# A Survey on Privacy Preserving Communication Protocol for IoT Applications in Smart Homes

**Fathima U**

*M.Tech Student, Dept of Computer science and Engineering, Cochin College of Engineering, Malappuram, Kerala, India*

---

**Abstract -** The improvement of the Internet of Things (IoT) has gained extraordinary progress in recent years in both academic and industrial fields. There are many smart home systems that have been developed in significant organizations to accomplish home automation. Notwithstanding, the nature of smart homes unavoidably raises security and protection concerns. In this paper, we propose an enhanced vitality effective, secure, and privacy-preserving communication protocol for the smart home systems. In our proposed conspire, data transmissions within the smart home system are secured by a symmetric encryption plot with secret keys being created by chaotic systems. In the mean time, we consolidate Message Authentication Codes (MAC) to our plan to ensure guarantee data integrity and authenticity.

**Index Terms: Internet of things, smart home systems, privacy preservation, chaotic systems.**

## 1. INTRODUCTION

The Internet of things (IoT) comprises of a network of physical devices, vehicles, and different things implanted with hardware, software, sensors, actuators, and network connectivity which empower these objects to gather and trade information. The improvement of the Internet of Things (IoT) has gained extraordinary progress in recent years in both academic and industrial fields. Home automation is building automation for a home, called a smart home. It includes the control and automation of home appliances. In previous couple of years, there is a creating excitement on smart home system. The primary issue of IoT based smart home automation is that anyone can automate the system. On the off chance that no security is given the client protection information can be effortlessly taken by the by the attacker or any malicious entity. In this way, to enhance the vitality productivity and security protection security privacy preserving communication protocol is used in the smart home.

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. We take into considerations that the agents in smart home systems usually have limited computing capability and performing asymmetric encryption and decryption will be exposed excessively processing assignments on the agents.

In this manner, we pick MAC over digital signature to achieve integrity and authentication. The chaos-based cryp-tography has been widely adopted in securing communica-tions. A chaotic system is extremely sensitive to the initial conditions. With slightly different inputs can be significantly different. The butterfly impact feature makes chaos-based cryptography extremely suitable for key generations. One of the popular chaotic systems the logistic map to generate one-time symmetric keys to secure data transmissions.

## 2. RELATED WORKS

M. Wang, G. Zhang, C. Zhang, J. Zhang, and C. Li proposes an IoT-based appliance control system with detailed specifications of hardware configurations[1]. Their proposed architecture enabled householders to remotely manipulate home appliances through the Internet. A wireless approach can replace wire harnesses inside home network identifying and control system applications. Furthermore, with the self- configuration and self-organization technologies, an appli-ance takes part into or withdraws from a home network effortlessly.

A smart central controller is the core 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. At the point when a home has been introduced such a control system, the householder can utilize a smart phone or computer to monitor home appliances and carry out some operations remotely, such as turn on or off a light. Nonetheless, in their design, every one of the appliances was associated with an assigned controlling module, which made acknowledgment of such a savvy home framework harder and costlier.

R. Yang and M. W. Newman published a survey based on Nest learning thermostat[2]. The Nest utilizes machine learning, detecting, and networking technology, as well as eco-criticism highlights. The advantage is the thermostat can then learn people's schedule, at which temperature they are utilized to and when. Using built-in sensors and phones' locations, it can shift into energy saving mode when it understands no one is at home. The problem is the Nest Thermostat system was having trouble understanding the users intent when the users manually adjusted the thermostat.

Y. Jie, J. Y. Pei, L. Jun, G. Yun, and X. Wei published[3]. They proposed a five layer architecture that contained re- source layer, interface layer, agent layer, kernel layer, and user application layer. They introduced the use of Certifi-cation Authority (CA) to enhance the security quality. A dual checking process to verify if an entity is qualified to manipulate another entity. The advantage is incorporated security measures to their system that utilized RFID tags to uniquely identify an appliance. They introduced the use of Certification Authority (CA) to enhance the security strength. However, the implementation of CA on the agents features high computational complexity that will result in low energy efficiency.

A. Chakravorty, T. Wlodarczyk, and C. Rong presented a privacy-preserving scheme for multiple smart home systems to present their data to central data analytics[4]. Privacy is associated with gathering, storage, use, processing, sharing or devastation of by and by identifiable information. 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 exchanges their sensor information to a data cluster at standard interims. The second module is the data receiver. In this it gets the gathered information sent by the data collector and changes them into two different datasets. The storage unit, de-identified sensor data stores the real data with primary identifiers values hashed. The third module is the result provider. It authorizes the end users and guarantees that privacy of any shared results is safeguarded.

The identities of the clients in each smart home and the related data are hashed and stored in an identifier dictionary. At the point When the data analytic was required to analyze the data, it de-identified the clients and their data by finding them up in the identifier dictionary. The primary preferred standpoint, it is ensured that the legitimate entities can acquire the real data and that malicious entities are not able to access the real data.

Ying-Tsung Lee, Wei-Hsuan Hsiao, Yan-Shao Lin, and Seng-Cho T. Chou proposes a cloud based smart home based on a three-layered hierarchical architecture on[5]. A smart community public housing projects consist of a huge number of households. The cloud based smart home is a three-layered hierarchical architecture contains home con- troller, 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. Furthermore, these are integrated in a cloud stage for data analytics access control mechanism. The community broker not only performed home and community-level information partition and accumulation.

The cloud stage gave free to information investigation, questions, and administration. Privacy preservation was then accomplished by coordinating informing, enforcement and a fine-grained access control mechanism of the communities and homes. Data collected from smart home systems are separated into family-shared and individual data. The com- munity

broker provides security assurance in the community and home levels through data separation, aggregation, and fusion. The cloud stage gives access to predefined public information for investigation and management services. The principle advantage is that system performs data minimiza-tion and data hiding to provide the privacy preservation in the cloud-based smart home. In any case, to approve singular relatives more refined customized benefit proposals required. Also, future research should additionally examine how to affirm approval in apparently less-private communities which lack stakeholders or agents.

Mohsin B Tamboli, Dayanand DAmbawade published[6] based on the system focuses on CoAP which provide fine grain access control. The proposed solution uses another ver-ification and access control framework like Kerberos along with the CoAP protocol and an fication and access control framework like Kerberos alongside the CoAP convention and an upgraded adaptation of ECDSA (Elliptical Curve Digital Signature Algorithm) uses elliptic curve cryptography. It is utilized to make a digital signature of data is implemented within smart things which gives efficient privacy. CoAP has two kinds of messages they are Confirmable message (CON) and Non Confirmable Message (NON). CON implies a demand message that requires an affirmation (ACK). The reaction can be sent either synchronously inside the ACK or it tends to be sent asynchronously with a different message. The other sort is Non Confirmable Message (NON) in this a message that does not need to be acknowledged. CoAP also supports the block wise transfer of huge messages in which it parts messages and sends them with reference order.

The principle favourable circumstances of the framework are it provides data integrity, Non-repudiation and Confiden-tiality. The issue is proposed solution uses another validation and access control framework like Kerberos alongside the CoAP protocol. It gives the sensors to computational over- head.

Khusvinder Gill, Shuang-Hua Yang, Fang Yao, and Xin Lu proposed System is a novel, stand alone, low-cost and flexible ZigBee based home automation system[7]. The sys- tem enables home owners to monitor and control the devices in the home, through a variety of controls. The controls incorporated into the framework are ZigBee based remote control, and any Wi-Fi empowered gadget. A gateway is provided between heterogeneous Zigbee and Wi-Fi networks, and facilitates local and remote control and monitoring over the homes devices it basically comprises of four stages. The remote client can get to the framework using the Internet. The remote users communications traverse the navigate the web until the point when it achieves the home system and then wireless transmitted to the Home Gateway using the homes Wi-Fi network. The virtual home is given on the home gateway. These interchanges are checked and processed by the home gateway and virtual home. The security and safety of the home automation network are done on the Home Gateway.

Pavithra.D, Ranjith Balakrishnan proposed an IoT based Monitoring and Control System for Home Automation is used for monitoring and controlling the home appliances by World Wide Web[8]. The IoT-based architecture gives high- level adaptability at the communication and information. It is a methodology which is a wide range of conditions, for example, patient monitoring system, security, traffic signal control or controlling different applications. The fundamental goal is to design and to execute a cost-effective and open source home automation framework. The Infrared sensor (IR) is a low cost infrared object recognition unit that is connected at home using IR LED. It gets trigged when the light is identified. At the point when the sensor is detected it sends a flag to the raspberry pi. From the raspberry pi, by methods for wifi setup and IoT concept the system can turn ON/OFF the light.

It for the most part comprises of physical layer, data link layer, network and transport layer and the application and presentation layer. The physical layer comprises of the devices which are to be controlled. The data link layer con-tains the IoT gateway router, device manager and different communication protocols. The raspberry pi is used as the IoT gateway which communicates to personal computer or smart phone by implies internet in the network and transport layer. The application and presentation layer comprises of a web portal which is only designing a web page by which we can control the different appliances. The appliances can likewise be controlled by making an app on a mobile phone which is like a web portal. The system is appropriate for real- time home safety monitoring and for remotely controlling the home appliances and protection from fire accidents with quick arrangements. The system might be utilized in numerous spots like banks, hospitals, labs and so forth to give the security. Be that as it may, a controlling and consistent observing framework to control different home machines with an Android advanced mobile phone.

Kalyani Pampattiwar, Mit Lakhani, Rinisha Marar Rhea Menon presented[9]. Home Automation System (HAS) pro- vides a low cost wireless communication between a Rasp- berry 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 principle control framework implements wireless technology to give remote access from raspberry pi. It plays out the activi-ties, for example, controlling the lighting, setting alarms and reminders, smart security system and an entertainment system. For the security a smart doorbell is introduced. The incorporates speakers associated with the Raspberry Pi through Bluetooth. The android application manages the Raspberry Pi.

E. Isa N. Sklavos proposed[10]. It provides a security sys- tem 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, prototyping, computing platform used for framework advancement. The GSM shield makes to send and receive short text messages, make voice calls and associate with the Internet. Alongside the GSM an ethernet shield is given to permit the microcon- troller to interface the Internet through an Ethernet wire. The microcontroller segment is connected to I/O devices. Input devices include a keypad board, a camera and a couple of sensors. The keypad board is used for system control, similar to activation and deactivation, changes of both security levels and activity modes. Sensors units identify movements, or position changes of items in the zones of obligation. A camera is utilized for photographs catch purposes, when an event occurs, similar to a sensor actuation or a change to the framework's task state: from activation to deactivation and opposite, and so forth. Output units include a LCD screen, a GSM shield and a speaker. The LCD screen underpins a typical user interface. The embedded GSM shield contains a SIM card, and it is used to send data, as short text messages to particular end clients or to central security offices, in the case of alarms.

H. Ghayvat, J. Liu, S. C. Mukhopadhyay and X. Gui pro- posed The Wellness Protocol focuses an event and priority- based communication[11]. It offers sensible packet delivery metrics and expansive data handling. This protocol 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. The sensor data is sent to Intel Galileo where it is handled by two algorithms, one is packet encapsulation, and the other is intelligent sampling and con- trol. The packet encapsulation algorithm is common for all sensor hubs in a network while the intelligent sampling and control algorithm is designed independently as indicated by sensor compose and its application. The preferred standpoint is they Uses WSN conventions which is backbone numerous frameworks and they give a safe environment for the well- being of its occupants. But the predictive decision is not to present also the energy consumption is comparatively high.

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 transceiver, which can directly get commands to control the home appliance and send answers about the state of the home appliance to the management station. An isolated WSN, which incorporates different sensor nodes and one coordina-tor that is coordinated with the PLC transceiver, is deployed in each room to gather ecological data, such as temperature, illumination, humidity, and other data. WSNs are in charge of gathering ecological parameters and transmitting them to WSN coordinators. While PLCs are used as a network back- bone to associate all WSN coordinators and exchange the gathered ecological information to the management station and the control messages to home appliances. The primary reasons for the proposed design are to expand the coverage of a smart home control network and relieve the effect of wireless interference on the WSN data gathering subsystem. But there are different technical problems between wireless network and power line communications.

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 Communi- cation (GSM) modem to control home appliances[13]. In the proposed 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 to empower the communication between both the GSM modem and PIC microcontroller. An outgoing message from the framework containing the home appliances status is conveyed to the mobile phone through GSM modem. The microcontroller gets guidelines and decodes them 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. A feedback status of any devices under control whether turned on or off will be given by the microcontroller. The devise can be controlled from a long distance and they are practical outline likewise effortlessly actualized in homes. But they are network dependent and they just permit to send the message in a settled configura-tion.

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[14]. They initially investigate the relationship between Cyber-Physical Systems (CPS) and IoT, the two of which play important roles in understanding a smart cyberphysical world. At that point, existing structures, enabling technologies, and security and privacy issues in IoT are introduced to enhance the understanding of IoT advancement.

To explore the fog/edge computing-based IoT, they like- wise examine the relationship between IoT and fog/edge computing and talked about issues in fog/edge computing- based IoT. At last, a few applications, including the smart grid, smart transportation, and smart cities, are introduced to show how fog/edge computing-based IoT to be implemented in real world applications. CPS underlines the associations among cyber and physical components and has an objective of making the monitoring and control of physical compo- nents secure, efficient, and intelligent by leveraging cyber components. CPS and IoT can quantify the state information of physical components via smart sensor devices without humans input. In the interim, in both CPS and IoT, the measured state data can be transmitted and shared through wired or wireless communication systems.

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 /wear- able sensors and the data sink/data consumers by utilizing Ciphertext-Policy Attribute Based Encryption (CP ABE) and mark to store the information in ciphertext format at the data sink[15].Our method comprises four Algorithms. Algorithm 1 presents the framework introduction performed by KGC. Algorithm 2 is 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. The encryption scheme is detailed in Algorithm 3: a session key K should be encrypted with an access tree T determined by the sensor, which is known as the sender in the protocol. Algorithm 4 implements decryption and authentication, which ought to be executed by the data consumer to get the session key in light of his properties and the corresponding secret keys for his characteristics since he receives only encrypted data from the sensor/sender. Note that Algorithm 4 is like the initially proposed by CP ABE. In the meantime, outlines a convention to secure the data communications between implanted /wearable sensors and the data sink/data consumers. The challenge is the means by which to reduce the calculation cost for better use in the BAN.

E. Fernandes, J. Jung, and A. Prakash propose the first inside and out exact security analysis of one such rising smart home programming platform[16].The Smart Things ecosystem consists of three major noteworthy parts: hubs, the SmartThings cloud backend, and the smartphone companion app. Each hub points, bought by a client, supports different radio protocols including ZWave, ZigBee, and WiFi to in- teract with physical devices around the clients home Clients deal with their hubs, associate devices with the hubs, and install SmartApps from an app store using the smartphone partner application. The cloud backend runs SmartApps. The cloud backend likewise runs SmartDevices, which are programming wrappers for physical devices in a clients home. The sidekick application, hubs, and the backend impart over an exclusive SSL-ensured protocol. SmartApp can send SMSs and make network calls using SmartThings APIs. SmartDevices speak with the hub over an exclusive convention. Our procedure included making a rundown of potential security issues in view of our investigation of the SmartThings design and widely testing every potential security issue with model SmartApps.

W. S. Sayed, A. G. Radwan, and H. A. H. Fahmy, an ar- rangement of four summed up tent maps where the traditional guide is a unique case [17].Maps have 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.

SVinod Choudhary, Aniket Parab, Satyajit Bhapkar, Neetesh Jha, Ms. Medha Kulkarni propose a mobile and web based Smart Home framework that comprises of a mobile phone with android capabilities, a web based application, and a home server[18]. The fundamental destinations are to design and implement a home automation system using IoT that is equipped with controlling and automating most of the house appliances through a simple sensible web interface. The proposed framework has a great adaptability by using Wi-Fi innovation to interconnect its distributed sensors to the home automation server. This will reduce the deployment cost and will build the capacity of upgrading. The proposed plan of

Smart home is using the Wi-Fi as the interfacing media to associate with the database. They use hardware description Arduino Uno R3, Channel Relay, PIR Sensors and Temperature Sensor. Also, software description as Android SDK and Arduino IDE. Its an ease, secure auto- configurable, remotely controlled solution. The composed framework not just screens the sensor information, like temperature, motion sensors, yet in addition impels a procedure as per the necessity. It also stores the sensor parameters in the database in a timely manner. The proposed system is better from the scalability and adapt- ability perspective than the commercially available home automation systems.

P. Tobin, L. Tobin, M. M. Keever, and J. Blackledge, proposed framework producing boundless interesting OTPs to encode data locally by the end-client using systems[19]. Exporting PSpice analogue signals using copy and paste does not work for digital data. Instead, binary signals are exported using Vector1 parts which indicate the registry area and record name. The Javascript application ignores the time vector and an algorithm concatenates the set and reset bit to form the OTP. The objective was to fleeting data and evacuate the bit 00 and 11 pairs- states that should never happen. A biased OTP was created by running a short simulation to show unwanted examples in the encrypted image. The VN algorithm ought to be connected to two uncorrelated information streams but this is tended in the final circuit by XORing two chaos independent data streams from Lorenz and Chua oscillators. This arrangement gives more prominent control and finish certainty to the end client security on the grounds that the OTP is the main demonstrated unbreakable cipher- provided it is utilized just once. This condition is met anyway as another OTP is created each time new data is uploaded to the cloud.

L. Kocarev proposed chaos-based cryptography[20]. Al- most all chaos-based cryptographic algorithms use dynamical frameworks characterized on the set of real numbers, and in this manner are troublesome for viable acknowledgment and circuit implementation. Security and execution of all proposed chaos-based methods are not examined as far as the procedures created in cryptography. Besides, the vast majority of the proposed techniques create cryptographically frail and moderate algorithms. Cryptography is by and large recognized as the best technique of data protection against passive and active fraud. Diffusion implies spreading out of the impact of a single plaintext digit over numerous ciphertext digits so as to hide the statistical structure of the plaintext. An extension of this thought is to spread the impact of a single key digit over many digits of ciphertext. Confu-sion implies the use of transformations which complicate dependence of the statistics of ciphertext on the statistics of plaintext. The blending property of chaotic maps is firmly identified with the diffusion in encryption changes. While the motion of the dynamical framework in the continuous (microscopic) state space is deterministic, its motion in the partitioned (macroscopic) space is stochastic and the trajec- tories are sequences of symbols. A chaotic system merely converts the data about its underlying state into a form which is noticeable to the measuring system. The Imperative issue in chaos based cryptography is whether chaos can offer improvements to the performances of cryptographic algorithms.

## 3. CONCLUSION

In this paper provides the review on the privacy preserving communication protocol for the smart home. A smart home architecture comprises 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 guarantee security and privacy preservation, we outline a communication protocol for the agents to communicate with the central controller. We propose a lightweight secure and privacy-preserving communication protocol that uses chaos- based encryption and Message Authentication Codes (MAC). We join MAC to guarantee the integrity and authenticity of the data. Considering the restricted processing power on the agents deployed in the smart home systems, we adopt a symmetric cryptographic system to encrypt the transmitted data. The one-time secret keys used for encryption and MAC estimation are created based on two distinctive chaotic systems. As an outcome, our proposed plot accomplishes high efficiency and security level.

## REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] M. B. Tamboli and D. Dambawade, "Secure and efficient coap based authentication and access control for internet of things (iot)," in Recent Trends in Electronics, Information & Communication Technology (RTEICT), IEEE International Conference on. IEEE, 2016, pp. 1245– 1250.

[7]K. Gill, S.-H. Yang, F. Yao, and X. Lu, "A zigbee-based home automation system," IEEE Transactions on consumer Electronics, vol. 55, no. 2, 2009.

[8] D. Pavithra and R. Balakrishnan, "Iot based monitoring and con- trol system for home automation," in Communication Technologies (GCCT), 2015 Global Conference on. IEEE, 2015, pp. 169–173.

[9] K. Pampattiwar, M. Lakhani, R. Marar, and R. Menon, "Home automation using raspberry pi controlled via an android application," 2017.

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

[11] 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.

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

[14] 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.

[15] 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.

[16]E. Fernandes, J. Jung, and A. Prakash, "Security analysis of emerging smart home applications," in 2016 IEEE Symposium on Security and Privacy (SP). IEEE, 2016, pp. 636–654.

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

[18] V. Choudhary, A. Parab, S. Bhapkar, N. Jha, and M. M. Kulkarni, "Desgin and implementation of wi-fi based smart home system," 2016.

[19] P. Tobin, L. Tobin, M. Mc Keever, and J. Blackledge, "Chaos-based cryptography for cloud computing," in Signals and Systems Conference (ISSC), 2016 27th Irish. IEEE, 2016, pp. 1–6.

[20] L. Kocarev, "Chaos-based cryptography: a brief overview," IEEE Circuits and Systems Magazine, vol. 1, no. 3, pp. 6–21, 2001.