ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

Privacy Preserving Communication Protocol with CoAP in Smart Home

Krishnenthu P Mani [1], Dr. S. Brilly Sangeetha [2]

P.G. Student, Department of Computer Science & Engineering, IES College of Engineering , Thrissur, Kerala, India[1]

Associate Professor& Head, Department of Computer Science & Engineering, IES College of Engineering, Thrissur, Kerala, India[2]

ABSTRACT: Internet of things had made extraordinary progress in both academic and in industrial fields. The privacy preserving communication protocol in smart homes is used for providing the security in data transmission in the smart home. To improve the energy- efficient, secure, and privacy-preserving communication protocol for the smart home systems. It mainly consists of monitor group, appliance group, central controller and user interface. Data transmissions within the smart home system are secured by a symmetric encryption scheme with secret keys being generated by chaotic systems and a Message Authentication Codes (MAC) is used to guarantee data integrity and authenticity in the system. It uses a face recognition mechanism so that only the home members can automate the system and focused on CoAP (Constrained Application Protocol) based framework to give service level access control on resource constrained devices. It gives fine grain access control and authentication is checked. CoAP is used to establish a secure communication channel when the smart device connects to the smart home system.

KEYWORDS: Internet of Things, Constrained Application Protocol , Message Authentication Code.

I. INTRODUCTION

Internet of Things (IoT) is defined as the network of physical devices, vehicles and other things that are embedded with software, sensors, and electronics to communicate and transfer data between each other. Now days IoT had made extra ordinary progress in both industrial and in academic fields. There are few smart home systems which have been developed by major companies to achieve the home automation. Home automation is building automation for a home, called a smart home. Smart home is used to control and automate the home appliances used in the home. The main problem of IoT based smart home automation is that anybody can automate the system. If no security is provided then the user privacy data can be easily taken by the attacker or any malicious entity. For example in smart home system the end devices will communicate frequently with the central controller, if no security is provided then the user data can be easily taken by the attacker. Smart home systems do not take too much consideration of the security and privacy issues. Some of the attack may arise when the end devices in a smart home sends data frequently to the central controller and the types of the end devices used can reveal the identity of the user in the house then by this the information that can be captured by eavesdropping attacks. So to improve the energy efficiency and security, a privacy preserving communication protocol and constrained application protocol is used in the smart home. Smart home system mainly consists of monitor group, appliance group, central controller and a user interface. The two major challenges of designing a secure smart home system are privacy and efficiency. To provide the security in data transmission the smart home are secured by the symmetric encryption and the secrete key is generated by the system for the encryption. Symmetric-key encryption means a same key is used for both encryption of plaintext and for the decryption of cipher text. Message Authentication Codes (MAC) scheme is used to guarantee data integrity and authenticity. CoAP (Constrained Application Protocol) is one of the latest application layer protocol to connect to Internet. CoAP is a specialized web transfer protocol designed to provide web services to constrained nodes and to provide security in data transmission in the web. Face authentication is used in the system to identify that if a person enters into the system is correct or not. By the face authentication only the home member can activate the system.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

Privacy preservation communication protocol consists of four steps, they are key generation, encryption, MAC generation and verification and decryption. In the key generation stage the server generates a pair of secret key and assigns these pair of secret key to the agent. After the key generation the encryption has to perform in that agent will encrypt the message by using one of the key and it will generate the MAC. The server and agent want to generate the MAC. If the agent is generating the MAC then it want to send to the server and in that condition MAC verification should be performed in the server side. And if the server is generating the MAC then it want to send to the agent and in that condition MAC verification should be performed in the agent side. After the MAC verification if two MAC generated a same then server will decrypt the message by using the same key used in the encryption. If two MAC are not same then the server will discard the message.
CoAP is used to check the authenticity of the user and to provide the access control to user, if it is correct user. First the authenticity of the user is checked when the user gives the login service request. If the user is a validate user then the user is allowed to enters to the system but not allowed to access the system. For to access the system user want to give another access service request and based on that request validity the access service is given to the user.

II. LITERATURE SURVEY

Sometimes In 2013, Bando et al. Ying-Tsung Lee et al. (2017) proposes a privacy-preserving data analytics in cloud-based smart home with community hierarchy [1]. A smart community public housing projects consists of tens of thousands of households. The cloud based smart home is a three-layered hierarchical architecture consists of home controller, community broker, and cloud platform. The privacy-preserving system, a single home controller is connected to a community networking with datahiding capabilities and integrated these data to a hierarchical architecture. And these are integrated in a cloud platform for data analytics access control mechanism. The community broker not only performed home and community-level data separation and aggregation. The cloud platform provided public access to data analytics, queries, and management. Privacy preservation was then achieved by integrating informing, enforcement and a fine-grained access control mechanism of the communities and homes. The community broker provides privacy protection in community and home levels through data separation, aggregation, and fusion. The cloud platform integrates the enforcement process, access control mechanism, informing process scenario, and demonstrations at the community and home level to process privacy protection. The main advantage is that system performs data minimization and data hiding to provide the privacy preservation in cloud based smart home.
Mohsin B Tamboli & Dayanand DAmbawade (2016) proposes secure and efficient coap based authentication and access control for IoT[2]. During the interaction between devices IoT gets suffered from severe security challenges. The system focuses on CoAP which provide fine grain access control. The proposed solution uses another authentication and access control system like Kerberosalong with the CoAP protocol and an optimized version of ECDSA (Elliptical Curve Digital Signature Algorithm) uses elliptic curve cryptography. It is used to create a digital signature of data is implemented within smart things which provides efficient privacy. CoAP also support block wise transfer of big messages in which it splits messages and send them with reference order. The main advantages of the system are it provides data integrity, Non-repudiation and Confidentiality.
Khusvinder Gill et al. (2009) proposed a zigbee-based home automation system [3]. ZigBee based home automation system is implemented for the monitoring and control of household devices. It identifies the reasons for this slow adoption of the home automation system. The proposed System is a novel, stand alone, low-cost and flexible ZigBee based home automation system. System allows home owners to monitor and control the devices in the home, through a variety of controls. The controls included in the system are ZigBee based remote control, and any Wi-Fi enabled device. And a gateway is provided between heterogeneous Zigbee and Wi-Fi networks, and facilitates local and remote control and monitoring over the home's devices. The security and safety of the home automation network is done on the Home Gateway. Kalyani Pampattiwar et al. (2017) proposed a home automation using raspberry pi controlledvia an android application. Home Automation System (HAS) [4] provides a low cost wireless communication between a RaspberryPi module and an android based application to the IP appliances at home. It performs the operations such as controlling the lighting, setting alarms and reminders, smart security system and an entertainment system. For the security a smart doorbell is introduced. The system includes speakers connected to the Raspberry Pi via bluetooth.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

III. SMART HOME SYSTEM

The smart home system consists of four groups of entities: appliance group, monitor group, the central controller, and user interfaces. For simplicity, the entities that are in the appliance group and the monitor group are called agents. The agents communicate with the central controller via wireless networking technologies. The user controls the smart home system through user interfaces. Appliance group contains the home appliances including TV set, stove, oven, thermostat, etc. Each member of the group has a unique ID so that it can be uniquely identified by the central controller. The entities in the appliance group can perform limited operations such as switching on/off, turning up/down, reporting status, etc. Monitor group is formed by sensors and detectors such as smoke sensor, motion sensor, electricity meter, and home security monitoring sensor. The sensors keep sensing the data and periodically send the data to the central controller. Central controller has two components they are processor and a database. The processor is capable of performing aggregation algorithms so that the controller can adjust the behaviors of the home appliances and sensors. The database stores the data reported by the sensors and appliances with time stamps for future reference. The database also stores the initial parameters of the logistic maps that are to be assigned to the sensors and appliances. User interfaces offer a gate for the smart home system to interact with users. The user interfaces take many forms such as a control pad installed in the house, website and software installed on personal computers, and applications on smart hand-held devices. The user interfaces enable the users to configure, monitor, and remotely control the smart home system via the central controller.

IV. SYSTEM ARCHITECTURE

Fig 1 is the system architecture. The smart home system architecture mainly consists of Server, Agent, Privacy preserving communication protocol, Constrained application protocol and Face authentication.

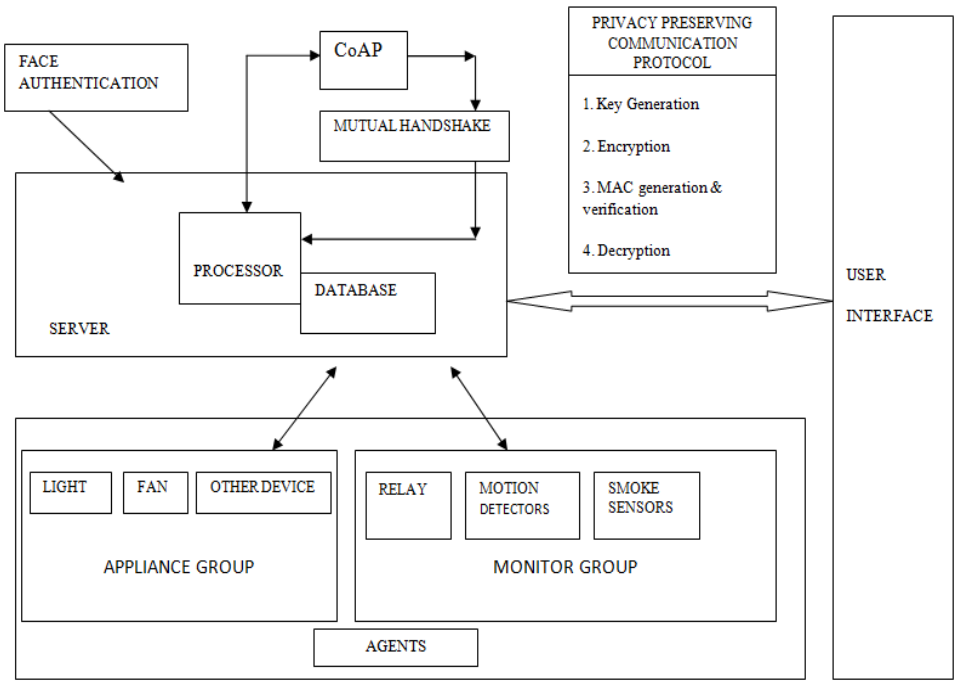

Fig 1 . System Architecutre

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

A. Agent

The agents are formed by the sensors, actuators, and monitors that are deployed over the smart home. They are activated as soon as their installations are finished, and they keep sensing contextual data in the house as time goes. They periodically report the collected data to the central controller. In the meantime, the agents continuously listen to responses and commands sent by the central controller.

B. Server

The central controller of the smart home system is termed as the server. So the server has a processor and a database. The server listens to the data reported by the agents and sends back responses and commands. The server also act as an gateway for the users to configure, monitor, and control the smart home system.

C. Constrained Application Protocol

To establish a secure connection in the smart home CoAP is used. The CoAP is performed on the raspberry pi part. To properly work a smart home the internet connection is required so the CoAP is used. CoAP is one of the latest application layer protocols for smart devices when they connect to Internet. In Fig 2, first it performs an authentication with the devices and then performs the access control. A new user enters into the system then user want to make registration on the database server. To check the authenticity the user givers a login service request, based on that request server will checks that if it is a correct user or not by checking the information stored on the database. If it is a correct user then the server will issues a response as validated user and a ticket TGT ticket is issued. TGT is defined as ticket to get ticket and it is a timeout ticket. If the authenticity of the user is valid then TGT is issued and if the authenticity of the user becomes unsuccessful then no ticket is issued. The properties of the TGT tickets are following:

- Ticket is unique per user and service.
- Ticket has particular timeout, after that it becomes invalid.
- Ticket length could be configurable according to the requirement.

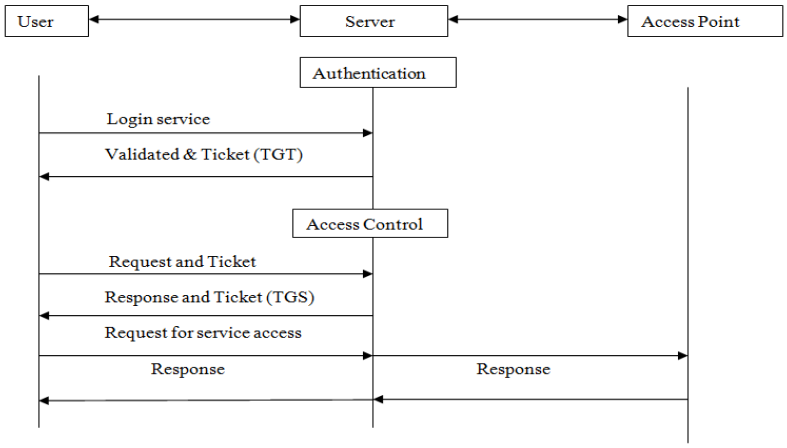

Fig 2 . CoAP Architecutre

After the authentication the user is allowed to enter to the system by not allowed to access the system for that the access control has to be checked. The second process is the access control. When user request for service access, CoAP checks the validity of ticket (TGT) user got during authentication along with the service name, Message ID. If the ticket is valid then server gives the response back and issues another ticket that is ticket for granting service (TGS). If the ticket is expired then the user request will not be proceed and the user is not allowed to access the services of the system. After getting the response and the TGT ticket the user is allowed to access the services of the system. The TGT is also a timeout ticket i.e., only up to a certain time the user is allowed to access the services of the system. The TGT ticket also has some properties they are following:

- Ticket is unique per user and service.
- Ticket has particular timeout, after that it becomes invalid.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

- Ticket could be encrypted to avoid attack on it.

D. Privacy Preserving Communication Protocol

To secure the data transmission the privacy preserving communication protocol is used.It mainly consists of four steps they are following:

(i) Key Generation

The server generates a pair of secret keys for each agent and assign the pair of keys to each agent.

1. At the installation stage of an agent i, the server randomly choosesr_0,r_1,x_0,$x_0^{'}$.
2. Server generates two logistic map
   $x_{t+1}^{(i)} = r_1 x_t^{(i)}(1 - x_t^{(i)})$

   $x_{t+1}^{(i)'} = r_2 x_t^{(i)'}(1 - x_t^{(i)'})$
3. Server assigns (r_0, x_0) and $(r_1, x_0^{'})$ to agent
4. After the initialization the server stores the parameter into the table.
5. Once agent i starts functioning and is ready to send the collected data, it computes a pair of one-time secret keys $x_t^{(i)}$, $x_t^{(i)'}$

(ii) Encryption

The agents encrypt the data using the generated key.

- **On agent i's side:**

1. Agent i collects data for a period of time and stores the data in a vector A= (a1;a2; ...).
2. Agent i appends the timestamp T and its index to the data to form the plaintext message, M =A+i+T
3. Encrypt M
4. $C = E_{x_{(t)}^{(i')}}(M)$

- **On server side**

1. The server encrypts the message along with the time stamp and computes the cipher text.
   $C = E_{x_t^{(i)'}}(M)$

(iii) MAC Generation and Verification:

Both the server and the agents want to generate the MAC using their shared secret keys and upon receiving a message from the server/agents, the agents/server check(s) the authenticity of the message using the same signing algorithm and the shared secret key.

- **On agent side:**

1. After the message is encrypted, the agent computes MAC
   $MAC(C) = MAC_{x_t^{(i)}}(C)$
2. Sends C||MAC(C) to server.
3. The agent first computes$MAC_{x_t^{(i)}}(c)$
4. Agent proceeds to decrypt the message after verifying MAC(C)

- **On server side:**

1. After the message is encrypted, the server computes MAC
   $MAC(C) = MAC_{x_t^{(i)}}(C)$
2. Sends C||MAC(C) to agent.
3. The server first computes
   $MAC_{x_t^{(i)}}(c)$
4. Server proceeds to decrypt the message after verifying MAC(C)

(iv) Decryption

The server and the agents decrypt the message after the authenticity of the message is verified.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

V. PRIVACY PRESERVING COMMUNICATION PROTOCOL ALGORITHM

a. Algorithm 1 Initialization

1: t ← 0
2: for each agent i do
3: The server selects two logistic maps:
$x_{t+1}^{(i)} = r_1^{(i)} x_t^{(i)}(1 - x_t^{(i)})$ And
$x_{t+1}^{(i)'} = r_2^{(i)} x_t^{(i)}\left(1 - x_t^{(i)'}\right)$
4: The server shares the parameters with agent i.
5: end for

b. Algorithm 2 PPCP

1: Agent i computes the symmetric key $x_t^{(i)'}$ from logistic map ,
$x_{t+1}^{(i)'} = r_2^{(i)'} x_t^{(i)'}(1 - x_t^{(i)'})$
2: Agent i generates cipher text $C = E_{x_t^{(i)'}}(M)$.
3: Agent i computes the key $x_t^{(i)}$ from logistic map
4: t ← t + 1
$x_{t+1}^{(i)} = r_1^{(i)} x_t^{(i)}(1 - x_t^{(i)})$
5: Agent i computes $MAC(C) = MAC_{x_i^{(t)}}(c)$
6: Agent i sends C||MAC(C) to the server.
7: Agent i updates its own counter t ← t + 1.
//Upon receiving a message C||MAC(C) from agent i.
8: Server generates the pair of keys $(x_i^{(i)}, x_t^{(i)})$ from the two logistic maps.
9: Server updates the parameter table with t ← t + 1.
10: Server updates the counter in the parameter table.
11: Server extracts the cipher text C and computes $MAC_{x_t^{(i)}}(C) = MAC(C)$.
12: if $MAC_{x_t^{(i)}}(C) = MAC(C)$ then
13: Server decrypts C using the key $x_t^{(i)'}$.
14: Server extracts the data A and timestamp T.
15: if T is consistent with the current system time then
16: Server responds the message based on the requests from the client;
17: else
18: Server discards the message.
19: end if
20: else
21: Server discards the message.
22: end if

VI. EXPERIMENTAL RESULTS

a. Confidentiality

Here symmetric key encryption with 256-bit key is used so the probability of an eavesdropper successfully cracking the key using a brute-force manner is 1/256. The secret keys are generated by logistic maps are only be used for one-time

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

encryption, which means that the key extracted by the attacker is of no use for decrypting any other messages. As a result, even if the attacker successfully cracks the secret key for one transmission, the attacker can not crack all the other keys within non-negligible probability.

b. Data Integrity and Authentication

The data integrity is provided by tagging the MAC to the ciphertext. In the sender side of view the MAC is generated by using the logistic map concept and that are not known to a third party. In the receiver side of view, the receiver can make sure that the message is not modified or altered during the transmission by computing and verifying the MAC of the ciphertext. Thus, one can see that the data integrity is protected. In addition, a third party cannot pass the authentication by forging a fake MAC as the third party does not have knowledge of the shared secret key.

c. Privacy

Here privacy is provided in two methods. First is here symmetric encryption algorithm is used to encrypt the original data so that data is kept confidential from a third party. And the second is that the smart home system design requires the agents to periodically report data to the server, which makes it harder for an attacker to perform inference attacks by monitoring the traffic.

d. Communication Overhead

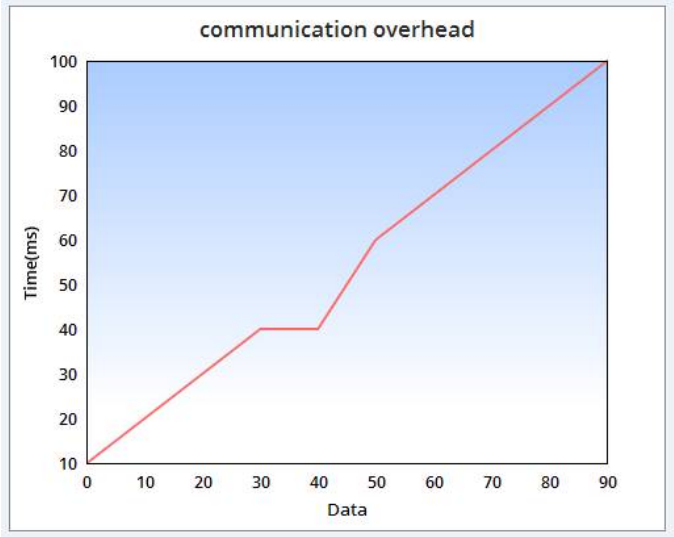

Fig 3 . Communication Overhead

By using the constrained application protocol the communication overhead is decreased from 45 percentage i.e in proposed work the 10kbps of data can be transmitted in 15ms and in the existing system this data is transmitted in 85 ms. In the privacy preservation protocol the key generation doesnot produce any communication overhead. And the communication overhead only occurs durning the messageexchange between the server and agent.

VII. CONCLUSION

This paper provides how the privacy preserving communication protocol and constrained application protocol works in a smart home. A smart home architecture consists of an appliance group, a monitor group, a central controller, and user interfaces. The agents in the appliance group and the monitor groups periodically report the current statuses to the central controller. To achieve security and privacy design privacy preserving communication protocol is provided with the symmetric key encryption and the message authentication code generation. The data transmission access control

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

within the wireless system through the wifi is controlled by the CoAP and a face recognition mechanism is provided so that the only home member can control the system.

REFERENCES

[1] Tianyi Song, Ruinian Li1, Bo Mei1, Jiguo Yu, Xiaoshuang Xing, Xiuzhen Cheng, "A Privacy Preserving Communication Protocol For Iot Applications In Smart Homes", IEEE Internet of Things, 2017.

[2] Ying-Tsung Lee, Wei-Hsuan Hsiao, Yan-Shao Lin, and Seng-Cho T. Chou, "Privacy-Preserving Data Analytics in Cloud-Based Smart Home with Community Hierarchy, IEEE Transactions on Consumer Electronics", Vol. 63, No. 2, May 2017.

[3] Mohsin B Tamboli, Dayanand DAmbawade (2016)," Secure and Efficient CoAP Based Authentication and Access Control for Internet of Things (IoT)", IEEE International Conference On Recent Trends In Electronics Information Communication Technology, May 20-21, 2016.

[4] Khusvinder Gill, Shuang-Hua Yang, Fang Yao, and Xin Lu ," A ZigBee-Based Home Automation System", IEEE Transactions on Consumer Electronics, Vol. 55, No. 2, MAY 2009.

[5] Earlence Fernandes, Jaeyeon Jung, Atul Prakash," Security Analysis of Emerging Smart Home Applications", IEEE Symposium on Security and Privacy, 2016.

[6] Pavithra.D, Ranjith Balakrishnan," IoT based Monitoring and Control System for Home Automation", IEEE Global Conference on Communication Technologies, 2015.

[7] Kalyani Pampattiwar, Mit Lakhani, Rinisha Marar and Rhea Menon, " Home Automation using Raspberry Pi controlled via an Android Application", International Journal of Current Engineering and Technology, 11 May 2017.

[8] E. Isa and N. Sklavos," Smart Home Automation: GSM Security System Design & Implementation", Journal Of Engineering Science and Technology Review, 15 January 2016.

[9] Antorweep Chakravorty, Tomasz Wlodarczyk, Chunming Rong," Privacy Preserving Data Analytics for Smart Homes", IEEE Security and Privacy Workshops, 2013.

[10] Pooja N.Pawar, Shruti Ramachandran, Nisha P.Singh, Varsha V.Wagh," A Survey on Internet of Things Based Home Automation System", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 4, Issue 1, January 2016.

[11] Ravi Kishore Kodali, Vishal Jain, Suvadeep Bose and Lakshmi Boppana," IoT Based Smart Security and Home Automation System", IEEE International Conference on Computing, Communication and Automation (ICCCA), 2016.

[12] Pooja Dahiya, Neha, Dr. SRN Reddy," IoT based Home Alert System using Wi-Fi and Cloud Technologies", National Conference on Product Design (NCPD), July 2016.

[13] Nisha Sangle, Shilpa Sanap, Manjiree Salunke, Sachin Patil, " Smart home system based on IoT", International Journal of Emerging Technology and Advanced Engineering, September 2016.