Smart Home Automation Security Design Using Data Encryption

Ihsan Faishal Rasyid - 18217032

Majoring on Information System and Technology Studies, Sekolah Teknik Elektro dan Informatika (STEI) Institut Teknologi Bandung

Abstract: Smart Home is a technology that functions intelligently connecting various sensors and information technology-based devices to facilitate the automation of household appliances, home lighting, heating, and cooling systems, as well as security and safety systems at home. Although the application of Smart Home technology promises ease and comfort in carrying out daily life at home, many technical challenges must be overcome to achieve guaranteed comfort and safety. Special security design is needed for access control and considers how to set a simple and safe access control policy for visitors for the devices and home resources that visitors use. The design of Smart Home tends to be systematic, intelligent, and convenient and can be arranged in the form of a set of security protection systems for web-based Smart Home which accesses data through an encryption process.

Index Terms: Automation, Cloud, Data Security, Encryption, IoT, Network, Smart Home

1. INTRODUCTION

Smart Home technology promises ease and comfort in carrying out daily life at home. Promises ease and comfort so nowdays Smart Home technology is growing so fast and big in the market as an tertiary need for people. Market research by Zion‟s Market Research shows that the value of smart home in 2016 was USD 24.10 billion and in 2022 it is expected to grow to USD 53.45 [1]. A smart home is linking together computer innovation, pervasive technology, image processing, advanced communication technology and finally a network of connected devices to deliver services to home users [2]. The conventional digital home is connected based on wired technology which imposes constraint such as setting up the cabling, costly installation, and poor system scalability. Whereas today smart home is designed in a wireless sensor network, absorb less installation cost and support great system versatility [3]. The important aspects of users adopting smart home are because of energy efficient, home security, convenience, entertainment, remote health monitoring and connectivity [2].

Tremendous development of Internet and communication technologies has lead smart home for a better home facilities. In the smart home environment, internet of things (IoT) is one of the technologies that play a crucial role in connecting various devices to IoT application to track user‟s activities and acquire data generated in the home [5]. An immense amount of resources are being invested by the government bodies and industries in providing the public with technologies related to IoT and smart home. [4]. IoT is an evolving technology that embeds physical devices, vehicle, appliances, sensors, intermediate devices which helps to communicate between these devices to make our lives smarter. Most smart home devices are supported by both wired and wireless communications.

In smart homes, different home appliances for example, lighting, AC, CCTV cameras, smart TV, washing machines and other items are controlled by using a remote, smartphone or a tablet [1]. Integrated homes display a dynamic way of viewing and controlling the devices [4].

The purpose of writing this research paper is to understand the technical work of a smart home system that uses information assets while the system works by providing comfort and ease of management of household facilities, information asset transfer mechanisms along with threats to the security of information accessed, and home security design applications. Smart Home is ideal by applying data encryption methods. The structure of the rest of the paper will be as follows:

1. Section 2 – Smart Home System Explanation
2. Section 3 – Smart Home Security Threats
3. Section 4 – Encryption Methods
4. Section 5 – Data Encryption Implementation on Smart Home Security
5. Section 6 – Conclusion

2. SMART HOME SYSTEM EXPLANATION

Smart Home has to be understand as a system that provides easiness for people to do their daily home needs by implements computer innovations, pervasive technologies, image processing, advanced communication technology, and a network of connected devices to deliver services to home users. To have a better understanding of the smart home system, it has to be known some preliminary explanation about smart home that includes: Definition of Smart Home, Purpose of Smart Home, Smart Home Architecture, Internet of Things and Smart Home Relationship, Cloud and Smart Home Relationship, and Application in Smart Home.

2.1. Definition of Smart Home

A smart home is a place with heterogeneous systems to many front devices with the support of embedded information and communication architectures [6]. Meanwhile, [7] describe the smart home as a home with an integration of digital sensing and communication devices to produce services through seamless communications. The technology of a home which makes the housework or household activity to be automated is named home automation [8].

The types of home automation are technology in controlling lights, air conditioner and heating appliances, high-security gates and locks [9][10][14]. Researcher [11], mentions that a smart home is a home with reduced or no human intervention, produce services and information from a composite of other information. Moreover, the smart home is a standard home with a few home automation systems that basically extract the data representing the environment and information gathered at home reliably supports the home services [10].

2.2. Purpose of Smart Home

Smart Home has a purpose of providing services such as control of energy, better security, and home entertainment, dependent and independent lifestyle planning [7]. Its objective is also to reduce human intervention to operate manual homes and help users to get services and information gathered from the smart home. [2]. A smart home is recognized to give convenience, tranquility and centralizing access to control automation [12]. The purpose of smart is to provide home users support in decision making and informed choices through equipping them with important information about their household context [13].

2.3. Smart Home Architecture

Since the concept of IoT was introduced to the smart home implementation, this field knew some great changes and improved a lot. Smart home is designed to make houses more automated and intelligent to offer the residents a comfortable life where they can easily control and monitor all devices inside the home. According to Satpathy[15]: “A home which is smart enough to assist the inhabitants to live independently and comfortably with the help of technology is termed as smart home. In a smart home all the mechanical and digital devices are interconnected to form a network which can communicate with each other and with the user to create an interactive space”.

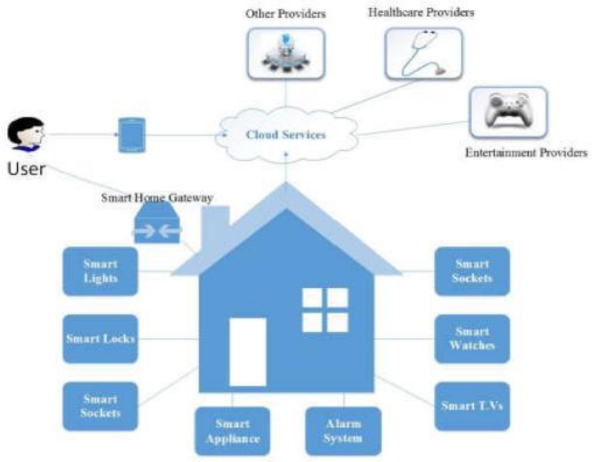

Figure 1. Architecture of a smart home [15]

A smart home comprises a multitude of devices that supports different communication technologies. They are connected to applications and gateways providing connectivity to the Internet and building a tunnel between different technologies within the house. These devices form a heterogeneous network by interacting and cooperating with each other. The user connects to the smart network using smartphones, tablets, etc.

We can identify three elements that guarantee the success of the smart home concept:

- Connected objects (IoT).
- Cloud
- Applications

2.4. Internet of Things and the Smart Home Relationship

There is no standard, unified and shared definition of the Internet of Things but after several researches, a definition that we found more relevant “the Internet of Things is a network of networks which enables the identification of digital entities and physical objects – whether inanimate (including plants) or animate (animals and human beings) – directly and without ambiguity, via standardized electronic identification systems and wireless mobile devices, and thus make it possible to retrieve, store, transfer and process data relating to them, with no discontinuity between the physical and virtual worlds”.

In Figure 2 [16] we describe the main and the most important communication protocols used in a smart home based on the Internet of Things (IoT) according to the OSI model. Those protocols provide the communication between the components of a smart home and transport the information between devices.

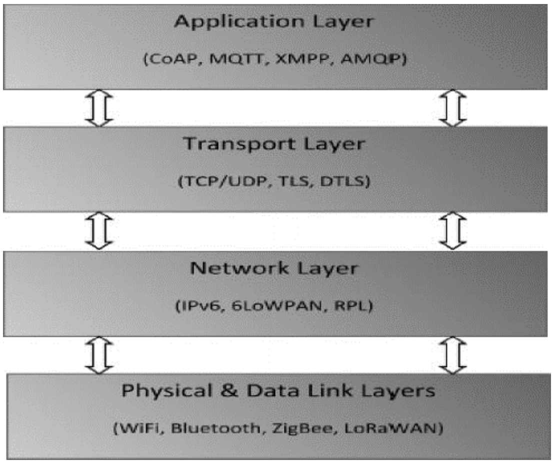

Figure 2. IoT Protocols[16]

Physical and Data Link Layers: The most well known physical and data Link layers protocols used to construct the smart home are WiFi, Bluetooth, ZigBee based on the 802.15.4 standard and LoRaWAN.

Network Layer: Network layer protocols for the IoT and smart home applications are responsible for connecting the smart things, network devices and servers. Thanks to IPv6 functionalities (the large address space, stateless and stateful address configuration) needed by the IoT applications including smart homes to enable addressing (without using NAT Translation) of smart devices andbthe direct routing of packets. Other protocols are used such as IPv6 over Low power Wireless Personal Area Networks (6LoWPAN) and Routing Protocol for Low power and Lossy Networks (RPL).

Transport Layer: Regarding the transport layer which ensures that the data is sent rapidly and efficiently, UDP is preferred as a simple OSI transport layer protocol for client/server network applications based on IP and Datagram Transport Layer Security (DTLS) which provides communications privacy for datagram protocols and a better security in a way to prevent eavesdropping, tampering, or message forgery.

Application Layer: The application layer is responsible for delivering specific application to the user. The most important application layer protocols for IoT and smart home environments are Constrained Application Protocol (CoAP), MQ Telemetry Transport (MQTT), eXtensible Messaging and Presence Protocol (XMPP) and Message Queuing Protocol (AMQP).

2.5. Cloud and the Smart Home Relationship

The data generated every second from smart home may contain very important and private information, but its amount can be too much to store or to be analyzed locally. To solve these problems, the cloud computing has been adopted in smart home environment. The cloud is the most important and complex part integrated in the smart home architecture. The smart home can send data into the cloud; the user’s devices will be connected to the cloud where he has the access to the shared data when he needs it.

Recently, the term cloud computing has become more and more popular in our daily life where we can store our important files and data to prevent a computer fault from destroying it. The main task of the cloud computing is that it can adapt to user’s conditions and to different circumstances such as CPU speed, memory size, storage space , etc.

The NIST organization defines: “Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics (On-demand self-service, Broad network access, Resource pooling, Rapid elasticity, Measured Service); three types of services (Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS), Cloud Infrastructure as a Service (IaaS)); and four deployment models (Private cloud, Community cloud, Public cloud, Hybrid cloud)”.

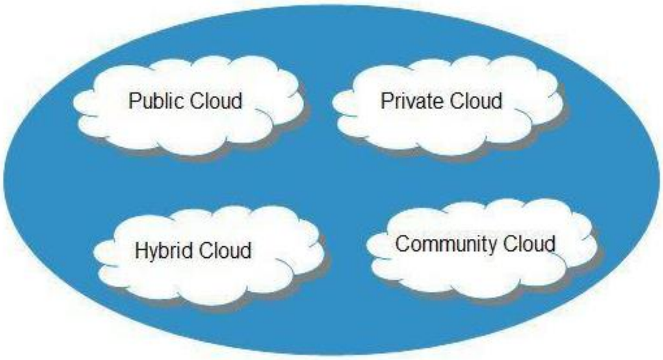

Figure 3. Four Cloud Deployment Models [17]

Generally, there are four deployment models for a cloud infrastructure: private, hybrid, public and community cloud. A private cloud is used only by the same company or by a third party and still be a private cloud for that company, this type of cloud is secure and easy to maintain but it needs a high cost to deploy it. In the public cloud different users from anywhere can easily access the public cloud via a public network like the Internet, this type of cloud has security issues and it is vulnerable to attacks. The hybrid cloud is a combination of multiple cloud computing models interconnected with each other to offer more benefits to the environment. And the community cloud is shared by different organization belong to the same community, it is usually hosted externally but it may be hosted internally by a member.

In addition, there are three types of services in use by the cloud models. Those services are Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). IaaS aims to provide access to a virtualized computer park. The consumer is capable to install an operating system or applications, for example: Openstack, OpenNebula, etc… In the PaaS the operating system and infrastructure tools are under the responsibility of the vendor. The consumer has control only on the applications but he doesn’t have the control over the underlying infrastructure like Amazon Web Services. The applications in SaaS are available to consumers; they can be manipulated using a web browser, emails…from many devices like computer, mobile or tablet. Example of SaaS: Google Docs, Gmail, etc.

2.6. Applications in Smart Home

In smart homes, there are many kinds of applications, which provide intelligent and automated services to the user which makes his life more comfortable and even more interesting. Those applications help in the daily activities and help in maintaining a routine for individuals. Some of these applications are:

Smart bed: Smart bed system can be fabricated as a part of the smart home to provide a safe, sound and secured living environment for the inhabitant of smart home for example to monitor an elderly person or disabled person living alone [18].

Smart refrigerator: The smart refrigerator can meet the user's need with food storing function, it is equipped with a shopping and storage application that require managing and tracking the products in the refrigerator as well as sending an alert to the user if a product is about to pass its expiration date or it has not been used in a long period [19].

Smart window: Smart window system is a very important part of smart home. The windows are automatically controlled opened and closed by measuring environmental parameters. This system is developed to control the wind, the rain, the smoke…to make reasonable judgment to protect the user [20].

Smart locks: Smart lock system is very important especially because it is related to the safety of the user. The user can simply use his mobile to open and close door also he can monitor who is entering and leaving his home while he is absent [21].

Smart light: A lighting control system for smart homes has been developed and implemented to automatically control light in the home based on the movement of the user, it can turn off automatically when the room is unoccupied and it can turn on when the user enter the room [22].

Smart TVs: Smart TV provides better environment for watching TV contents due to Ultra High Definition (UHD) along with watching movies, playing games, browsing, and full support for web 2.0 features that allows viewers to satisfy their need by using the smart TV large screen. In addition, beside storage capabilities, processing and connectivity, smart TVs have full support for internal and external sensors, such as camera, face detection and recognition, voice recognition [23].

3. SMART HOME SECURITY THREATS

Smart Home includes home appliances, control for each system within the home. It's deployed various technologies including sensors, devices and appliances which are communicating to each other or to the user [24]. In a smart home environment, there are various devices with different mechanisms, so the security depends on which device used. But the smart home elements consists of IoT implementations, Cloud technology implementations, and application to device also home facilities or appliances. Those implementations in smart home system raise security threats to the information and privacy from the home users.

Informations are transferred every time the smart home system is being used through various communication technologies. The smart home uses various communication technologies such as: LAN, WAN and Wireless technologies. For example, for wireless technologies , it's easy for the attacker to capture signals, gain an access and obtain confidential information to manipulate it [25]. About the security attacks in smart home, they can be categorized into two categories (active and passive attacks).

The passive attacks aim to listen without modifying the data or the performance of the network. In the passive attacks, the attacker obtains information from the system, monitors the system, transmits the messages and does not modify them but he learns something from it. Generally, these types of attacks are undetectable. The active attacks aim to modify the data or the messages, breaking into the network equipment or disrupting the performance of this network. Examples of active attacks include denial of service, message modification, and password cracking. Some of the major threats in the smart home environment are mentioned as follows [26] [27] [28]:

- **Eavesdropping:** It's an attack on confidentiality of the smart home environment. An attacker can monitor the data traffic from the smart home networks without knowing it. So, there is a violation of the confidentiality of the home's users.

- **Masquerading:** the attacker imitates unauthorized access to the smart home internal network system in order to get secret data or acquire service.

- **Replay attack:** An intruder arises between two parties and gets the messages transmitted to get a copy of legitime service that the home user is authorized.

- **Message modification:** the aim of the intruder is to hijack the communication between two legitime parties in order to change values in information.

- **Denial of service (DoS):** the attacker sends a huge number of messages to servers, devices to restrict the internal traffic inside the smart home, to make the network unavailable and reduce the accessibility of network service.

- **Malicious codes:** Malicious it's a software threat, it's applied to alter, demolish or obtain information, this is the most risks in smart home environment due to the lack of unawareness of home user's about data and network security.

4. ENCRYPTION METHODS

Smart Home System elements consists of IoT implementations, Cloud technology implementations, and application to device also home facilities or appliances. Those implementations are in smart home system are using the user data and information through various communication technology that raise security threats to the information and privacy from the home users. To solve those security threat problems, the smart home system must consists security

4.1. Encryption Methods on IoT

IoT application protocols used by most IoT devices nowadays include one of the following data-link and network protocols: 1. Devices that use the IEEE802.15.4 protocol. Such devices are utilized for middle coverage range personal area networks [29, 30]. 2. Devices that use the LoRaWAN MAC protocol for long-range communications, 3. Devices that use the BLE protocol for close proximity data exchanges [31] and 4. Devices that use custom RF open MAC, suitable for low or medium coverage range protocols, implemented on FSK, GFSK, ASK and OOK capable transponders connected to microprocessors (RF12B, RF22, RF69) via I2C, SPI, or UART bus [32, 33, 34].

The IEE802.15.4 standard is the base specification used by many other implementations such as the 6LoWPAN, WirelessHart, Xbee or Zigbee for creating Personal Area Networks. IEEE802.15.4 network security includes a PAN-id field to identify devices in the same network through concentrators responsible for network coordination and addressing. When these networks are functioning in secure mode may use AES-128 algorithm in eight different security levels [36]. In AES-CTR mode only payload encryption, is provided by the encryption of a node concentrator nonce value and a frame counter value with a node placed static key XORed with the frame payload. The AES-CBC-MAC mode is used for data authenticity; in this mode the frame payload is left unencrypted while the payload generated integrity code is encrypted. This mode also requires the installation of a predefined application key to each node. Finally, in AES-CCM mode apart from data authenticity achieved similarly to AES-CBC-MAC, an additional AES key is used to encrypt the frame payload. In IEEE802.15.4, node authentication is provided by the generation of the authentication integrity code token taken from the node source address, the frame counter and the key sequence counter [35,36].

BLE protocol uses four security levels: 1. No security, 2. Unauthenticated pairing with encryption, 3. Legacy mode and 4. Secure connections [31, 37]. BLE 4.x nodes use the up to 6 digit number and a generated nonce in a process called pairing for BLE sensor-node identification (LE Legacy mode) [37], following the public key generation and exchange for the process of data encryption. For BLE devices (gateways) that do not include input interfaces, a more of a static key pairing code build in to each device is used. Furthermore, the paired sensors usually are accepting pairing requests indefinitely. Nevertheless, even if the authentication pairing process is susceptible to man-in-the-middle attacks, eavesdropping and brute force attacks, BLE 4.2 devices provide as an amendment the use of strong authentication instead of pairing. This is achieved by using sensor-node random generated nonce’s verification after a public key exchange process [31].

BLE uses the AES-CCM [31, 38] algorithm to provide data integrity and security upon authentication using two keys for modes 2, 3 and a single 128bit session key (Long Term Key-

LTK, LE secure connections) for mode 4 [37]. In mode 4, the AES session key is exchanged between the node and the sensor end using a sophisticated Diffie-Hellman with elliptic curve cryptography (ECDH) P-256bit [31, 38], making BLE the state of the art representative for IoT data encryption and integrity.

LoRaWAN protocol uses two main modes of authentication and data encryption: 1. ABP (Activating device By Personalization) and 2. OTAA (Over the Air Activation) [39]. For LoRaWAN protocol, authors are focusing on commonly used class A configuration only [40]. LoRaWAN uses AES 128bit for encryption with a 4-byte integrity code for data authenticity verification, for frames send to the LoRaWAN server through the gateways. The protocol encryption and data integrity (Message Integrity Code –MIC) follows the IEEE802.15.4 specification part B (AES-CCM) [40, 42]. More specifically, all LoRaWAN v.1.1 specification [40] devices and servers include a 64bit device id (DevEUI) and a unique per application 64bit AppEUI, used for device authentication to the server. For ABP mode manual network activation is performed using the device address (16bit) a unique network session key (128bit) and a unique application session key (128bit) stored to the LoRaWAN server database and to each node accordingly [40]. The network session key is used to encrypt LoRaWAN frame header commands (options) as well as to calculate the MIC code. The application session key is used to encrypt the payload data [40, 41].

For LoRaWAN OTAA mode, the devices-motes themselves generate and exchange the network session and application session keys during the OTAA join request phase, using an AES-128 commonly shared application key stored both at the LoRaWAN server and motes [40, 41]. The integrity of those key exchange messages is assured with an AES128-CMAC process (MIC generation) that includes devEUI values, a frame counter value and a nonce value [40].

RF12B, RF22 and RF69 devices provide library frameworks for the developers to build their own custom data encryption and integrity implementations [32, 33, 34]. The frameworks include AES-128 encryption and decryption functions for ECB, CBC and CTR modes. These frameworks do not provide a specification mechanism for security but rather the MAC capabilities and AES functions for the developers to create their own custom protocol security implementations. These frameworks lack of support for any kind of non-symmetric algorithm implementation for the process of key exchange or even fair authentication mechanisms. The authentication mechanisms of the provided libraries utilize only network ids for the process of network identification and unique node ids for node distinction.

4.2. Encryption Methods on Cloud

Cloud-based storage be particularly attractive for consumers by providing on-demand capacity, low-cost service, and long-term archive. Furthermore, consumers can access applications and data from the cloud anywhere in the world on demand. However, several recent surveys [43] show that 88% potential cloud consumers worry about the privacy of their data, security is often cited as the top obstacle for cloud adoption. Unfortunately, traditional security mechanisms, such as access control technology, are not suitable for the cloud environment due to the outsourcing-service characteristics of cloud storage and the untrusted or honest but curious assumption of cloud providers.

In order to solve this issue, attribute-based encryption (ABE) [44, 45, 46] has been proposed in the recent years. ABE is a new cryptographic technology, which encrypts a message in terms of access constraints based on fine-grain access control (FGAC) model [47, 48]. By using access policy on attributes describing the out-sourced data, only authorized users can access and decrypt the data. For example, we can use ABE to encrypt a file by a policy (($Faculty = Prof.$) and (($Dep. = CS$) or ($Dep. = EE$))) If a user obtains a private key with an assignment of at-tributes $\{Faculty := P\ rof., Dep. := CS\}$, she/he can de-crypt this file based on the match between access policies embedded into the file and identity attributes described in the user's private key. Although ABE is a powerful tool which meets a variety of application requirements, ABE still has some disadvantages in its practical uses. For example, ABE is a more individual-oriented access control system. The reason is that ABE, as a fine-grained access control method, requires a user's direct intervention to define the access policy for each protected resource. Hence, it is not like traditional access control systems, such as RBAC, which are transparent to all users (e.g., the system does not require user's direct intervention). When an application needs to deal with a large amount of data, the requirement for the user to specify a perfect and sound access policy, will consume large amounts of user's energy. Sometimes, it may be unrealistic when the user's policies are required to keep consistent with constantly changes of the system. These restrictions hinder the applicability and popularity of ABE to secure cloud storage.

Therefore, it is necessary to develop a more user-friendly security mechanism for data security in the cloud. To solve the above issues, we put our attention to role-based access control (RBAC) that has been widely adopted by various information systems over the past few years. Compared with FGAC used in ABE, advantages of RBAC include simplicity, easy-to-use, and automatic running with-out user's intervention. For example, in a Windows-based network system, a role's responsibilities and relationships are specified by the administrator and various access controls are completely transparent to ordinary users. Typically, users do not need to develop access policies for their own resources, but if necessary, they can customize their own policies. Implementation of RBAC model into the ABE scheme could be transplanted into secure cloud storage. The benefit from the combination is that a more user-friendly and easy-to-manage security mechanism can be achieved to protect user's data in the cloud.

One of technical challenges to implement RBAC model is to realize role hierarchy (or called Lattice) used in RBAC into ABE, as well as partial order relation. There has been some cryptographic work [49, 50]to realize the hierarchical key in terms of RBAC, but they cannot be directly used for ABE. In addition, some work in ABE have supported the tree-hierarchy (called hierarchical ABE) [51, 52, 53], but they cannot support full RBAC-type hierarchy which is a lattice with tree, inverted tree, general hierarchies on them. Therefore, it is necessary to develop a new construction for ABE with full RBAC-type hierarchy.

New ABE scheme called Attribute-Based Encryption with Attribute Lattice (ABE-AL). ABE-AL provides an efficient approach to support attribute lattices with arbitrary partial order relations, including the comparison operation ($A \preceq v$or $A \wr v$) for a poset of attribute values $H =(V,\preceq)$on$V = \{v1, \cdots ,vn\}$, a attribute variable A and an attribute value $v \in V$. We also prove that our ABE-AL scheme is se-mantic secure and unforgeable under the eDDH and m-SDH assumptions. Compared with prior schemes, our scheme provides more succinct and richer policy representation for flexible access control.

5. DATA ENCRYPTION IMPLEMENTATION ON SMART HOME SECURITY

Based on Smart Home security issues, data encryption methods are implemented on IoT and Cloud Environment to ensure the data and privacy security for the home users. The data encryption methods implemented on IoT elements for smart home is according to the OSI model for each of IoT layers (Physical and Data Link Layer, Network Layer, Transport Layer, and Application Layer). The encryption through protocols on each layer are mentioned as follows:

- **Physical and Data Link Layers:** protocols used to construct the smart home are WiFi, Bluetooth, ZigBee based on the 802.15.4 standard and LoRaWAN.

- **Network Layer:** Network layer protocols for the IoT and smart home applications use IPv6 functionalities. over Low power Wireless Personal Area Networks (6LoWPAN) and Routing Protocol for Low power and Lossy Networks (RPL).

- **Transport Layer:** Regarding the transport layer which ensures that the data is sent rapidly and efficiently, UDP is preferred as a simple OSI transport layer protocol for client/server network applications based on IP and Datagram Transport Layer Security (DTLS) which provides communications privacy for datagram protocols and a better security in a way to prevent eavesdropping, tampering, or message forgery.

- **Application Layer:** The application layer is responsible for delivering specific application to the user. The most important application layer protocols for IoT and smart home environments are Constrained Application Protocol (CoAP), MQ Transport (MQTT), eXtensible Messaging and Presence Protocol (XMPP) and Message Queuing Protocol (AMQP).

For mostly Smart Home data attacks happened through physical and data link layer in IoT, so the protocol LoRaWAN uses authentications and data encryption to ensure data security. LoRaWAN protocol uses two main modes of authentication and data encryption: 1. ABP (Activating device By Personalization) and 2. OTAA (Over the Air Activation) [39].

As the data encryption is implemented on IoT, the data encryption is also implemented on Cloud Environment in smart home system. Because traditional security mechanisms such as access control technology are not suitable for the cloud environment due to the outsourcing-service characteristics of cloud storage and the untrusted or honest but curious assumption of cloud providers, Attribute-based encryption (ABE) [44, 45, 46] has been proposed in the recent years to ensure data security on Cloud Environment. ABE is a new cryptographic technology, which encrypts a message in terms of access constraints based on fine-grain access control (FGAC) model

[47, 48]. By using access policy on attributes describing the out-sourced data, only authorized users can access and decrypt the data.

Although ABE is a powerful tool which meets a variety of application requirements, ABE still has some disadvantages in its practical uses. For example, ABE is a more individual-oriented access control system. The reason is that ABE, as a fine-grained access control method, requires a user's direct intervention to define the access policy for each protected resource. To solve the issue in smart home system, would be best for smart home system implements new ABE scheme called Attribute-Based Encryption with Attribute Lattice (ABE-AL) which provides an efficient approach to support attribute lattices with arbitrary partial order relations, including the comparison operation ($A \preceq v$or A २ v) for a poset of attribute values H =(V,⪯)on$V = \{v1, \cdots ,vn\}$, a attribute variable A and an attribute value $v \in V$. We also prove that our ABE-AL scheme is se-mantic secure and unforgeable under the eDDH and m-SDH assumptions.

6. CONCLUSION

In conclusion, a home is a place where our private information needs to be respected. Unlike the traditional houses, smart homes can store the user's sensitive and important data and make his life better and comfortable. Even so, the user should apply effective and appropriate security measures to prevent or to secure his data from network attacks. In this paper, the writer understands those security threats in smart home system and identified the security solutions through data encryption with various methods on IoT and Cloud Environment. Additionally, based on data encryption methods effectiveness it can be concluded which data encryption method that would be suited smart home system security needs.

REFERENCES

[1] Global Smart Home Market to Exceed $53.45 Billion by 2022: Zion MarketResearch:.https://globenewswire.com/news-release/2018/01/03/1281338/0/en/Global-Smart-Home-Market-to-Exceed-53-45-Billion-by-2022-Zion-Market-Research.html. Accessed : 2018-6-6.

[2] Yang, H., Lee, H., and Zo, H., 2017. User acceptance ofsmart home services:An extension of the theory of plannedbehavior. Industrial Management & Data Systems, 117(1),68-89.

[3] Li, M., Gu, W., Chen, W., He, Y., Wu, Y., and Zhang, Y.2018. Smart Home: Architecture, Technologies and Systems.Procedia computer science. 131, 393-400. DOI=https://doi.org/10.1016/j.procs.2018.04.219.

[4] Hui, T.K., Sherratt, R.S., and Sánchez, D.D. 2017. Majorrequirements for building Smart Homes in Smart Citiesbased on Internet of Things technologies. Future GenerationComputer Systems. 76, 358-369. DOI=https://doi.org/10.1016/j.future.2016.10.026

[5] Wu, C.L., Tseng, Y.S., and Fu, L.C. 2013. Spatio-temporalfeature enhanced semi-supervised adaptation for activity recognition in IoT-based context-aware smart homes. InGreen Computing and Communications (GreenCom), 2013IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical andSocial Computing .460-467.

[6] Babakura, A., Sulaiman, M.N., Mustapha, N., and Perumal,T., 2014. “Home-based decision model for smart homeenvironment”.International Journal of Smart Home, 8(1),pp.129-138.

[7] Gram-Hanssen, K. and Darby, S.J. 2018. “Home is where thesmart is”? Evaluating smart home research and approachesagainst the concept of home. Energy Research & SocialScience, 37, 94-101.

[8] Wang, M., Zhang, G., Zhang, C., Zhang, J. ,and Li, C. 2013.June. An IoT-based appliance control system for smarthomes. In Intelligent Control and Information Processing(ICICIP), 2013 Fourth International Conference on. pp. 744-747. IEEE

[9] Vani, K.S. and Shrinidhi, P.C., 2015. “Automatic TapControl System in the Smart Home using Android andArduino,” International Journal of Computer Applications,127,8.

[10] Bouchard, K. and Giroux, S. 2015. Smart homes and thechallenges of data. In Proceedings of the 8th ACMInternational Conference on PErvasive Technologies Relatedto Assistive Environments. 66.

[11] Yang, C, Mistretta, E, Chaychian, S., and Siau, J. 2016.Smart Home System Network Architecture,Paper presentedat 1st EAI International Conference on Smart Grid InspiredFuture Technologies, Liverpool, United Kingdom.

[12] Brush, A.J., Lee, B., Mahajan, R., Agarwal, S., Saroiu, S.,and Dixon, C. 2011. May. Home automation in the wild: challenges and opportunities. In proceedings of the SIGCHI Conference on Human Factors in Computing Systems ,2115-2124. ACM.

[13] Wilson, C., Hargreaves, T., and Hauxwell-Baldwin, R. 2015.Smart homes and their users: a systematic analysis and key challenges. Personal and Ubiquitous Computing. 19, 2, 463-476.

[14] Feng, S., Setoodeh, P. and Haykin, S., 2017. Smart home: Cognitive interactive people-centric Internet of Things. IEEECommunications Magazine. 55,2, 34-39.

[15] L. Satpathy, “SMART HOUSING: TECHNOLOGY TO AID AGING IN PLACE - NEW OPPORTUNITIES AND CHALLENGES,” p. 192.

[16] M. R. Palattella et al., “Standardized Protocol Stack for the Internet of (Important) Things,” IEEE Communications Surveys & Tutorials, vol. 15, no. 3, pp. 1389–1406, 2013.

[17] Mosweu, Tshepho & Luthuli, Lungile & Mosweu, Olefhile. (2019). South African Journal of Information Management. 10.4102/sajim.

[18] A. Gaddam, K. Kaur, G. Sen Gupta, and S. C. Mukhopadhyay, “Determination of sleep quality of inhabitant in a smart home using an intelligent bed sensing system,” 2010, pp. 1613–1617.

[19] A.-D. Floarea and V. Sgarciu, “Smart refrigerator: A next generation refrigerator connected to the IoT,” 2016, pp. 1–6.

[20] S. Gao, Y. Qian, F. Cao, and L. Wang, “The design of smart window control system based on GSM network,” 2011, pp. 1297–1299.

[21] M. Ye, N. Jiang, H. Yang, and Q. Yan, “Security analysis of Internet-of-Things: A case study of august smart lock,” 2017, pp. 499–504.

[22] A. Prasetio, S. R. Akbar, and B. Priyambadha,
“Implementation of semantic system in the smart home lights device based on agent,” 2017, pp. 93–99.

[23] I. Alam, S. Khusro, and M. Naeem, “A review of smart TV: Past, present, and future,” 2017, pp. 35–41.

[24] A. Lazakidou, K. Siassiakos, et K. Ioannou, Éd., Wireless Technologies for Ambient Assisted Living and Healthcare: Systems and Applications. IGI Global, 2011.

[25] N. Markus H., Sebastian S., Secure and QoS-aware Communications for Smart Home Services. New York: Wiley, 2012.

[26] G. W. Kim, D. G. Lee, J. W. Han, et S. W. Kim, « Security technologies based on home gateway for making smart home secure », in International Conference on Embedded and Ubiquitous Computing, 2007, p. 124–135.

[27] M. Haque et S. I. Ahamed, « Security in pervasive computing: Current status and open issues », Int. J. Netw. Secur., 2006.

[28] S. Ul Rehman et S. Manickam, « A Study of Smart Home Environment and its Security Threats », Int. J. Reliab. Qual. Saf. Eng., vol. 23, no 3, p. 1640005, juin 2016.

[29] R. Doomun, J. Doma and S. Tengur (2012). AES-CBC Software execution optimization, https://arxiv.org/pdf/1208.3227.pdf.

[30] ZigBee Alliance (2012). ZigBee Specification, ZigBee Document 053474r20, https://www.zigbee.org/download/standards-zigbee-specification.

[31] C. Gomez, J. Oller, and J. Paradells (2012). Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology, Sensors 12(9), 11734-11753.

[32] HopeRF (2016). RFM69 LowPowerLabs library and protocol stack, https://github.com/LowPowerLab/RFM69.

[33] [Jeelabs (2009). RF12B library and improved library, http://jeelabs.org/2009/02/10/rfm12b-library-for-arduino/index.html, https://hallard.me/rfm12b_arssi-library/.

[34] RadioHead (2016). RadioHead Packet Radio library for embedded micro processors with RF transponders, https://www.airspayce.com/mikem/arduino/RadioHead/index.html.

[35] X. Fan, F. Susan, W. Long, and S. Li (2017). Security Analysis of ZigBee, https://courses.csail.mit.edu/6.857/2017/project/17.pdf, Tech. report.

[36] G. Sharma, Nitin Pandey, Iqra Hussain, Sunil Kumar Kathri (2017). Design of framework and analysis of Internet of things at data link layer, 2nd International Conference on Telecommunication and Networks, 1-4.

[37] Bluetooth Core Specification (2016). Bluetooth SIG, ver. 5, https://www.bluetooth.com/specifications/bluetooth-core-specification.

[38] Nordic semiconductors (2011). Bluetooth Low Energy wireless technology backgrounder, https://www.nordicsemi.com/eng/content/download/3045/40678/version/1/file/Bluetooth_le_technology_backgrounder_4.pdf.

[39] I. Gutierrez and H. Calderon (2017). Evaluation of cryptographic algorithms over an All programmable SoC (AP SoC) Device, iisci.org Systemics, Cybernetics and Informatics Journal, 15(2), ISSN 1690-4524.

[40] Lora Alliance Inc. (2017). LoRaWAN v.1.1 Specification, http://net868.ru/assets/pdf/LoRaWAN-v1.1.pdf.

[41] I. Butun, Ismail, N. Pereira, and M. Gidlund (2018). Analysis of LoRaWAN V1.1 Security: Research Paper, In Proc. of the 4th ACM MobiHoc Workshop on Experiences with the Design and Implementation of Smart Objects, ACM, DOI://10.1145/3213299.3213304.

[42] IEEE standards association (2007). IEEE 802.15.4 standard - amendment https://standards.ieee.org/standard/802_15_4a-2007.html, approved 2003, amend 2007.

[43] F. R. Institute. Personal data in the cloud: A globalsurvey of consumer attitudes. Available online: http://www.fujitsu.com/downloads/SOL/fai/reports/fujitsu/personal-data-in-the-cloud.pdf, 2010.

[44] Vipul Goyal, Omkant Pandey, Amit Sahai, and BrentWaters. Attribute-based encryption for fine-grainedaccess control of encrypted data. In ACM Conferenceon CCS, pages 89–98, 2006.

[45] Rafail Ostrovsky, Amit Sahai, and Brent Waters.Attribute-based encryption with non-monotonic accessstructures. In ACM Conference on Computer andCommunications Security, pages 195–203, 2007.

[46] Shucheng Yu, Cong Wang, Kui Ren, and WenjingLou. Achieving secure, scalable, and fine-grained dataaccess control in cloud computing. In INFOCOM,pages 534–542. IEEE, 2010.

[47] Lingyu Wang, Duminda Wijesekera, and SushilJajodia. A logic-based framework for attribute basedaccess control. In FMSE, pages 45–55, 2004.

[48] Rakeshbabu Bobba, Omid Fatemieh, Fariba Khan,Arindam Khan, Carl A. Gunter, Himanshu Khurana,and Manoj Prabhakaran. Attribute-based messaging:Access control and confidentiality. ACM Trans. Inf. Syst. Secur., 13(4):31, 2010.

[49] Mikhail J. Atallah, Marina Blanton, Nelly Fazio, andKeith B. Frikken. Dynamic and efficient keymanagement for access hierarchies. ACM Trans. Inf. Syst. Secur., 12(3), 2009.

[50] Sabrina De Capitani di Vimercati, Sara Foresti, SushilJajodia, Stefano Paraboschi, and Pierangela Samarati.Over-encryption: Management of access controlevolution on outsourced data. In Christoph Koch,Johannes Gehrke, Minos N. Garofalakis, DiveshSrivastava, Karl Aberer, Anand Deshpande, DanielaFlorescu, Chee Yong Chan, Venkatesh Ganti,Carl-Christian Kanne, Wolfgang Klas, and Erich J.Neuhold, editors, VLDB, pages 123–134. ACM, 2007.

[51] Rakeshbabu Bobba, Himanshu Khurana, and ManojPrabhakaran. Attribute-sets: A practically motivatedenhancement to attribute-based encryption. InMichael Backes and Peng Ning, editors, ESORICS,volume 5789 of Lecture Notes in Computer Science,pages 587–604. Springer, 2009.

[52] Guojun Wang, Qin Liu, and Jie Wu. Hierarchicalattribute-based encryption for fine-grained accesscontrol in cloud storage services. In Ehab Al-Shaer,Angelos D. Keromytis, and Vitaly Shmatikov, editors,ACM Conference on Computer and CommunicationsSecurity, pages 735–737. ACM, 2010.

[53] Jin Li, Qian Wang, Cong Wang, and Kui Ren.Enhancing attribute-based encryption with attributehierarchy. MONET, 16(5):553–561, 2011.