A Survey on Secure Protocols of Communication for IoT Components in Smart Homes

Dibin D Muttickel[1], Ambarish A[2]

[1]*M.Tech scholar, MCET, Thrissur, Kerala*
[2]*Asst. Prof. (CSE Department), MCET, Thrissur, Kerala*

---***---

Abstract - *The development of the Internet of Things (IoT) has made extraordinary progress in recent years in both academic and industrial fields. There are quite a few smart home systems that have been developed by major companies to achieve home automation. 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. In this paper, we propose an improved energy-efficient, secure, and privacy-preserving communication protocol for the smart home systems. We introduce a new method in which, data transmissions within the system are secured by an encrypted code with secret keys being generated by systems. Meanwhile, we incorporate Message Authentication Codes (MAC) to our scheme to guarantee data integrity and authenticity.*

***Key Words*:** **IoT, Smart Home, Communication Protocol, Arduino, Home Automation**

1. INTRODUCTION

The Internet of things (IoT) is the modern day technology which connects all type of devices 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. These days IoT had made large impact in both industrial and in academic fields. When IoT added with home components the home will become smart home. It involves the control and automation of home appliances. One of the concerns for IoT based smart home automation is, security-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. 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.

A privacy preserving communication protocol for IoT applications in smart homes system have an architecture of future smart home systems that contains home appliances and environment detectors as the agents, a central controller possessing a processor and a database as the brain of the system, and user interfaces for legitimate users to manipulate the agents via the central controller. Some of the attacks may arise when the end devices in a smart home send data frequently to the central controller and the types of the end devices used can disclose the identity of the user in the house then by this the information that can be captured by eavesdropping attacks. The two noteworthy difficulties of planning a secure smart home system are privacy and efficiency

To give the security in data transmission the brilliant home is secured by the symmetric encryption and the secrete key is produced by the framework for the encryption. Message Authentication Codes (MAC) scheme is to en-sure information data integrity and authenticity. Symmetric- key encryption suggests the same key is utilized for both encryption of plaintext and for the decryption of cipher text.

2. RELATED WORK

R. Yang and M. W. Newman published a survey based on Nest learning thermostat [1], using machine learning. The advantage is the thermostat can then learn people's behavior, at which temperature they are utilized to and when. Using built-in sensors and phones' locations but not understands the users intent.

M. Wang, G. Zhang, C. Zhang, J. Zhang, and C. Li proposes an IoT-based appliance control system with detailed specifications of hardware configurations [2]. Their architecture helps householders to remotely control home appliances through the connectivity. A smart central controller is the main component of the WSAN which is in charge of sorting out and setting up the wireless network with control modules. Each appliance is controlled by a relating control module. These adaptable control modules are in charge of controlling appliances and communicating with the central controller. The householder can on or off the light or other equipments using a smart phone or computer to monitor home appliances. Every appliances was associated with an assigned controlling module, which made home framework harder and costlier.

A. Chakravorty, T. Wlodarczyk, and C. Rong presented a privacy-preserving scheme such that presenting IoT data to central data analytics [3]. The system consists of three modules and two storage units; data collector, data receiver, result provider. . It authorizes the end users and guarantees that privacy of any shared results is protected

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 flexibility at the communication. It is an approach which is used in many different environments such as patient monitoring system, or controlling various applications.

A five layer architecture proposed by Y. Jie, J. Y. Pei, L. Jun, G. Yun, and X. Wei [5]. They introduced the use of Certification Authority (CA) to enhance the security quality. A double checking agent is there to verify if an entity is qualified to control other. Certification Authority (CA) enhances the security strength but high computational complexity will result in low energy efficiency.

Mohsin B Tamboli, Dayanand DAmbawade published [6] based on the system focuses on CoAP which provide fine grain access control. Adaptation of ECDSA (Elliptical Curve Digital Signature Algorithm) uses elliptic curve cryptography is the key behind this system. The proposed solution uses another verification and access control framework like Kerberos along with the CoAP protocol. It uses a digital signature of data is within smart things which gives efficient privacy. The principle advantages are it provides data integrity, Non-repudiation and Confidentiality.

Kalyani Pampattiwar, Mit Lakhani, Rinisha Marar & Rhea Menon, 2017 proposed a home automation using raspberry pi controlled via an android application [7] It provides a low cost wireless communication between a Raspberry Pi module and an android based application components at home. It uses wireless technology to provide remote access from raspberry pi. It performs setting alarms and reminders, smart security system and an entertainment system etc

Ying-Tsung Lee, Wei-Hsuan Hsiao, Yan-Shao Lin, and Seng-Cho T. Chou Introduces a cloud based smart home based on a 3-layered hierarchical architecture on [8]. The cloud based smart home is a three-layered hierarchical architecture contains 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 incorporated this information to a hierarchical architecture. And these are integrated in a cloud stage for data analytics access control mechanism. The cloud stage gave investigates information and Privacy preservation was then accomplished by coordinating access control mechanism. The advantage is that system performs data hiding to provide the privacy preservation.

Khusvinder Gill, Shuang-Hua Yang, Fang Yao, and Xin Lu proposed System is a ZigBee based home automation system [9]. This is a highly flexible and low cost system. It enables users to provide various options to control in addition to wifi such that zigbee controlled remote system. A gateway is provided between wifi and zigbee since they are heterogeneous systems. The signals from remote navigate through internet till the electrical component.

H. Ghayvat, J. Liu, S. C. Mukhopadhyay and X. Gui pro- posed The Wellness Protocol focuses an event and priority- based communication [10]. It offers sensible packet delivery metrics and expansive data handling. This covers complete smart home solution, beginning from the sensor hub to real-time analysis, data streaming, decision-making, and control. The sensor alone is not good adequate to process the data with the help of a XBee RF module, so an Intel Galileo Board was used.

E. Isa N. Sklavos proposed [11]. It provides a security system for smart home automation. Smart home automation has been developed at an incredible rate and a considerable lot of the systems have been developed, that productively cover every possible security required. The frameworks comprise of a microcontroller device, embedded in an Arduino system module. Arduino is an open-source electronic platform used for framework advancement. The GSM mobile makes to send and receive SMS-short text messages, make voice calls and associate with the Internet. Alongside the GSM an ethernet is also given. Input devices include various sesnors keyboard and camera. A LCD screen comprises of user interface area. The SIM card inside GSM module will help to communicate between devices.

M. Li, and H. J. Lin proposes Design and implementation of smart home control systems [12] based on Wireless sensor networks (WSNs) and power line communications (PLCs). Each home appliance is outfitted with a PLC receiver, which can directly get commands to control the home appliance and send answers about the state of the home appliance to the management station. A WSN, incorporates different sensor nodes and one coordinator is coordinated with the PLC transceiver data, such as temperature, illumination, and other. WSNs gathering ecological parameters and transmitting coordinators. The effect of wireless interference on the WSN data gathering subsystem is the main reasons for the proposed design are to expand the coverage of a smart home control network and relieve. But there are different technical problems between wireless network and power line communications.

C. Hu, H. Li, Y. Huo, T. Xiang, and X. Liao proposes a communication architecture for BANs, and design a method to secure the data communications between implanted /wearable sensors and the data sink/data consumers by utilizing CiphertextPolicy Attribute Based Encryption (CP ABE) and mark to store the information in ciphertext format at the data sink [13]. Firstly presents the framework introduction performed by KGC then it executed by KGC to create private keys for the clients. For each property a user possesses, a private key should be generated, which can be used later to decrypt a ciphertext if the attributes fulfil the access tree of the original data.

R. Teymourzadeh, S. A. A. Ahmed, K.W. Chan, and M.V. Hoong proposed testing and implementation of the smart home technology with Global System for Mobile Communication (GSM) modem to control home appliances[14]. In this framework outline, incoming SMS message is sent from the client cell to the GSM modem as a text message via the cellular network. The GSM modem by then point sends the directions in text mode to the PIC microcontroller. MAX232 is used for communication between both the GSM modem and PIC microcontroller. The microcontroller decodes information to give device address and command, then sends comparing signs to the driver of the power circuit. Also, the microcontroller guarantees dual independent task activity to turn on the device or switch it off.

W. S. Sayed, A. G. Radwan, and H. A. H. Fahmy, an arrangement of four summed up tent maps where the traditional guide is a unique case [15]. Maps has additional degrees of opportunity which give distinctive chaotic characteristics and increase the design flexibility required for a number of applications. A summed up bidirectional tent map with marked parameters is proposed. The general schematic for each map and its bifurcation diagram are included. The bifurcation structure for negative framework parameter case was called most positive tent map as per the greatest chaotic range of the alternating sign output.

J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, lays out a study on comprehensive overview of IoT with respect to system architecture, enabling technologies, security and privacy issues and present the integration of fog/edge computing and IoT, and applications[16]. They initially investigate the relationship between Cyber-Physical Systems (CPS) and IoT. At that point, existing structures, enabling technologies, and security and privacy issues in IoT are introduced to enhance the understanding of IoT advancement.

3. CONCLUSION

In this paper provides the review on Secure Protocols of Communication for IoT components in smart homes. A smart home architecture comprises of Components set, a controller set, a central administrator, and user interfaces. The members in component group and the controller groups continuously communicate the current statuses to the central administrator. To ensure security and privacy preservation, we outline a communication protocol for the components to communicate with the central administrator. We propose a lightweight secure and privacy-preserving communication protocol that uses chaotic encryption and Message Authentication Codes (MAC). MAC used to guarantee the integrity and authenticity of the data. Considering the restricted processing power on the components deployed in the smart home systems, we adopt a symmetric cryptographic system to encrypt the transmitted data. That is one-time secret keys used for encryption and MAC estimation are created based on two distinctive chaotic systems. As a result, our proposed system become high efficient and secure.

REFERENCES

[1] R. Yang and M. W. Newman, “Learning from a learning thermostat: lessons for intelligent systems for the home,” in Proceedings of the 2013 ACM international joint conference on Pervasive and ubiquitous computing. ACM, 2013, pp. 93–102

[2] M. Wang, G. Zhang, C. Zhang, J. Zhang, and C. Li, “An iot-based appliance control system for smart homes,” in Intelligent Control and Information Processing (ICICIP), 2013 Fourth International Confer- ence on. IEEE, 2013, pp. 744–747.

[3] A. Chakravorty, T. Wlodarczyk, and C. Rong, “Privacy preserving data analytics for smart homes,” in Security and Privacy Workshops (SPW), 2013 IEEE. IEEE, 2013, pp. 23–27.

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

[5] Y. Jie, J. Y. Pei, L. Jun, G. Yun, and X. Wei, “Smart home system based on iot technologies,” in Computational and Information Sciences (ICCIS), 2013 Fifth International Conference on. IEEE, 2013, pp. 1789–1791.

[6] 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.

[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] Y.-T. Lee, W.-H. Hsiao, Y.-S. Lin, and S.-C. T. Chou, “Privacy- preserving data analytics in cloud-based smart home with community hierarchy,”IEEE Transactions on Consumer Electronics, vol. 63, no. 2, pp. 200–207, 2017.

[9] 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.

[10] H. Ghayvat, J. Liu, S. C. Mukhopadhyay, and X. Gui, “Wellness sensor networks: A proposal and implementation for smart home for assisted living,” IEEE Sensors Journal, vol. 15, no. 12, pp. 7341–7348, 2015.

[11] E. Isa and N. Sklavos, "Smart home automation: Gsm security system design & implementation." Journal of Engineering Science & Technology Review, vol. 10, no. 3, 2017.

[12] M. Li and H.-J. Lin, "Design and implementation of smart home con- trol systems based on wireless sensor networks and power line com- munications," IEEE Transactions on Industrial Electronics, vol. 62, no. 7, pp. 4430–4442, 2015.

[13] C. Hu, H. Li, Y. Huo, T. Xiang, and X. Liao, "Secure and efficient data communication protocol for wireless body area networks," IEEE Transactions on Multi-Scale Computing Systems, no. 2, pp. 94–107, 2016.

[14] R. Teymourzadeh, S. A. Ahmed, K. W. Chan, and M. V. Hoong, "Smart gsm based home automation system," arXiv preprint arXiv:1806.03715, 2018.

[15] W. S. Sayed, A. G. Radwan, and H. A. Fahmy, "Design of a generalized bidirectional tent map suitable for encryption applications," in Computer Engineering Conference (ICENCO), 2015 11th International. IEEE, 2015, pp. 207–211.

[16] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1125–1142, 2017.