International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 08 | Aug 2021 www.irjet.net p-ISSN: 2395-0072

IoT Smart Home Using Li-Fi: Security Challenges and Solutions

Shubham Yadav[1], Gilna Meethal[2]

[1,2]U.G. Student, Department of Information Technology, B. K. Birla College of Arts, Science and Commerce (Autonomous), Kalyan, Maharashtra, India

---

Abstract - *Internet of Things (IoT) is going to make a particular world where physical things (smart home appliances, and smartwatches, etc.), information networks and, services providing systems, which provides innovative and smart services to humans. In a Smart home, security is a major concern when storing sensitive data to maintain the privacy of the data. A hacker can easily throw an attack on the smart home Router. There are several attacks like DDoS, Botnet, phishing in order to get access to smart homes and to gather sensitive data. In this paper, we secure smart homes from various security attacks, threats, with the help of Li-Fi and various encryption algorithms. Additionally, why we considered Li-Fi instead of Wi-Fi for better security. In this paper, we also discussed proper solutions for IoT devices. Eventually, we predicted the rise of cyber-attacks in the next few upcoming years. Therefore, the main objective of this work is to make our smart home system more secure.*

***Key Words*: IoT, Li-Fi, Encryption, Attacks, VPN**

1.INTRODUCTION

IoT is a concept of interconnecting the things or objects which are outfitted with sensors like vehicles, machines, home appliances, etc, and uses APIs to connect and exchange data through the internet. The industry utilizes a variety of IoT called IIoT, to automate its manual things like industrial operation, security inside or outside the industry sensitive area, automation of notification by the many industrial devices, etc. In the current scenario, approximately 71% of the total use of IoT is used by the industry, and the rest 29% of total use is under consumer IoT [1].

The Internet of Things (IoT) will make such a world home environment that provides innovative features, security, and smart service to humans. Although the smart home is more convenient and controls all home appliances, the smart home's, inter-connected, dynamic, and heterogeneous nature are the challenges in security issues. Considering the challenges on security issues in IoT we will focus on the encryption algorithm, Li-Fi technology, and various attacks in home automation security. As an example, in the below diagram Fig. 1: shows the architecture of the smart home scenario, consisting of many connected devices belonging to different applications, communicating among each other using Li-Fi technologies, and connected to a few gateways/routers which provide connectivity to outside networks. The gateway is the place where everything is associated with the cloud and users can access it.

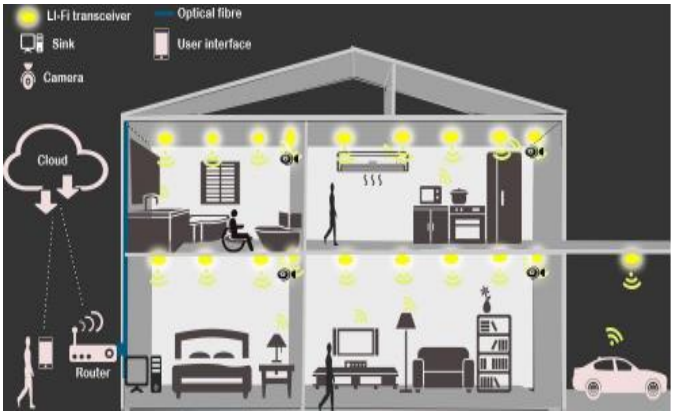

Fig -1: Li-FI Smart Home [2]

In this paper, we propose a home framework that utilizes Li-Fi innovation as the mode of condemnation between every one of the associated devices and utilizes a video surveillance framework dependent on Wireless Visual Sensor Organization. Li-Fi uses a visible light spectrum for the transmission of data [2].

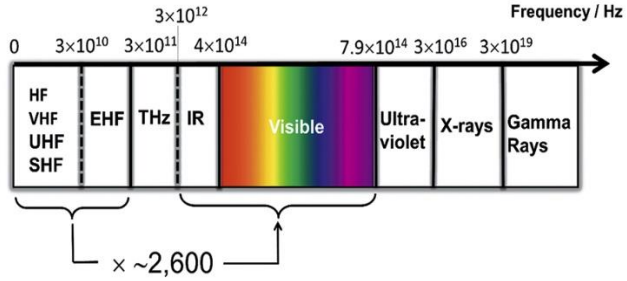

Fig -2: visible light spectrum
Source: led-professional.com

2. LI-FI

Li-fi stands for Light Fidelity. It is a high-speed bi-directional wireless technology that utilizes a visible light spectrum for the transmission of data [3]. Nowadays, many smart homes are using wi-fi (Wireless Fidelity) which uses radio waves for communication between the IoT devices. Li-fi provides more than 10,000 frequencies and thus it provides immunity to interference or noise in the network [2].
Li-Fi uses a LED that is outfitted with a chip and sends data using light and the hardware(photoreceptor) that is present on the receiving end of the IoT device senses the blinking of led (cannot be tracked by the human eye) and converts that blinking into binary data. Thus, obtaining the original

message and according to that, the machine performs necessary actions. Li-Fi is very cheap and at the same time, it also provides light to the house.
Li-Fi can be used underwater because visible light can travel a long distance in that medium for the transmission of data [2].

Fig -3: Li-FI Vs Wi-Fi

As mentioned in Fig-3, The speed of Li-Fi is much better than the traditional wi-fi. Li-Fi can achieve speed up to 224 Gbps [2]. As far as security is concerned, the light signals transmitted from the LED stay within the boundaries of the four walls of the IoT home. Thus, attackers cannot break this system easily whereas in the case of wi-fi the radio waves penetrate through the wall and attackers can easily attack this network and can take access to the IoT home devices.

Alongside the different benefits of Li-Fi, there are a few difficulties in this Li-fi technology. As light cannot penetrate through the walls it gives a short range of network. But we can overcome this problem by using a greater number of LEDs in the smart home.

3. ENCRYPTION

However, our data is secured in the smart home by using Li-Fi, but the data between the user and the cloud is still unsecured. We need to encrypt data to maintain confidentiality.
Encryption is the process of encoding the original representation of information in the form of plain text to ciphertext. The name comes from whether a similar key is utilized for encryption and decryption. There are two types of encryptions in far and wide use today: symmetric and asymmetric encryption.

Symmetric Key Encryption: Depends on public and private key encryption methods. It is utilizing the same key for encryption and decryption of the message [4].

Asymmetric Key Encryption: It utilizes one public key and another is the private key. In general, a public key is utilized for encryption while private key is just utilized for decoding measures that are available only to the particular person it is also called secret-key [4].

Types of Algorithms:

I. AES

The Advanced Encryption Standard (AES), furthermore known by its special name Rijndael. The key length decides a few boundaries of the AES calculation.

The algorithm has been categorized into:
- Data Security or protection against well-defined attacks.
- Code speed and minimization on different stages.

There are 3 different key lengths (128, 192, 256 bits). 10 rounds for 128-bit keys,12 for 192-bit keys, and 14 rounds for 256-bit key length for encryption and decryption. A round comprises several processing steps, in which a simple text input is replaced, mixed, and transformed into the final output of encoded text. AES is very fast and secure as compared to the other three attacks explained here and is the de facto world standard. Rounds in AES are byte substitution, shift row, mix column, and key addition. AES is fast and takes the least time to encrypt [11].

II. DES

DES stands for data encryption standard. It is a 64-bit symmetric block encryption algorithm. DES involves 16 rounds of identical operations. This does not affect the security of the algorithm. The DES algorithm is used for encryption and decryption. Only half of the original 64-bit block is used in one run. The rounds alternate between the two halves. Rounds in DES are substitution, Expansion, XOR operation, and permutation. Blowfish takes more of the memory while DES takes the least of the memory. DES utilizes minimum CPU usage [11].

III. Blowfish

In 1993, the first symmetric encryption algorithm developed by Bruce Schneier was blowfish [11]. Blowfish uses a block size of 64, and the length of the generated key is between 32 to 448 bits. Blowfish is faster than DES but it takes higher CPU usage as compared to others. It has a lesser number of operations to perform as compared to another encryption algorithm. The key schedule of this algorithm takes an enormous amount of time, but this can be advantageous as brute-force attacks are becoming a difficult task [11].

4. ATTACKS

In this section, we will see how attackers perform various attacks and get access to our IoT devices. The attack is information security that implies an endeavour to acquire,

change, destroy, eliminate, or reveal data without authorized access or permission by the user.

We group the security attacks into two specified categories:

Passive attack: An attacker is attempting to get the user system's information without affecting their system resources. User mail, user/worker message or document moves are the activities of transmission which can be checked by an attacker. But these kinds of attacks are difficult to detect because it doesn't modify the information, but only extracts the data [5].

Active attack: In active attack, adversaries use information gathered during the passive attack and use it in an attempt to change system resources or modify the system operations and adversaries try to gain unauthorized access to the system [5].

TYPES OF ATTACKS:

A. **DoS and DDoS:** In DoS (Denial of Service), an attacker sends a massive number of unwanted requests to the targeted server. The server cannot handle such a large request at the same time and that leads to disrupting services of genuine server. When the attacker does the same thing but with the help of multiple sources by sending unwanted requests to the server is known as DDoS (Distributed Denial of Service) [6] [7].

B. **Phishing attack:** In a phishing attack, the attacker puts his minimal effort. It is a type of social engineering attack where an attacker makes a false website or login page to get the user's login Id and password [8].

C. **Sleep deprivation attack:** Most of the sensors work on the batteries associations that work as per rest and work routine, to augment battery life. Sleep deprivation attack makes the sensor work constantly which prompts burning the energy rapidly that outcomes in closing down the device [6].

D. **Man-In-The-Middle attack:** When an attacker or perpetrator position himself in the middle of the conversation between a user and an application is called as MITM(Man-In-The-Middle) attack. The attacker can extract and manipulate the data between the user and the application [8] [6].

E. **Sinkhole attack:** It is similar to the Man-In-The-Middle attack but here the attacker discards all the packets between the communication instead of forwarding them to the desired location [8].

F. **Cryptanalysis attack:** Suppose the attacker already has ciphertext. Then the attacker tries to get the encryption key by breaking the system encryption structure is known as a Cryptanalysis attack [8].

G. **Cloud Malware Injection:** In the cloud, an attacker can inject malicious codes or can inject a virtual machine and the attacker can pretend to be a valid service by creating multiple instances of the virtual machines. So, in this way, the attacker can collect the sensitive data of the users that are present on the cloud [6].

H. **Botnet attack:** It is a collection of internet-connected devices that contains some malware which was installed by attackers in the different systems and they can access the system from anywhere and can use it as a bot and the network of bot termed as botnet. These botnets can be used for a DDoS attack. Mirai attack is one of the best examples among them. In 2016, the Mirai attack infected more than 2 million devices [9].

I. **Ransomware:** It is one type of malware that locks the information or encrypts the victim's data in another format which makes it unusable until the victim makes a ransom payment which is usually done in the form of cryptocurrencies to the attacker[10]. In section 6, we discussed the loss in businesses due to ransomware

5. SECURITY OBJECTIVES

A. **Confidentiality:** Confidentiality guarantees the security of users. In Confidentiality, the user's data is encrypted and kept secure, and it can be accessed only by authorized users [9].

B. **Integrity:** Integrity is used to ensure that the content of messages between the communication is protected against any manipulation by an attacker without the victim being able to track this manipulation. In the IoT system by the use of Integrity checks each node carries out the message exchange so the attacker can't track the receiver [8].

C. **Availability:** It guarantees that the services haven't interfered over a wireless network from an attack like DoS and DDoS attack. To get availability, it is essential to restrict various activities from the fundamental capacities and to give only functional access [9].

D. Authentication: However, the user's data and resources of the IoT system need to be secured. Authentication is the proper identification where only the authorized user can access it [8].

6. SECURITY SOLUTIONS FOR SMART HOME

1) **Firmware Updates:** Always try to keep your IoT devices up-to-date. There are various serious threats available on the internet that can affect your IoT device [8].

2) **Strong Authentication:** Many users are still using the default user Id and password of the device that was provided by the manufacturer which is very weak and easy to crack. Use more complicated passwords and use two-step authentication [8].

3) **Encryption:** Our data is very precious to the attackers so it becomes very important to encrypt our data with some advanced method of encryptions like AES, WPA2, etc [1].

4) **VPN (Virtual Private Network):** Always try to avoid connecting any IoT device to the public network unless it becomes important, in that scenario use VPN connections that open a private tunnel for your connection and keeps your device and data safe [6].

5) **Fog layer:** The number of IoT devices is increasing on a large scale which generates a huge amount of data and this data is termed big data. Cloud cannot handle such enormous data at a time and hence, the concept of fog layer came into existence. The fog layer is an extension of the cloud which helps in local data analytics, it gives security alerts and sends only selective data to the cloud [1].

7. FORECASTING ABOUT CYBER ATTACKS

In this section, we will predict the number of cyberattacks in the next upcoming years. In a cyber-crime report, it is stated that 1.1 million web attacks are carried out in a single day. In 2020, Ransomware attacks cost businesses around $20 billion, which is 50 times since 2015. Between 2005 and 2020, there have been around 11,762 data breaches recorded. According to IBM as of 2020, the average cost of a data breach cost around $3.86 million.
We can anticipate how many cyber-attacks will occur in the following years based on these figures.

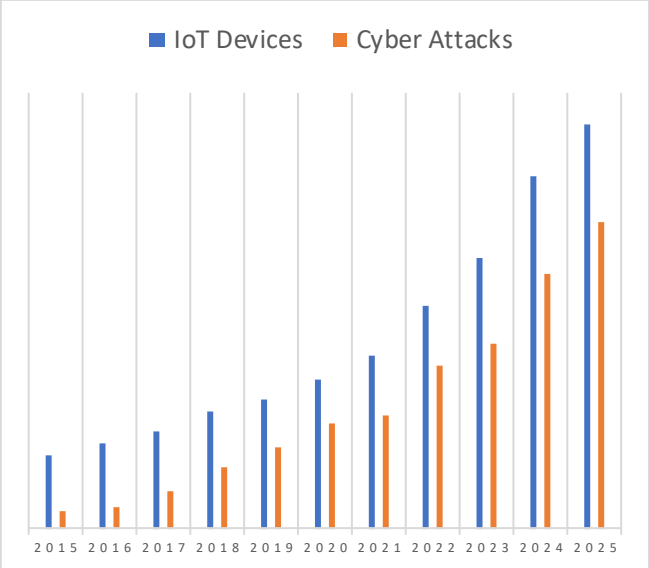

Fig -4: cyber-attacks against IoT

The fig-4 shows that the number of IoT devices is increasing rapidly every year. Since the IoT devices are rising, the cyber-attacks on IoT will also increase [5].
According to our estimations, cybercrime will cost businesses worldwide $10.5 trillion annually by 2025, as you can see in fig-5.

Fig -5: Business Loss Graph

8. CONCLUSION

IoT is a huge field and developing day by day improving the existence of humankind. In this paper, the smart home operates with the help of Li-Fi technology which uses LED for the transmission of data which rates better than that of the traditional Wi-Fi system while being secure and with no harm to the people. We highlighted some encryption algorithms and various crucial attacks performed by the attackers on the IoT devices. Additionally, we pointed out some issues and challenges related to security in IoT smart homes. In the last section, we predicted the number of cyber-attacks that will arise in the next few upcoming years.

ACKNOWLEDGEMENT

We would like to acknowledge the support and guidance of Prof. Swapna Augustine Nikale, Department of Information Technology, B. K. Birla College (Autonomous), Kalyan.

REFERENCES

[1] A. K. Ray and A. Bagwari, "IoT based Smart home: Security Aspects and security architecture," in 2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT), Gwalior, India, Apr. 2020, pp. 218–222. Doi: 10.1109/CSNT48778.2020.9115737.

[2] V. Shrivastava, K. Fernandes, G. Mathias, and S. Pereira, "Advanced Home Automation using Light Fidelity," p. 4.

[3] M. Afaf and R. Said, "SMART HOME BASED ON LI-FI TECHNOLOGY," p. 4.

[4] V. R. Kadam and P. S. Naidu, "Lightweight Cryptography to Secure Internet of Things(IoT)," vol. 07, no. 05, p. 5, 2020.

[5] W. Ali, G. Dustgeer, M. Awais, and M. A. Shah, "IoT based Smart Home: Huddersfield, UK, 7-8 September 2017 Security Challenges, Security Requirements and Solutions," p. 6.

[6] D. K. Alferidah and N. Jhanjhi, "A Review on Security and Privacy Issues and Challenges in Internet of Things," p. 23, 2020.

[7] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," IEEE Access, vol. 7, pp. 82721–82743, 2019, Doi: 10.1109/ACCESS.2019.2924045.

[8] H. F. Atlam and G. B. Wills, "IoT Security, Privacy, Safety and Ethics," in Digital Twin Technologies and Smart Cities, M. Farsi, A. Daneshkhah, A. Hosseinian-Far, and H. Jahankhani, Eds. Cham: Springer International Publishing, 2020, pp. 123–149. Doi: 10.1007/978-3-030-18732-3_8.

[9] Z. Shouran, A. Ashari, and T. Kuntoro, "Internet of Things (IoT) of Smart Home: Privacy and Security," IJCA, vol. 182, no. 39, pp. 3–8, Feb. 2019, DOI: 10.5120/ijca2019918450.

[10] M. Humayun, N. Jhanjhi, A. Alsayat, and V. Ponnusamy, "Internet of things and ransomware: Evolution, mitigation and prevention," Egyptian Informatics Journal, vol. 22, no. 1, pp. 105–117, Mar. 2021, DOI: 10.1016/j.eij.2020.05.003.

[11] Goyal, V., & Zafar, A. (2020a). A Cryptographic Approach for Securing IoT Devices. ., 7(DEC), 1222–1226. https://www.irjet.net/archives/V7/i12/IRJET-V7I12219.pdf