Fortifying Smart Living: An In-Depth Review of Robust IoT Security Solutions for Connected Homes

Prof.Sir.Bashiru Aremu **Mohd Abdul Nayeem**

Professor & Vice Chancellor, Crown University Int'l Chartered inc.(CUICI) USA

Research Schalor, Department of Computer Science & Engineering, CUICI, USA

Abstract

Recently, the term "smart house" has gained popularity. Modern technologies and technical advancements have led to the creation of the smart house. All objects are connected to the Internet through Internet of things (IoT) technology. Smart gadgets across a range of industries, including industrial monitoring, public security, government work, intelligent fire control, smart homes, intelligent transportation, and environmental protection. An array of Internet of Things (IoT) gadgets that are networked and can be managed from a computer or smartphone constitutes a "smart house." IoT devices have become more and more common in recent years, along with increased development in all spheres of life and the emergence of new security threats. The security and privacy of the people residing in smart homes are the main topics of this study, which surveys a number of earlier studies, including Examine the security and hazards that smart homes face, as well as any weaknesses that may be used to access authorised data or deny service. You should also analyse some of the Internet of Things device systems that were used to help manage and secure these smart homes.

Keywords: *IOT, Smart Home. Advance engineering*

Introduction

The Internet of Things (IoT) connects everything to the network. IoT is used in many different fields, including smart homes, government work, environmental protection, intelligent transportation, industrial monitoring, senior care, and personal health [1]. As the economy grows, smart housing based on IoT security is being developed in smart houses and districts. Given the services they already have, we can argue that these smart homes can operate as cities in the modern period. However, ongoing management and monitoring are still required. The number of Internet users worldwide is expected to increase from 3.9 billion (51% of the population) in 2018 to 5.3 billion cumulative users (66% of the population) by 2023 due to the ongoing expansion of Internet networks and Cisco's annual Internet survey. As a result, given their widespread use, smart devices that interface with the Internet of things need to be appropriately regulated and safeguarded [2]. Additionally, unlike individuals, smart houses are unaffected by environmental hazard concerns. The benefit of having smart devices in the home is that they can handle situations where people might become fearful or panicked and lose control. For example, in the event of a house fire, the owner can use their phone to arm the home security system and turn on or off devices. However, there are also drawbacks to having smart homes, chief among which being the high ongoing costs associated with maintaining and controlling these systems, which are also thought to be challenging to secure. Since the IoT framework is still relatively new, IoT security is an issue of concern for protecting smart devices. Since limited space and weak capabilities are among the vulnerabilities that hackers exploit in penetrations, smart homes require a system that integrates as many devices as possible. Therefore, devices must be carefully chosen and purchased from reputable companies [3]. It is advisable to employ a suitable system that satisfies the security criteria (access control, authentication, secrecy, safety, and non-repudiation) [4].

Aspiration

- Examines the hazards and security that smart homes confront, finding weak points that might be used to bypass security measures or deny service.
- Examination of some IoT device solutions that aided in the upkeep and security of these smart homes.
- Evaluation of security and feature comparison for smart home systems. To be more precise, the privacy of the residents of the smart home and the security of the home are our main concerns in this study. Hackers can take advantage of a range of vulnerabilities present in different household devices that are connected to the Internet. The physical and electronic actions of linked home appliances, as well as assisted living devices, can be used to track homeowners' movements in the case of a security breach. This is how the remainder of the paper is organised: Section 2 provides a history of smart homes; Section 3 shows the security status of the system; Section 4 reviews the system; Section 5 compares the security of the system under evaluation with the preceding section; and Section 6 concludes.

2. History of smart houses

The first hoover cleaner was created in 1901 along with other appliances. The hoover cleaner itself was established in 1907. A few years later, electric dryers, freezers, irons, and other appliances were created in 1966–1967. The ECHO IV was the first appliance control device to regulate both the temperature of the home and the on/off of equipment [5]. technologies for controlling lighting and security were invented in the 1970s [6]. The majority of people in England had colour television in the 1980s, and half of them owned video recorders by 1990 [7]. 1991 - Using ageing technology to assist senior citizens [5]. Along with cordless home phones, DVD players, PlayStations, and multimedia PCs, rotary dryers saw an increase in popularity in 1994.1998: Offers new ICTs including video phones and web television, as well as communication networks like ISDN and the Internet [7]. The emergence of various technologies at reasonable prices in 2000 also contributed to the growing popularity of the smart home [5]. Provide smart home users with a remote control in 2002 [8]. Initial wearable smart health system released in 2005 [9]. As part of the smart home system, the cloud was utilised in 2009 [10]. A voice controller for smart homes was employed in 2015 [11].

3. Safety in smart houses

Smart IoT devices transmit data from sensors over a wired or wireless transmission network in smart homes, as seen in figure 1. The system needs to be able to handle data from a lot of sensors without losing any of it because of network congestion, make sure that it is transferred with the right security procedures, and shield it from outside influence or surveillance. When some consumers purchase Internet of Things (IoT) gadgets for their homes, they frequently consider the device's use and performance above any potential security risks. Unfortunately, most smart home equipment and Internet-connected gadgets lack adequate security computing capability as well as a standardised implementation environment. As a result, comprehensive security plan implementation is challenging [12]. In the actual world, there is very little chance that someone will enter a house with an open door; yet, in networks, there are many individuals who are always monitoring every entrance. The security of the Internet of Things (IoT) devices, user control system, network layer, and cloud of things is covered in this section.

3.1 Internet of Things devices

Two sets of Internet of Things devices make up a smart house. Devices that require two-way communication are in the first group. One-way connection home equipment such a smart TV, lighting system, and charger make up the second group. The first category includes solar panels, which need two-way communication in order to supply the utility company with non-essential electricity. In order to lower power density, the utility provider is expected to send a signal to the alternating current. On the other hand, the second group can transmit the data on electricity consumption with just one connection. In comparison to devices in the first category, those in the second group are capable of more resources [13].

3.1.1. Thread and security of IoT devices

Its owners could encounter numerous obstacles, hazards, and difficulties. One of the researchers noted that concerns about the security and privacy of the devices being utilised were among the most significant of these issues [14]. In order to handle the security and privacy threats presented by the Internet of Things, the majority of users of IoT devices are unaware of the IoT security architecture that is required. Due to the simplicity of data transfer between these numerous smart devices, Internet of Things devices are among the primary targets that some electronic attacks aim to obtain some personal information of users. Weak passwords and insufficient security safeguards make many IoT devices easily targeted or compromised. Approximately 70% of the most widely used IOT devices have been incorporated, and the majority of IOT devices gather personally identifiable information in one piece [15]. A DDOS assault, for instance, caused the majority of the automated systems, such as thermostats, to shut down in two buildings in Lappeenranta, Finland, in November 2016.

Distribution, ventilation, and hot water have all been tried, and as a result of these attacks that rob people of their comfort, put them in danger, and ruin infrastructure, the heating equipment have been out of commission for more than a week [16].

A few of the most important legal issues that should not be disregarded are data security, privacy, and management access. Since the gadgets hold sensitive information about the user, there are numerous legal concerns with data privacy and preservation. Thus, in order to keep data from ending up in the wrong hands, permissions for access, display, and security must be established for all types of data audio, video, and other and devices [17].

As a result of the following factors, these devices will rank among the most crucial targets for hackers: they have some of the primary means by which hackers can gain access to them and insert their destructive programmes into them. These factors include, but are not limited to:

A. Smart devices, like cellphones in general, are easy to disseminate and acquire everywhere.
B. The majority of smart gadgets in use today operate on open platforms, making it simple for hackers to take advantage of their flaws.
C. Total ignorance of the risks and dangers connected to these devices.

3.2. Control device for users

The use of a smart home-smartphone system involves more than just regulating; it also involves data exchange and meeting user needs. Although the user's life is made easier by this kind of system, security issues are also raised [18].

A. Device malfunction related to power and internet: Device malfunction related to power or internet access can result in the owner's device losing connection with the home device.
B. Software failure: The smart home-smartphone system is the target of the attacker due to a software implementation weakness.
C. Disclosure of Confidential Data: When a computer is unreliable or does not use data encryption, information can be lost or disclosed over the network.
D. Denial of service (DoS): Users will not be able to use their smart home system when a DoS attack takes place.
E. Eavesdropping attack: With this technique, hackers can obtain a login and password from a user when they validate their access to a smart device application.

3.3. Layers of networks

There are two main ways that a Home Area Network (HAN) can talk to Internet of Things (IoT) devices. Using smart metres as a conduit to network operations centres and other stakeholders is one method. Using a different control and aggregation node to directly communicate with WAN and NAN is another method [19]. The smart metre (SM), which is a component of the infrastructure of the communication network between devices on the HAN, is connected to the AMI smart network, to which all communications in the smart house are made [19]. We give a quick overview of the various wireless network threats in this section.

A. RFID attacks: RFID technology allows devices to be uniquely identified, controlled, and distinguished from one another in smart settings. However, RFID has a few security flaws [20]:

- Attacks on RFID Tags: Cloning and spoofing attacks pose a serious risk to the information contained in RFID tags. Making a close replica of the RFID tags is the aim of this attack.
- RFID reader assaults are classified as eavesdropping attacks. intercept information from the RFID reader and obtain private tag data.

B. Attacks on Wireless Sensor Networks A network is a wireless link made up of distinct nodes with sensors and a bandwidth constraint.The primary communication between the base station and sensor is done through these networks. Attacks by [20] are possible.

- False routing attack: the attacker delivers erroneous route information that disrupts normal connection.
- Unfairness Attacks: these attacks involve a malicious node that generates a noise signal to cause data transmission collisions between nodes and deplete the resources.

C. The Wi-Fi Business Alliance developed WPA (WiFi protocol access), a security technology for wireless local area networks (LANs), based on IEEE 802.11i. The two most crucial security factors in WiFi are encryption and access control. The original WiFi authentication technique, which has been shown to be dangerous, is used by the WEP [21].

D. Bluetooth is a low transmission power and low range set of protocols and operations wrapped in a stack. The majority of Bluetooth attacks stem from users failing to modify their devices' default settings. A few Bluetooth attacks [22]:

- Denial of Service Attack: Bluetooth can only process a certain quantity of data concurrently. An attacker can send a lot of pairing request packets in order to take advantage of this vulnerability. that stops an authorised user from pairing, draining the device's power, or potentially damaging the device.
- Replay Attack: the attacker adds the desired data to a capture file and uses a single line of code to deliver the reply attack [23].

3.4. Smart homes with the Cloud of Things (CoT)

The broker and database are located in the cloud area. Every home device is connected to the broker, and data gathered from those devices is stored in the database. The three primary components of the cloud are the MongoDB database, the MQTT broker Mosquito, and Node.js for backend processing [24].

As stated in section 3.1, a smart home is made up of two groups of devices: each group has controllers connected to the Cloud of Things so that data can be accessed and monitored via a smartphone. Through network technologies like Bluetooth, Wi-Fi, and ZigBee, the controllers communicate with the CoT. When IoT architecture is cloud-based, it increases an enormous quantity of data analysis and gathering done online. Risk and difficulties in data privacy and security were brought about by this expansion and a lack of IoT device security [25]. Certain issues are contingent upon the end-user's and cloud's geographical locations. The national laws have an impact on the data. Unauthorised access by other users operating on comparable servers is another problem that arises with multi-tenancy difficulties [26].

4. The devices used in smart homes

Numerous issues plague smart home systems, including expensive device operating costs, the inability to remotely monitor a home, and security flaws in the system. Numerous systems were developed by researchers to address these issues. We go over five of the suggested systems in this section.

4.1. Blockchain-Integrated IoT-Based Smart Home System

The proliferation of IoT devices and their integration into smart homes has coincided with a rise in security risks, however, as most manufacturers fail to consider security protocols during the manufacturing process, hence rendering it more facile for hackers to compromise IoT devices. For example, default usernames and passwords provided by manufacturers are the source of the most well-known malware assault, known as Mirai, with 70.2% of consumers expressing serious security and privacy concerns. In order to find out what issues smart homeowners in Saudi Arabia had with using IoT devices in their homes, the researchers in this paper interviewed 270 of these individuals. These individuals were chosen at random, and the results showed that 72.2% of the respondents did not trust the cloud, and 41.1% did not know how their sensitive information was

handled and stored there. Based on these findings, the researchers concluded that security, privacy, and dependability are the main issues. Because smart houses require a system through which they can manage and monitor smart devices to meet security requirements, previous researchers proposed a mechanism by which a secure, easy-to-maintain, and cost-effective system for smart houses is designed. A blockchain is a series of blocks connected by a previous hash [27]. Blockchain is a distributed open ledger where records are accessible to all users of the network [1]. Three Internet of Things devices make up the researchers' suggested smart home scenario in this study. IoT security camera and light. This system satisfies the following requirements: availability, integrity based on a hash algorithm, confidentiality utilising asymmetric cryptography, and authentication via digital signature algorithm (DSA) [1].

4.2. Internet of Things (IoT): A Multi-Layer Security Monitoring System for Smart Homes

The IoTArgos machine learning (ML)-based two-stage intrusion detection module. Investigating supervised classification techniques in the initial phase to identify known assaults. In the classification stage, the second stage relies on the identification of unsupervised anomaly algorithms that capture newly emerging zero-day assaults without being noticed. The four main parts of the IoTArgos system architecture are as follows: 28].

A. IoT Multi-Layer Data Collection Data: One of the router-centered security monitoring system's strengths is its flexibility in gathering all communication data at one central location. At home programmable routers, IoTArgos gathers wireless packets (Zigbee, Bluetooth, and Wi-Fi protocols) and network flow records.
B. Characterising IoT communications data: Using multi-layer data collected from house programmable routers, characterise the communication behaviours of all IoT devices in smart houses, such as how, when, and why they communicate with local IoT hubs, house routers, control devices, and cloud servers. The ML-based intrusion detection component depends on traffic features from an IoT communication data collection.
C. ML-based intrusion detection: identify and stop known and unidentified threats, To detect intrusions using machine learning, IoTArgos employs a two-step procedure:
    - In the supervised classification step, the collected data is subjected to a supervised machine learning technique to distinguish between IoT attacks and traditional IoT data flows.
    - To find behaviours that are missed by the supervised classification step, an anomaly detection technique is applied in the unsupervised anomaly detection stage.
D. The real-time mitigation and defence component of IoTArgos initiates the necessary measures upon detecting and identifying intrusion activities. For instance, the compromised IoT devices and their corresponding hubs will be stopped or disconnected, an automated email will be sent to the homeowners, and the home router's firewall policies will be set up.

4.3. GHOST: Using Personalised Real-time Risk Control to Safeguard Home IoT Environments

GHOST is a reference architecture for protecting Internet of Things (IoT) systems in smart homes, financed by the European Union's Horizon 2020 research and innovation programme. It is a layered system design that maintains a high level of dependency within the framework while allowing the independent components to evolve separately. The following are the GHOST system and there are:

A. To enable consistent access to gateways managing IoT devices in smart homes, the gateway layer links the current gateway software environment with the Interoperability Middleware (IM) of the GHOST solution.

B. The direct network data collection and extraction are handled by the Data Interception and Inspection layer. Three components make up this composition:

Net Data Flow Analysis (NDFA) collects information from incoming network traffic that is routed through the Interoperability Middleware in order to identify anomalies in other components.

- Attack detection-specific metrics (cyber security metrics) are extracted using the Context Reasoning Time Series Approach (CR-TSA).
- Important context data (generic metrics) is gathered by the Context Reasoning Communication Events (CR-CE) component.

The parts manage data flow information that was previously managed by NDFA in order to pinpoint communications related to specific events that are happening for smart home devices.

C. The contextual profiling layer depends on the functionality of multiple components and offers the status of data and related behaviour of the network data provided by IoT devices: Profile Building (PB), Data Classification (DC), Template Extraction for Cyber Security (TE-CS), and Cross-Layer Anomaly Detection Framework (CLADF) are examples of templates.

D. The risk assessment layer conducts real-time risk assessments and reviews intelligence reports pertaining to notable warnings. It is made up of Safety Pattern Refinement (SPR) and Risk Engine (RE).

E. Supervision and tracking: The elements of this layer make sure that the risk reports that are available are shown in a way that is easy to use for homeowners.

- GHOST platform control and configuration can be accomplished by users through the methods and features offered by Configuration (CFG).
- Security Intervention (SI) facilitates user visualisation of risk tracking and outcome assessment.
- Information derived from contextual profiling, risk assessment layers, and data interception and inspection utilised in feedback analytical (FA) components for high-performance data monitoring and analysis.

F. Blockchain Defence Infrastructure: GHOST uses a Blockchain technique to guarantee data integrity for data exchanged across devices for central decision-making for risk assessment.

G. Gathering anonymized security intelligence and insights from web sources and other GHOST instances, the cyber security knowledge base is a cloud-based knowledge warehouse. Malicious actors and their assets are monitored. User feedback generates the data about the security intervention component. Subsequently, the information is examined in further detail and sent into the safety pattern refinement component, which enhances each GHOST platform separately.

- Public blacklisting: several installations work together to jointly build and maintain a list of harmful IP addresses.
- Consent forms: The miner nodes hash transaction records into an encrypted format. A Form of Consent is digitally signed by the users to notify them of the network's functioning principles and request their acceptance.
- Software integrity: The blockchain defence infrastructure network can store the data on GHOST installed software on IoT devices and smart home gateways. By guaranteeing that no unauthorised party may alter the firmware for software or devices, this will provide an additional degree of protection.

H. Shared data storage: A PostgreSQL database and its service are readily accessible to the GHOST components. Additionally, PostgreSQL offered an externally accessible secure interaction service. Technical aspects of data encryption are also employed to fulfil security needs.

I. The inter-component communication layer provides two ZeroMQ-based exchange patterns and links all of the components for direct communication:

- Upon connecting to a service, a client can initiate a request and receive a response.
- Publish/Subscribe: A client gives a group of subscriber’s access to data, and they can choose to designate a middleman broker.

Additionally, as Protocol Buffer is an effective way to encapsulate a succession of structure data, use it to encrypt messages between the components [29].

5. Monitoring the differences in smart home technologies

Many systems for smart homes were discussed in the preceding section. System security in smart homes was intended to be enhanced by the systems. Different implementations of the three basic security principles layering, limiting, and diversity allow blockchain, IoTArgos, and GHOST systems to meet the main security requirements (CIA). Comparing the systems' core security principles is shown in the table below.

Table 1. System security comparison

Systems	Layering	Diversity	Limiting
Blockchain system	Blockchain layer. Security built in smart house device.	This system has two different layers	It is limiting the access
IoTArgos system	Intrusion detection based on ML. Security built in smart house device.	This system has two different layers.	It is limiting the access
GHOST system	Gateway layer Data interception and inspection layer. Contextual Profiling layer Risk assessment layer Control and monitoring Blockchain defense infrastructure the inter-component communication layer	This system has many different security layers.	It is limiting the access

6. Conclusion

As our technological age progresses at a quick pace, smart homes which rely on the Internet of Things have started to emerge and grow in recent years. It saves homeowners comfort as well as a great deal of time and work. Numerous security issues also surface in return.

This study focuses on individual privacy and the security of smart homes, and it identifies exploitable weaknesses. The security and hazards that smart homes confront were examined by surveying a large number of prior studies on the subject. Comparing and contrasting the systems that are used to manage smart homes, as well as talking about the work that has been done in this area. In order to meet the security and privacy needs of smart homes, a number of academics have looked into the creation of an autonomous smart home operating system employing contemporary technology. This study outlined the advantages for anyone wishing to build a smart home by assisting researchers in conducting several experiments on smart home technologies and helping them select a system that satisfies security standards.

References

[1] Abdullah, A., Hamad, R., Abdulrahman, M., Moala, H., & Elkhediri, S. (2019, May). CyberSecurity: a review of internet of things (IoT) security issues, challenges and techniques. In 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS) (pp. 1-6). IEEE.

[2] Al-Enazi, M., & El Khediri, S. (2021). Advanced Classification Techniques for Improving Networks' Intrusion Detection System Efficiency. Journal of Applied Security Research, 1-17.

[3] Umakant Dinkar Butkar, Manisha J Waghmare. (2023). Hybrid Serial-Parallel Linkage Based six degrees of freedom Advanced robotic manipulator. *Computer Integrated Manufacturing Systems*, *29*(2), 70–82. Retrieved from http://cims-journal.com/index.php/CN/article/view/786

[4] Umakant Dinkar Butkar, Manisha J Waghmare. (2023). Novel Energy Storage Material and Topologies of Computerized Controller. *Computer Integrated Manufacturing Systems*, *29*(2), 83–95. Retrieved from http://cims-journal.com/index.php/CN/article/view/787

[5] Umakant Dinkar Butkar, Manisha J Waghmare. (2023). Advanced robotic manipulator renewable energy and smart applications. *Computer Integrated Manufacturing Systems*, *29*(2), 19–31. Retrieved from http://cims-journal.com/index.php/CN/article/view/782

[6] Umakant Dinkar Butkar, Manisha J Waghmare. (2023). Crime Risk Forecasting using Cyber Security and Artificial Intelligent. *Computer Integrated Manufacturing Systems*, *29*(2), 43–57. Retrieved from http://cims-journal.com/index.php/CN/article/view/784

[7] Umakant Dinkar Butkar, Dr. Pradip Suresh Mane, Dr Kumar P K, Dr. Arun Saxena, Dr. Mangesh Salunke. (2023). Modelling and Simulation of symmetric planar manipulator Using Hybrid Integrated Manufacturing. *Computer Integrated Manufacturing Systems*, *29*(1), 464–476. Retrieved from http://cims-journal.com/index.php/CN/article/view/771

[8] Umakant Dinkar Butkar* & Dr. Nisarg Gandhewar. (2022). AN RESULTS OF DIFFERENT ALGORITHMS FOR ACCIDENT DETECTION USING THE INTERNET OF THINGS. *Harbin Gongye Daxue Xuebao/Journal of Harbin Institute of Technology*, *54*(10), 209–221. Retrieved from http://hebgydxxb.periodicales.com/index.php/JHIT/article/view/1366

[9] Umakant Dinkar Butkar, Dr. Nisarg Gandhewar. (2022). ALGORITHM DESIGN FOR ACCIDENT DETECTION USING THE INTERNET OF THINGS AND GPS MODULE. *Journal of East China University of Science and Technology*, *65*(3), 821–831. Retrieved from http://hdlgdxxb.info/index.php/JE_CUST/article/view/313

[10] Belimpasakis, P., & Moloney, S. (2009). A platform for proving family oriented RESTful services hosted at home. IEEE Transactions on Consumer Electronics, 55(2), 690-698.

[11] Mittal, Y., Toshniwal, P., Sharma, S., Singhal, D., Gupta, R., & Mittal, V. K. (2015, December). A voice-controlled multi-functional smart home automation system. In 2015 Annual IEEE India Conference (INDICON) (pp. 1-6). IEEE.

[12] Batalla, J. M., Vasilakos, A., & Gajewski, M. (2017). Secure smart homes: Opportunities and challenges. ACM Computing Surveys (CSUR), 50(5), 1-32.

[13] Alohali, B., Merabti, M., & Kifayat, K. (2014, September). A cloud of things (cot) based security for home area network (han) in the smart grid. In 2014 eighth international conference on next generation mobile apps, services and technologies (pp. 326-330). IEEE.

[14] Arabo, A., Brown, I., & El-Moussa, F. (2012, September). Privacy in the age of mobility and smart devices in smart homes. In 2012 International Conference on Privacy, Security, Risk and Trust and 2012 International Confernece on Social Computing (pp. 819-826). IEEE.

[15] Al-Qahtani, A. S., & Khan, M. A. (2021). Predicting Internet of Things (IOT) Security and Privacy Risks–A Proposal Model.

[16] Huraj, L., Šimon, M., & Horák, T. (2020). Resistance of IoT sensors against DDoS attack in smart home environment. Sensors, 20(18), 5298.

[17] Sanchez, V. G., Pfeiffer, C. F., & Skeie, N. O. (2017). A review of smart house analysis methods for assisting older people living alone. Journal of Sensor and Actuator Networks, 6(3), 11.

[18] Karimi, K., & Krit, S. (2019, July). Smart home-smartphone systems: Threats, security requirements and open research challenges. In 2019 International Conference of Computer Science and Renewable Energies (ICCSRE) (pp. 1-5). IEEE.

[19] Alohali, B., Merabti, M., & Kifayat, K. (2014, September). A cloud of things (cot) based security for home area network (han) in the smart grid. In 2014 eighth international conference on next generation mobile apps, services and technologies (pp. 326-330). IEEE.

[20] AL MOGBIL, R., AL ASQAH, M., & EL KHEDIRI, S. (2020, September). Iot: Security challenges and issues of smart homes/cities. In 2020 International Conference on Computing and Information Technology (ICCIT-1441) (pp. 1-6). IEEE.

[21] Wen, Y., & Liu, T. (2018, October). WIFI Security Certification through Device Information. In 2018 International Conference on Sensor Networks and Signal Processing (SNSP) (pp. 302-305). IEEE.

[22] Haines, B. (2010). Seven deadliest wireless technologies attacks. Syngress.

[23] Sevier, S., & Tekeoglu, A. (2019, January). Analyzing the security of Bluetooth low energy. In 2019 International Conference on Electronics, Information, and Communication (ICEIC) (pp. 1-5). IEEE.

[24] Malche, T., & Maheshwary, P. (2017, February). Internet of Things (IoT) for building smart home system. In 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) (pp. 65-70). IEEE.

[25] Kashyap, N., Rana, A., Kansal, V., & Walia, H. (2021, February). Improve Cloud Based IoT Architecture Layer Security-A Literature Review. In 2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS) (pp. 772-777). IEEE.

[26] Singla, S., & Bala, A. (2018, April). A review: cryptography and steganography algorithm for cloud computing. In 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT) (pp. 953-957). IEEE

[27] Al-Turkistani, H. F., & AlSa'awi, N. K. (2020, November). Poster: Combination of Blockchains to Secure Smart Home Internet of Things. In 2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH) (pp. 261-262). IEEE.

[28] Wan, Y., Xu, K., Xue, G., & Wang, F. (2020, July). Iotargos: A multi-layer security monitoring system for internet-of-things in smart homes.
In IEEE INFOCOM 2020-IEEE Conference on Computer Communications (pp. 874-883). IEEE.

[29] Augusto-Gonzalez, J., Collen, A., Evangelatos, S., A nagnostopoulos, M., Spathoulas, G., Giannoutakis, K. M., ... & Nijdam, N. A. (2019, September). From internet of threats to internet of things: A cyber security architecture for smart homes. In 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD) (pp. 1-6). IEEE.