International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor :6.887
Volume 6 Issue I, January 2018- Available at www.ijraset.com

A Survey on Privacy Preserving Communication Protocol with CoAP in Smart Homes

Krishnenthu. P. Mani[1], Dr. S. Brilly Sangeetha[2]
[1] *M Tech Student,* [2] *Associate Professor & Head, Department of Computer science and Engineering,*
IES College Of Engineering, Thrissur, Kerala, India

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 moniter 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 on a per service basis.
Keywords*: *Constrained Application Protocol, Message Authentication Codes, Internet of things, Acknowledgement

I. INTRODUCTION

The Internet of things (IoT) consists of network of physical devices, vehicles, and other items embedded with electronics, software, sensors, actuators, and network connectivity which enable these objects to collect and exchange data. Now days IoT had made extra ordinary progress in both industrial and in academic fields. Home automation is building automation for a home, called a smart home. It involves the control and automation of home appliances. The main problem of IoT based smart home automation is that anybody can automate the system. If no security is provided the user privacy data can be easily taken by the attacker or any malicious entity. So to improve the energy efficiency and security privacy preserving communication protocol is used in the smart home. A privacy preserving communication protocol for IoT applications in smart homes system mainly consists of monitor group, appliance group, central controller and a user interface. 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. 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. Message Authentication Codes (MAC) scheme is provided to guarantee data integrity and authenticity. Symmetric-key encryption means a same key is used for both encryption of plaintext and for the decryption of cipher text. 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.

II. LITERATURE SURVEY

Ying-Tsung Lee, Wei-Hsuan Hsiao, Yan-Shao Lin & Seng-Cho T. Chou (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 data-hiding 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. But also it supported the functions of the surrounding environmental data being imported to enrich data analytics. 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. Data collected from smart home systems are divided into family-shared and individual data. A predefined format of data source is then generated through predefined classifications, such as main identifiers, semi-identifiers, sensitive data, and non-sensitive data. 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 platform provides access to predefined public information for analysis and management services. 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. During the interaction between devices [2], 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 Kerberos along 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 has two types of messages they are Confirmable message (CON) and Non Confirmable Message (NON). CON means a request message that requires an acknowledgement (ACK). The response can be sent either synchronously within the ACK or it can be sent asynchronously with a separate message. The other type is Non Confirmable Message (NON) in this a message that does not need to be acknowledged. 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, Shuang-Hua Yang, Fang Yao & Xin Lu (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. It mainly consists of four steps. The remote user can access the system using the Internet. The remote user's communications traverse the internet until it reach the home network and then wirelessly transmitted to the Home Gateway using the homes Wi-Fi network. The virtual home is provided on the home gateway. These communications are checked and processed by the home gateway and virtual home. Once checked the communications then sent to the real home automation system and the respective device. A local ZigBee based remote control can be used to directly control connected devices. The security and safety of the home automation network is done on the Home Gateway. ZigBee home automation network consists of a coordinator, routers and several end devices. During the initialisation phase, the coordinator scans the available radio channels to find the most suitable. All home devices connected to the ZigBee home automation network are assigned a fixed 64 bit MAC address. By using the ZigBee communications it will help to reduce the expense of the system.

Pavithra. D & Ranjith Balakrishnan (2015) proposed an IoT based Monitoring and Control System for Home Automation is used for monitoring and controlling the home appliances by World Wide Web [4]. The IoT-based architecture provides high-level flexibility at the communication and information. It is an approach which is used in many different environments such as patient monitoring system, security, traffic signal control or controlling various applications. The main objective is to design and to execute an cost effective and open source home automation system. The Infrared sensor (IR) is a low cost infrared object detection unit that is applied at home using IR LED's. It gets trigged when light is detected. When the sensor is sensed it sends a signal to raspberry pi. From the raspberry pi, by means of wifi configuration and IoT concept the system can turn ON/OFF the light. The PIR sensor is used to detect the human being presence and accordingly the fans are turned ON/OFF. The lights and fans are controlled by using a web server in personal computer, tablet or app in mobile. The fire detection sensor is triggered if there is any fire accident and immediately an alert message along with the image and video taken in camera is sent to mobile phone and an automatic phone call is made to nearby fire station. It mainly consists of physical layer, data link layer, network and transport layer and the application and presentation layer. The physical layer consists of the devices which are to be controlled. The data link layer consist of IoT gateway router, device manager and various communication protocols. The raspberry pi is used as the IoT gateway which communicates to personal computer or smart phone by means internet in the network and transport layer. The application and presentation layer consist of web portal which is nothing but designing a web page by which we can control the various appliances. The appliances can also be controlled by creating an app in mobile phone which is similar to web portal. The home automation provides the event of a home management and security system exploitation using Raspberry pi and Internet of Things technology. The system is suitable for real-time home safety monitoring and for remotely controlling the home appliances and protection from fire accidents with immediate solutions. The system may be employed in many places like banks, hospitals, labs etc for providing the security.

Kalyani Pampattiwar, Mit Lakhani, Rinisha Marar & Rhea Menon, 2017 proposed a home automation using raspberry pi controlled via an android application. Home Automation System (HAS) [5] provides a low cost wireless communication between a Raspberry Pi module and an android based application to the IP appliances at home. It controls electrical appliances in a home or office using an android application. The main control system implements wireless technology to provide remote access from raspberry pi. 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. The lighting, alarms, reminders and entertainment system can be remotely controlled by an android application in the user interfaces. The android application controls the Raspberry Pi. Regulating appliances means the appliances that fall under this category include fans and lights. The appliances mentioned can be switched on and off by using the android application. The reminders means the system can also be used to save reminders that help us with our important appointments or daily routines and the alarms can be set on the requested date and time in the system.

E. Isa & N. Sklavos, 2016 propsed smart home automation: gsm security system design & implementation [6], it provides a security system for smart home automation. Smart home automation has been developed at a great rate and many of the systems have been developed, that cover efficiently every possible security need. The systems detect the outbreak of fire at a very early stage by a temperature sensor, inform about a possible flood and some limit the human access at indoor and outdoor places. It consists of a microcontroller device, embedded in an Arduino system module. Arduino is an open-source electronic, prototyping, computing platform used for system development. It can be used to develop both stand-alone interactive objects, or can operate efficiently with software co-design, supported by another computing system. The GSM shield makes to send and receive short text messages, make voice calls and connect to the Internet. Along with the GSM an ethernet shield is provided to allow the microcontroller to connect to the Internet through an Ethernet wire. The microcontroller component is connected to I/O devices. Input devices include a keypad panel, a camera and a couple of sensors. The keypad panel is used for system control, like activation and deactivation, changes of both security levels and operation modes. Sensors units detect movements, or position changes of objects, in the areas of responsibility. . Camera is used for photos capture purposes, when an event happens, like a sensor activation or a change to the system's operation state: from activation to deactivation and opposite, etc. Output units include a LCD screen, a GSM shield and a speaker. The LCD screen supports a common user interface. The embedded GSM shield contains a SIM card, and it is used to send information, as short text messages to specific end users or to central security offices, in the case of alarms.

Antorweep Chakravorty, Tomasz Wlodarczyk & Chunming Rong, 2013 proposed Privacy Preserving Data Analytics for Smart Homes is for maintaining security & preserving privacy for analysis of sensor data from smart homes [7]. Privacy is associated with collection, storage, use, processing, sharing or destruction of personally identifiable data. The system consists of three modules and two storage units. The first module is the data collector. It is present at each smart home and transfers their sensor data to a data cluster at regular intervals. The second module is the data receiver. In this it receives the collected data sent by the data collector and transforms them into two different datasets. The storage unit, de-identified sensor data stores the actual data with primary identifiers values hashed. The identifier dictionary consists of hashed values and actual values for each unique set of primary identifiers. The third module is the result provider. It module controls end users access to data processing results. It authorizes the end users and ensures that privacy of any shared results is preserved. For security it replaces the personal identifiers of collected sensor data with hashed values before storing them into a de-identified storage. Separate identifier dictionary storage, with hashed and actual identifier values was also maintained as a point of reference for re-introduction of identifiers. It uses heuristic-based k-anonymization algorithms based on the end-users privacy level, requirements and authorization on the identifier dictionary storage. The hashed identifier from outputs of any data processing job on the de-identified store was replaced with their respective k-anonymized value, thus preserving privacy of any presented/shared results.

III.CONCLUSION

In this paper provides the survey on the privacy preserving communication protocol for the 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 a privacy-preserving communication protocol is provided with the symmetric key encryption and the message authentication code generation. The data transmission access control 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 (2017), "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 (2009)," A ZigBee-Based Home Automation System", IEEE Transactions on Consumer Electronics, Vol. 55, No. 2, MAY 2009.
[5] Earlence Fernandes, Jaeyeon Jung, Atul Prakash (2016)," Security Analysis of Emerging Smart Home Applications", IEEE Symposium on Security and Privacy, 2016.
[6] Pavithra.D, Ranjith Balakrishnan (2015)," 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 (2017), " 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 (2016), " 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 (2013), " 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 (2016), " 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 (2016), " 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 (2016), " 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 (2016), " Smart home system based on IoT", International Journal of Emerging Technology and Advanced Engineering, September 2016.