iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** IX **Month of publication:** September 2021

DOI: https://doi.org/10.22214/ijraset.2021.38026

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue IX Sep 2021- Available at www.ijraset.com

A Survey on Security Issues in IOT Enabled Smart Homes

Gummadi Rohith Madhu Chandra[1], Sri Harsha Samayamanthula[2]
[1, 2]*School of Computer Science & Engineering, Vellore Institute of Technology,Vellore, India*

Abstract: ***Smart home systems are having in great popularity and demand for the past few decades as they increase the comfort and quality of life. Smartphones and microcontrollers are used to control most of these devices.A smartphone application is used to monitor home functions and perform various tasks with wireless communication technologies. IoT has changed organizations by incorporating dexterity and effectiveness. However, one of the biggest concerns associated with this field is Security. In 2016, a hacker had discovered a weakness in video cameras that came about in very nearly 300,000 IoT gadgets assaulting other online media stages, which even cut down Twitter. This is only one of the numerous instances of how Security has frequently got compromised in 'things.' In this survey paper, our objective is to know the details of smart home ,its's archictecture and it's security issues in this contemporary world. We will survey the security concerns of IoT in Smart Homes. Towards the second part of the paper, we will also discuss some of the developments that have been made to overcome these challenges and used for security in smart homes.***

Keywords: Sensors, Internet of things, Security, Smart Homes, Home appliances.

I. INTRODUCTION

A smart home is an advanced home system in which numerous appliances can be connected remotely from anywhere with an internet connection using a mobile, pc, and other networking devices. Devices and appliances in a smart home are connected online; this fundamentally permits the client to control different functions, for example, security access to the home, temperature upkeep in homes, workplaces, lighting, and CC television cameras around the home. A smart home is the ideal mix of data innovation and sensor administrations using home networks with various home gadgets for a superior nature of way of life, hence clearing a path of living simpler[1]. It utilizes an assortment of innovations to prepare various gadgets by monitoring and controlling the keen lodging framework proficiently and cleverly. It empowers the home functionalities for smooth and blunder-free correspondence between them so day by day family errands also, capacities are conceivable consequently without human intervention or with the assistance of distant client control in a proficient, secure, simple, and reasonable way.

II. IOT IN SMART HOMES

Most pivotal functions of Iot based smart home are[2]-

A. Alert

In addition, the smart home system is capable of detecting its surroundings and sending warnings to the client through a device or account that is registered. You'll get a text message or e-mail with data from the nearby area.This information may contain whether the temperature is too high or low or moderate, humidity, whether the percent of water vapor is high or low, light intensity, etc. A periodic notification may be delivered to the client at a predetermined time. An email, SMS, or other form of notification may be used.

B. Moniter

Monitoring in a smart home is a very important task. With the help of numerous sensors and video feeds, a smart house can monitor its surroundings. A monitoring system is important because it keeps track of every action in the home, which is the basis for any further action or choice— For example, checking the room temperature and sending a warning to the customer to turn on the air conditioner if the temperature exceeds the limit, monitoring the elderly person in the home and pressing the emergency button when it recognises a sudden fall, etc.

C. Control

Controlling a smart home involves automating a variety of tasks that do not need direct human involvement. In addition to turning on/off lights and air conditioners as well as locking a door or opening a door to a bathroom, these control capabilities may also open/close emergency exits, among others. It's up to the customer whether they want to control things from the same spot or from a distance. In fact, this capability allows the client to automate actions such as turning on/off the climate control system based on the room's temperature.

D. Intelligence

Home Intelligence (HI) is the most important function of a smart home and the main reason for its intelligent behavior . This is the function which automatically involved in decision-making on various scenarios. In the smart home setting, HI relies on the Artificial Intelligence (AI) mechanism that is built in.

In addition to being the brain of smart home, HI is crucial from a security standpoint. It is an artificial intelligence (AI) tool in a smart home that creates an environment that can detect changing situations and situations and respond appropriately.HI is able to alert customers to unexpected situations and respond quickly when needed[3]. When a user arrives at home, for example, coffee is automatically brewed, and an alert is sent to the user if suspicious activity is detected at the door or inside the house, groceries are automatically ordered when there is a shortage in the refrigerator, electricians and plumbers are notified when maintenance is needed, etc.

III. LITERATURE SURVEY

When it comes to Internet of Things (IoT), this is a new technology that utilises internet connection to link sensors in cars, hospitals, businesses and consumers all around the globe. As a result of this design, smart cities, smart homes, smart agriculture, and a smart world have been developed. Because of the enormous number of devices, connection layer technologies, and services involved, IoT architecture is extremely complicated.

Nevertheless, Security is the essential factor in IoT. With the aid of Smart World, they provided an overview of IoT architecture in this paper. They examined the security issues in IoT, followed by IoT security methods, in the second portion of this paper. Finally, the difficulties addressed in the study might serve as research directions.[4]

Homes with IoT products and services are becoming increasingly popular, with numerous promises of improving people's quality of life.Nonetheless, the diverse, dynamic, and Internet-connected character of this ecosystem introduces additional problems as private data becomes available frequently without the owners' knowledge. Because of this accessibility, Data security and privacy breaches, as well as the importance of smart home security, should be examined. In this article, the authors provided an outline of the privacy and security issues raised by the smart home.They also identified restrictions, evaluated options, and addressed a number of problems and research concerns that deserve more examination.[5]

Maintaining privacy and overcoming security threats is a significant problem for IoT networks. This study examined IoT security issues in depth. For starters, the Internet of Things is described in the Industrial and Medical service settings and the safety concerns of various levels of healthcare engineering are examined. We also cover a wide variety of malware found in the context of the Internet of Things (IoT), such as spyware and malware. Last but not least, recent malware attacks such as Mirai, EchoBot and Reaper are causing concern for many people these days. A comparison of the efficiency of several machine learning algorithms in reducing security vulnerabilities is given. It has been discovered that the k- closest neighbor (kNN) machine learning method performs exceptionally well in identifying malware. In addition, this study examines several technologies for ransomware detection, categorization, and analysis. As a final step, an assessment of current security issues is given along with open challenges and possible future possibilities for IoT security assurance. [6]

The dynamic, diverse and connected nature of smart homes creates new security, authentication and privacy challenges. This study explores security risks in smart homes and their impact on system overall security. In the smart home context, they identified security requirements and solutions. They have also attempted to give remedies to a few authentication problems.[7]

IV. ARCHITECTURE OF SMART HOMES

An efficient and well-to-do smart home means a strong and powerful architecture that satisfies all the requirements for the perfect functioning of smart homes. The complete architecture has been divided into two major parts, the components that make up the smart homes and the architectural model that is the foundation of the core structure of smart homes.

A. Smart Home Components

1) *Smart Devices with interoperability capability:* A smart device is an electronic device that is controlled by specific actuators under the supervision of an electrical chip, microcontroller or microprocessor (microcontroller). These devices can connect to other devices or networks through various wireless protocols such as Bluetooth, BLE, ZigBee, NFC, Wi-Fi, Thread, Loravan, etc., so that they can work independently up to a certain point and share sensor data with each other, and their server locally. Store permanently in / Central Control Box etc. Artificial intelligence enables these gadgets to exhibit additional ubiquitous computing characteristics.

2) *Smart home Gateway or Central Control Box:*The Central Control Box (CCB) is the most important part of the smart home framework. CCB is a general purpose computer with the appropriate software and support that acts as an external display gateway that can store large amounts of data with efficient real-time processing and Internet support.The CCB/Gateway may be accessible from anywhere utilising mobile devices such as a tablet, smartphone, or laptop as soon as it is linked to the outside world or the Internet[8]. [9] The portal handles various tasks such as device configuration and identity management, analysis and access to cloud services, required integration of devices or services, authorization and authentication.
3) *Smart Home Network:* Using a Smart Home Network, you may learn about the network connection or performance of different nodes or devices, network intercommunication protocols, and wired/wireless connection medium. With its dynamic (because to device mobility) and mesh design, it aims to optimise connections between nodes and offer improved services to consumers. In addition, the home network may store mesh topology, a star topology, or centralised wireless peer-to-peer networks using the wireless protocol.
4) *Mobile application and web applications for remote access:* Small clients are used to enable access to devices placed in a smart home, following intelligent local gateway verification or service provider authorisation, and they integrate web service API by enabling procedures that allow the user to set up, operate, and access his or her IoT Device.. Aside from device detection, the CCB may also be used to react to alerts on devices for remedial actions.

B. Architectural Model

Wireless Sensor Networks and Hierarchical Mobile IP have been integrated into the architecture of Smart Homes [10]. As part of the current HMIPv6 technological requirements, the conventional collection of Smart Homes has been improved by enabling mobility. This may be shown in Figure 2, in which a home user can manage domestic goods or appliances linked to the home network even if he is accessing the external network. It is important to note that a PDA, mobile phone, or tablet that is used by a home user while they are away from the home network and connect in to an external network is concerned with an address that specifies the user's position. HMIIv6 enables users of mobile devices whose addresses are linked with a single network to continue to communicate even after moving from one network to another, even though they have a new IP address. Any packets transmitted by a device that has been linked to a user's device in a home network must have a care-of address (LCoA and RCoA) relayed back to the home network [10]. Regardless of where the mobile node is on the home network, each mobile node is identified by its address at home. For example, mobile IP is often used to transport devices across various LANs with distinct IP addresses in wireless wide area networks (WANs). Using IPv6 communication formats, a smart home system will be able to link nodes (home items) and share information. Authentication methods, such as this MIPv6 transmission system, will be used to verify that the home network is owned and maintained by a genuine resident and homeowner.

V. SECURITY CHALLENGES IN SMART HOME ENVIRONMENT

Expansion in IoT devices sees a huge profit for both organizations and businesses which work on a lot of processes, but there are also some disadvantages coming with it. One of these disadvantages is Security, protection and having our own information being communicated between devices accompanies the danger of losing a lot of our Security [11]. The IoT paves the way for some malevolent attackers who wish to misuse IoT device shortcomings to get to a person's personal data to be utilized for their own benefit. Security is a significant issue as IoT is expanding to many businesses and administrations while attempting to ensure that the delicate information and devices are well protected from any harmful attacks.

As in IoT, everything is associated with the Internet. Security will turn into a major issue. A great deal of personal data of an individual can be made out without the individual having any idea regarding it. Control on the dispersion of all such data is incomprehensible in the present situation. In this way, the clients of the IoT framework need to deal with their own information [12]. The people owning the network should realize who is utilizing their information and how it is going to cause problems.

There are also problems with IoT devices such as complex systems, which provide more opportunities for failure, and also, With all of this data being sent, the danger of losing all of the data is quite real indeed. They are particularly susceptible to DOS attacks due to the fact that data is sent wirelessly between sensors and equipment. These kinds of assaults are carried out by sending a stream of messages that collide with each other. These collisions cause the sensors to run out of battery power. Others include preventing users from exchanging configuration information by interfering with the communication medium. Another kind of physical assault is the sinkhole attack, which involves the attacker physically accessing the sensors. If any sensors are compromised by malicious code, attackers may keep a constant eye on the home.

A. Security Threats in the Smart Home

When it comes to security risks, even if Smart Home has a completely distinct environment, they are similar to other technological sectors. As a result, sensitive information may be leaked without consent. The unintentional discovery of sensitive medical data may arise from a privacy violation in home monitoring systems, for example. To detect whether or not a house is occupied as a prelude to theft, even apparently innocuous data may be utilised. Unauthorized access to the system will be a danger if items like unique keys and passwords are compromised.

Information that has been altered or updated may be detected or controlled by threats of authentication. Illegal system alarms, For example, he may deceive the housekeeper into believing that there is an emergency and may open doors and windows to allow an emergency escape when it is really intended to allow illegal entry.When it comes to automated software upgrades that are not adequately verified, significant problems may arise in the long run.

There is no question that access risks are the most serious ones. All systems are rendered vulnerable when there is an unauthorised access to the system controller.

This can be done with incorrect password and key management or by unauthorized devices connecting to the network.Unauthorized connections to the network, even if they are uncontrolled, may rob the network of bandwidth or cause genuine users to be unable to access the network at all.

Due to the fact that many Smart Home gadgets are powered by batteries and linked wirelessly in a low-performance cycle, flooding networks with requests may lead to end-to-end assaults and energy depletion attacks.

B. Security Vulnerabilities in the Smart Home

One of the extreme vulnerabilities in Smart Homes is network access. Because existing smart home applications are connected to the Internet, they can be attacked remotely by accessing communication control networks directly or by installing malware on devices. It is also difficult to get access to the system physically. Even if the home is secured, wireless network technologies and power-line networks may be accessed from outside. [13]

It's also possible that you've got a restricted budget. 8-bit microcontrollers with limited computation and storage capabilities have traditionally been used as device controllers. This limits the ability of device controllers to utilise sophisticated security methods. Heterogeneity inside a system is hazardous. In addition to being built by a variety of vendors, devices utilise a variety of connection protocols and software update capabilities.

Sometimes, there is no documentation regarding the devices' internal software or operating systems. Another issue is the need for updated firmware. Very few home products provide a regular software update service to protect against security threats, and those that do are rare. If a gadget costs more than a few dollars, there is a modest incentive to keep updating software to stay ahead of the security threats, according to the theory.

As a result, slow pick-up rates may be a problem. When it comes to Smart Home gadgets and programmes, most of them aren't as secure as other connected programmes such as a health monitoring system that adheres to industry standards. Because Smart Home networks are becoming more complicated, we believe it's very risky to handle them without the help of security experts. Only a small percentage of households can afford to pay for continuous technical support for their home network. Instead, amateur homeowners need to be able to quickly, securely, and safely manage their systems.

VI. PROPOSED METHOD

To ensure data transmission integrity and confidentiality between devices and other media, smart home gateways rely on the usage of blockchain to secure data transfer. When it comes to smart home networks, they all have a centralised network form, but they've been transformed from one into the other by using blockchain at the cloud layer. There are three levels of the proposed smart home gateway based on the blockchain: device layer, gateway layer and cloud layer. Devices and sensors make up the basic layer of the smart home network, called the device layer. The gateway layer stores the data generated by the device layer and makes it available to users as needed. The device layer is the first layer in the stack. The cloud layer contains the gateway ID and the third layer of the blockchain contains the data processed by each gateway. Blocks are shared so that users can access information at any time and from anywhere. [14]

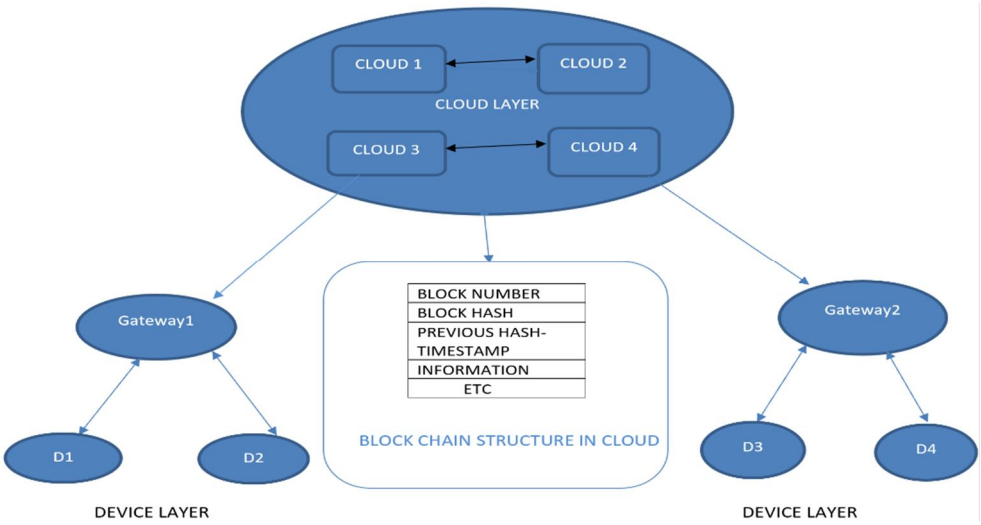


FIG. 1 STRUCTURE OF THE MODEL

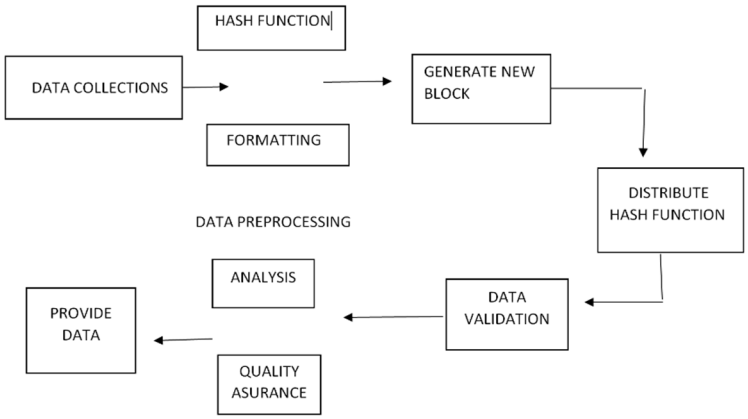


FIG.2 Flowchart

VII. RECENT DEVELOPMENTS IN OVERCOMING THESE CHALLENGES

Smart home devices that are connected should be safeguarded by a complete IoT (cloud-to-cloud) solution that does not disband the OEMs profit or marketing time and the service provider. Lately, during the past years, there have been many innovations in the field of Security to overcome the issues concerning Security in Smart Homes. According to researchers, the latest comprehensive IoT security solutions have started including the following capabilities:

A. Secure Booting

A cryptographic code signature method is used in the secure boot to ensure that the device only utilises OEM code produced by the device or another trusted party. Using secure boot technology, attackers cannot modify the firmware with malicious versions.

B. Mutual authentication service

A smart home gadget must be authenticated every time it connects to a network in order to receive and transmit any data. If the data originates from a legitimate device, it's safe to assume it's authentic. For two-way authentication, cryptographic methods with symmetric or asymmetric keys may be employed. If the data is derived from a legitimate device, it is safe to assume that it is genuine. Use the Secure Hash (SHA-x) algorithm for symmetric keys and the Elliptic Curve Digital Signature (ECDSA) algorithm for asymmetric keys.

C. Secure communication by encrypting data

A method for protecting data during the transfer from the device to the service (cloud infrastructure).It is ensured by encryption that only those who have a secret encryption key can get hold of the transmitted data. So, for example, a smart thermostat that transmits usage statistics to a service provider can securely retrieve data from digital spying.

D. Monitoring and analysis of Security

Records data from a variety of sources, including endpoint devices and network connections. Afterwards, the data is examined for any security breaches or system risks. Once found, a comprehensive list of actions taken in the context of the security policy of the entire system should be prepared, such as the elimination of devices according to undesirable behavior. Analyzing use patterns and possible attack scenarios may be done in real-time or at a later date. Endpoint devices must be secured against potential tampering and data fraud, which may lead to incorrect reporting of activities.

E. Life cycle management of security service

Using the life cycle management function, service providers and OEMs may monitor and manage the safety features of IoT devices while they are in operation. During a catastrophe recovery, fast over-the-air (OTA) key replacement guarantees minimum service interruption.In addition, the termination of the secure service ensures that discarded devices will no longer be used to connect to the service without permission.

REFERENCES

[1] International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163 Volume 2 Issue 1 (January 2015) www.ijirae.com 2014, IJIRAE- All Rights Reserved Page -81 Smart Home System Mr.Rohit Kadam1 ,Mr.Pranav Mahamuni2 ,Mr.Yash Parikh3 1 (Department of Computer Engineering, Sinhgad Institute of Technology and Science, Pune, India) 2 (Department of Mechanical Engineering, Sinhgad Institute of Technology and Science, Pune, India) 3 (Department of Mechanical Engineering, Symbiosis Institute of Technology, Pune, India).

[2] Internet of Things (IoT) for building Smart Home System February 2017, DOI:10.1109/I-SMAC.2017.8058258, Conference: I-SMAC

[3] David Bregman, “Smart Home Intelligence - The eHome that Learns”, International Journal of Smart Home, Vol. 4, No. 4, October, 2010.

[4] Internet of Things (IoT): A vision, architectural elements, and security issues, February 2017,DOI:10.1109/I-SMAC.2017.8058399, Conference: 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)

[5] On Privacy and Security Challenges in Smart Connected Homes Joseph Bugeja, Andreas Jacobsson, and Paul Davidsson Internet of Things and People Research Center and Department of Computer Science Malmö University, Malmö Sweden, {joseph.bugeja, andreas.jacobsson, paul.davidsson}@mah.se, 2016 European Intelligence and Security Informatics Conference.

[6] Prajoy Podder, M. Rubaiyat Hossain Mondal, Subrato Bharati, and Pinto Kumar Paul. Review on the security threats of Internet of things. International Journal of Computer Applications, 176(41):37–45, Jul 2020

[7] Privacy and Security issues in IoT based Smart Home Applications; H Manoj T Gadiyar, Dr. Thyagaraju G S, Bhavya T , Bhavana, Mamath, Ahana Assistant Professor, Department of CSE, SDMIT, Ujire Professor, Department of CSE,SDMIT.

[8] Waheb A Jabbar, Tee Kok Kian, Roshahliza M Ramli, Siti Nabila Zubir, Nurthaqifah SM Zamrizaman, Mohammed Balfaqih, Vladimir Shepelev, and Soltan Alharbi. Design and fabrication of smart home with internet of things enabled automation system. IEEE Access, 7:, 2019.

[9] T. Malche and P. Maheshwary. 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), 2017.

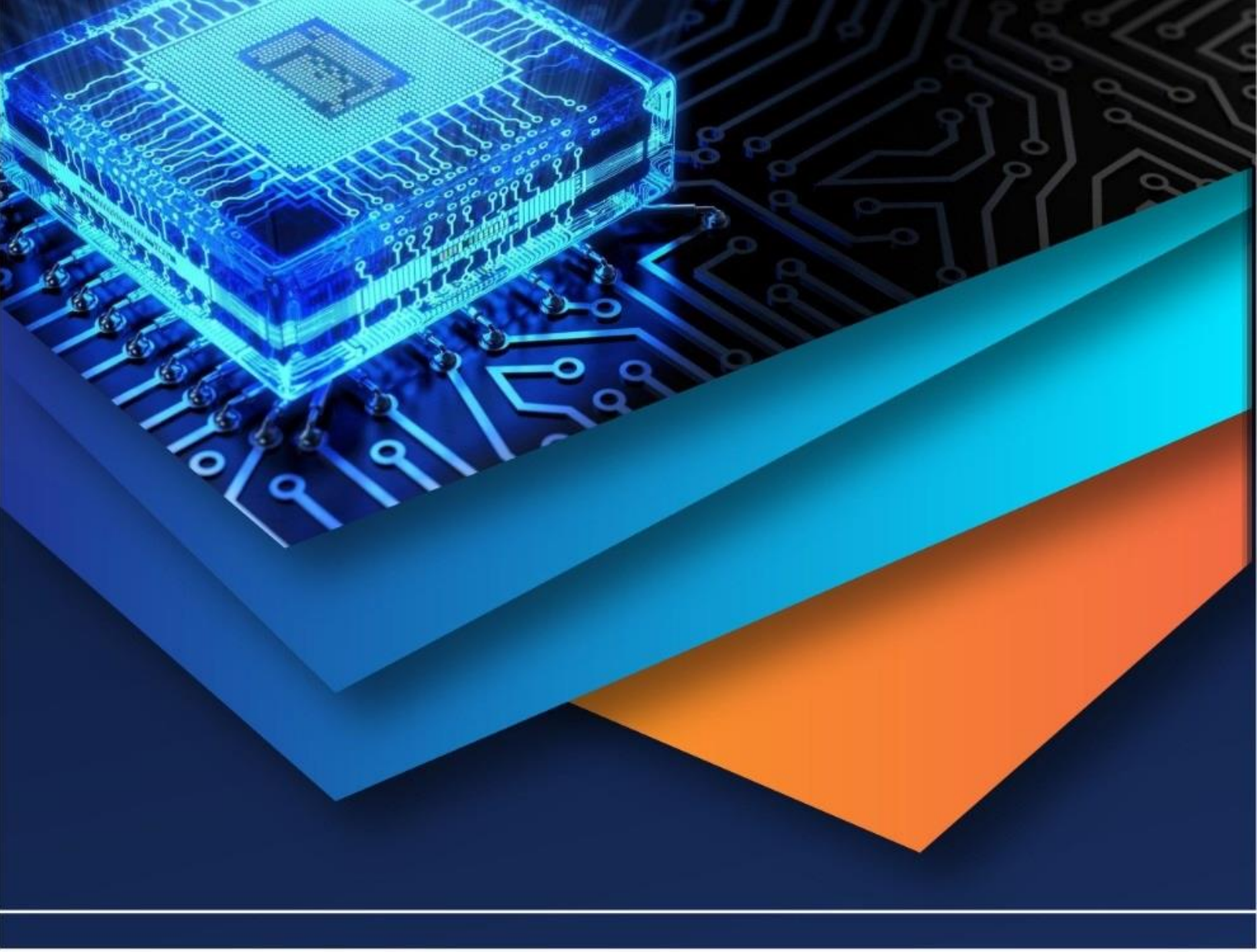
[10] K. Bing, L. Fu, Y. Zhuo, and L. Yanlei. Design of an internet of thingsbased smart home system. In 2011 2nd International Conference on Intelligent Control and Information Processing, volume 2, pages 921– 924, 2011

[11] Mookyu Park, Haengrok Oh, and Kyungho Lee. Security risk measurement for information leakage in iot-based smart homes from a situational awareness perspective. Sensors, 19(9):2148, 2019.

[12] Biljana L Risteska Stojkoska and Kire V Trivodaliev. A review of internet of things for smart home: Challenges and solutions. Journal of Cleaner Production, 140:1454–1464, 2017.

[13] Li Da Xu, Wu He, and Shancang Li. Internet of things in industries: A survey. IEEE Transactions on industrial informatics, 10(4), 2014.

[14] A blockchain-based smart home gateway architecture for preventing data forgeryYounghun Lee, Shailendra Rathore, Jin Ho Park & Jong Hyuk Park ,Human-centric Computing and Information Sciences volume 10, Article number: 9 (2020).



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY