industrially accessible can be isolated into two classes: privately controlled frameworks and remotely controlled frameworks. Privately controlled frameworks utilize an in-home controller to accomplish home mechanization. This permits clients complete utilization of their computerization framework from inside their home through a stationary or remote interface. Remotely controlled frameworks utilize an Internet association or combination with a current home security framework to permit the client complete control of their framework from their cell phone, PC, or through phone from their home security supplier. In one study scientists presents home computerization frameworks in light of Bluetooth, that utilizing Android Smart telephones. The gadgets that we used to get to and control is physically associated with a Bluetooth controller. The Smart telephone is then associated with it by utilizing as a part of assemble Bluetooth network which control that gadgets. In some other case specialists likewise give system interoperability and one vital element that is remote access to control home gadgets or apparatuses utilizing home entryways.

3. DESIGN AND DEVELOPMENT

In this we intend to make a HomeKit-empowered server (Raspberry Pi) which will acknowledge approaching call from customer and send reactions and warnings to enlisted customer. For this we require HomeKit specialized determinations, equipment specialized backing.

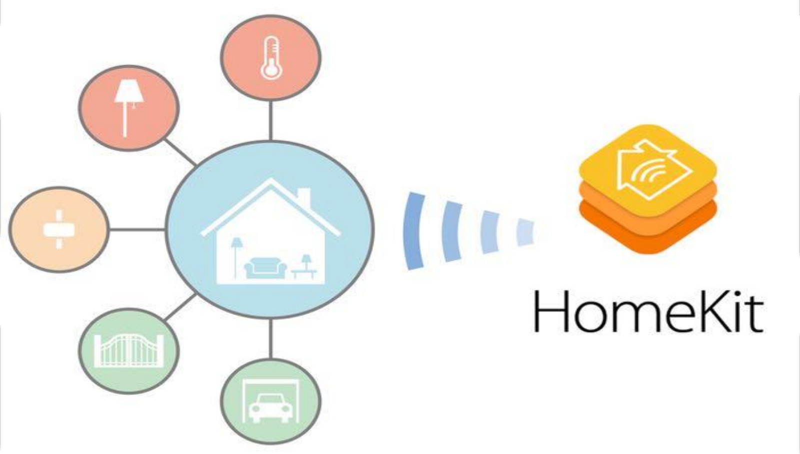


FIG 3: BLOCK DIAGRAM OF HOMEKIT

3.1 Designing Server

Keeping in mind the end goal to permit customer to interface with the server we have to introduce different bundles in Raspberry Pi which empowers client to make application as HomeKit embellishment Server. Taking after strides were taken after:

a) Installing AVAHI: To promote server on the system with the goal that customers can find it. summon to introduce AVAHI on Raspberry Pi (Raspbian): root@raspberrypi:/home/pi/avahi-0.6.31# sudo apt- get install libdns*

b) avahi establishment is fundamental for dns_sd.h library to be utilized. <dns_sd.h> is required for DNSServiceRegister capacity which enroll Bonjour administration name (_hap._tcp).

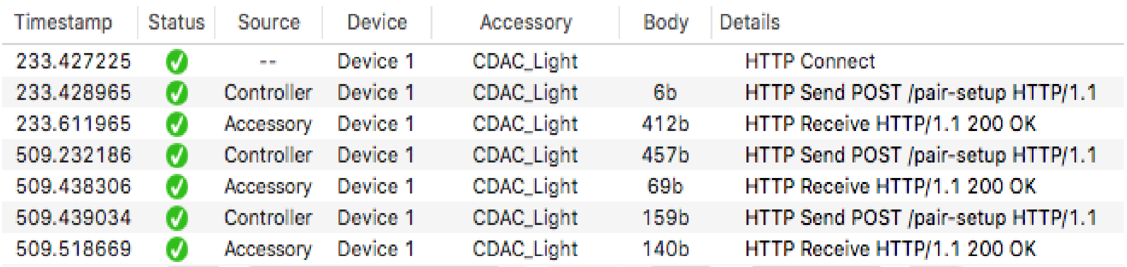
3.2 Client Application

For customer to associate with the server an application is required. HomeKit Accessory Simulator is utilized to recreate frill in a home. At the point when server is begun, it will publicize IP data of extra (Device ID, Bonjour Service Name, Bonjour Model and so forth.) over the system. Customer can now find and communicate with the server, control frill. At the point when customer tries to cooperate with server, Pair Setup and Pair Verify forms happen (clarified prior). Amid M1 iOS Device sends solicitation to the embellishment. Subsequent to accepting

M1 ask for, adornment will send M2 reaction to the iOS Device. Blending PIN window will open, customer need to enter 8 digit mystery secret key in the arrangement XXX-XX-XXX for finishing Pair Setup process. In the event that client enters wrong watchword then embellishment server will dismiss the Pair Setup Request and send mistake reaction to the customer. Solicitation and Response parcels from the customer or server are in TLV organize and take after HTTP GET and POST strategies for correspondence.

4. RESULT

Blending Pin is known not and server both. Notwithstanding, it is kept mystery from outside world. As it is not shared so any undesirable client can't get to or recover data transmitted over the system. After culmination of paring procedures customer will get Public Key and Secret Key of the HomeKit Accessory Server. The transmission happens in encoded shape subsequently gives security. Figure 5 demonstrates keys included in our examination.



Timestamp	Status	Source	Device	Accessory	Body	Details
233.427225	✓	--	Device 1	CDAC_Light		HTTP Connect
233.428965	✓	Controller	Device 1	CDAC_Light	6b	HTTP Send POST /pair-setup HTTP/1.1
233.611965	✓	Accessory	Device 1	CDAC_Light	412b	HTTP Receive HTTP/1.1 200 OK
509.232186	✓	Controller	Device 1	CDAC_Light	457b	HTTP Send POST /pair-setup HTTP/1.1
509.438306	✓	Accessory	Device 1	CDAC_Light	69b	HTTP Receive HTTP/1.1 200 OK
509.439034	✓	Controller	Device 1	CDAC_Light	159b	HTTP Send POST /pair-setup HTTP/1.1
509.518669	✓	Accessory	Device 1	CDAC_Light	140b	HTTP Receive HTTP/1.1 200 OK

FIG 4: PAIRING SUCCESSFUL

5. CONCLUSION

For creating HomeKit-empowered extra you have to join MFi(Made For iPhone) program and get to be MFi licensee. A MFi licensee gets HomeKit specialized details, MFi Logos and Identity Guidelines, Hardware specialized backing. This structure has awesome application in home computerization, mechanical mechanization, agribusiness and so fort

6. REFERENCES

1. N. Council, "Disruptive civil technologies: Six technologies with potential impacts on us interests out to 2025," in Conference Report CR, 2008.

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. A. Juels, "RFID security and privacy: A research survey," IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp. 381–394, 2006.

4. J.-P. Vasseur and A. Dunkels, Interconnecting smart objects with IP: The next internet. Morgan Kaufmann, 2010.

5. J. Hui, D. Culler, and S. Chakrabarti, "6LoWPAN: Incorporating IEEE 802.15. 4 into the IP architecture–internet protocol for smart objects (IPSO) alliance, white paper #3," 2009.

6. A. Dunkels and J. Vasseur, "IP for smart objects, internet protocol for smart objects (IPSO) alliance, white paper #1," 2008.

7. M. Potkonjak, S. Meguerdichian, and J. L. Wong, "Trusted sensors and remote sensing," in IEEE Sensors, pp. 1104–1107, 2010.

8. J. H. Kong, L.-M. Ang, and K. P. Seng, "Minimalist security and privacy schemes based on enhanced AES for integrated WISP sensor networks," Journal of Communication Networks and Distributed Systems, vol. 11, no. 2, pp. 214–232, 2013.

9. A. M. Dunn et al., "Eternal sunshine of the spotless machine: Protecting privacy with ephemeral channels.," in Operating Systems Design and Implementation (OSDI), pp. 61–75, 2012.

10. Y. Tang et al., "CleanOS: Limiting mobile data exposure with idle eviction.," in Operating Systems Design and Implementation (OSDI), vol. 12, pp. 77–91, 2012.

11. Z. N. Peterson, R. C. Burns, J. Herring, A. Stubblefield, and A. D. Rubin, "Secure deletion for a versioning file system.," in File and Storage Technologies (FAST), vol. 5, pp. 4–11, 2005.

12. D. Boneh and R. J. Lipton, "A revocable backup system.," in USENIX Security, pp. 91–96, 1996.

13. S. Diesburg et al., "TrueErase: Per-file secure deletion for the storage data path," in Anual Computer Security Applications Conference (ACSAC), pp. 439–448, 2012.

14. J. R. Smith et al., "RFID-based techniques for human-activity detection," Communications of the ACM, vol. 48, no. 9, pp. 39–44, 2005.

15. K. Rowe, "Securing microcontroller RTOSes for the internet of things." http://www.embedded.com/design/operating-systems/4429868/Securing-microcontroller-RTOSes-for-the-Internet-of-Things, 2014.