IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 11, Issue 1, January 2022

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.569

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 11, Issue 1, January 2022 ||

| DOI:10.15680/IJIRSET.2022.1101012 |

Access Controlling in Smart Homes

N.Divya[1], Dr. M. Sailaja[2]

PG Scholar, Department of Electronics and Communication Engineering, University College of Engineering, Kakinada, India[1]

Professor, Department of Electronics and Communication Engineering, University College of Engineering, Kakinada, India[2]

ABSTRACT*:* This paper comprises the design of Access Controlling in Smart Homes is the subject of this article. One of the greatest ways for dealing with this problem is access control, which has been utilized to protect smart homes. To implement the access control in smart homes presented in this paper, we created two applications using Android and Python. The results of the experiments reveal that the access of various unauthorized individuals may be controlled.

KEYWORDS-Smart Homes, Access Control, Authorized frameworks.

I.INTRODUCTION

People's lives have already been changing from a physical to a virtual dimension in that they can speak, messaging, work, and interact with interconnected objects since Kevin Ashton first proposed the Internet of Things (IoT)[1], and with the rapid progress of networking technologies and the IoT, people's lives have been changing from a physical to a virtual dimension in which they can talk, chat, work, and engage with linked objects performance.

The smart home was designed to make people's lives simpler and to change the way we live, play, and do business. Its purpose is to make life easier to adjust to, more comfortable, and pleasurable. Aside from the benefits of smart homes, there are a number of security and privacy problems that must be considered while designing and planning a smart home. While new home technologies are being introduced to make our houses smarter and more automated, cyberspace is rapidly expanding[2–5], surrounding our lives with billions of smart gadgets that can cause privacy and security concerns[6–10].

Many manufacturers and businesses are deploying smart home technology, which is one of the most important and fastest-growing domains. For local users, the smart home encompasses home automation, home monitoring, and home security. Smart homes are vulnerable to a variety of security and privacy risks. Hacking a smart home's security cameras, for example, can compromise the user's privacy and allow access to sensitive information. Numerous privacy and security issues exist for smart homes and their users.

Hacking a smart home's security cameras, for example, might compromise a user's privacy by gaining access to sensitive information such as health records, photos, and videos. These infractions and illegal access to the smart home can lead to a slew of serious and potentially fatal issues. Multiple people can utilize a user-friendly interface, such as a web browser or a mobile application, to access smart home equipment.

Third-party vendor applications connect with a back-end cloud system by controlling smart home devices via mobile and web browser interfaces. To tackle smart home authentication issues and ensure that intruders would not reach critical resources, firms and organizations must impose access control. There are indeed a variety of commercial authorization frameworks, including some that impose coarse-grained access limits.
An analysis on existing smart home authorization options has been offered, as well as their evaluation based on information stated. There have been rules and unsolved difficulties to address while creating smart home authorization mechanism.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 11, Issue 1, January 2022 ||

| DOI:10.15680/IJIRSET.2022.1101012 |

II.LITERATURE SURVEY

1. In smart cities, IoT-enabled smart Lighting system: The rapid urbanization has accelerated dramatically in recent years. In order to create a better livelihood in metropolitan regions, greater upgraded resources and apps are required. The notion of a smart city, which would be the interconnection of modern electronic innovations mostly in setting of a city, is a promising step towards better and effectiveness of urban services. With advent of Internet-of-Things (IoT) in the smart city, great possibilities to build services and combine diverse application areas one another have developed. During an IoT-enabled smart city setting, nonetheless, all apps must be operated using minimal power resources in order to provide smooth solutions.

2. From the internet to the intelligent world: The advancement of modernization and intelligence propels the Internet into a digital century. A quaternion cyber-physical-social-thinking hyperspace, based on which an embryo of a digital environment is being constructed via diverse places, is created by a profound merging between many cyber space, physical space, social space, and thinking space. The bright world is supposed to be an appealing vision integrating omnipresent detection, processing, and networking in order to accomplish complete linkages of observation, cyber interaction, social correlation, and cognitive thinking.

3. In protected ZigBee networks, a timestamp technique is used to prevent replay attacks: ZigBee is a connection - oriented protocol that is commonly used in Internet of things applications. Several communication functions are deactivated in common development circumstances low-cost and low-power IoT devices, compromising ZigBee privacy. In a protected ZigBee network, the ZigBee standard believes that frame counters are adequate to prevent replay attacks. We provide a timestamp-based technique to prevent replay assaults as a prevention method. Our prevention technique uses very little electricity, and reasonably powerful systems would be responsible for supplying the present timestamp to power-constrained devices.

4. Evaluation of the safety of new smart home apps: Various smart home programming frameworks which permit third-party application software had emerged as competitors. Users profit from these frameworks, but they may also be exposed to cyber threats. The first in-depth empirical security examination of one such emergent smart home software platform is presented in this work. We looked at Samsung's Smart Things, which has the most apps of any smart home platform presently available and supports a wide variety of equipment such as motion sensors, fire alarms, and door locks. The software runtime is hosted on a proprietary, closed-source cloud back end, makes examination difficult. With a basic source code evaluation of 499 Smart Things apps (named Smart Apps) with 132 device handlers, as well as pre prepared test cases, we were able to overcome the problem.

In the industrial Internet of Things, there are security and privacy concerns: Embedded, mobile, and cyber physical systems are already commonplace, with applications ranging across control systems to contemporary cars and essential services. Present conditions and projects, including "Industry 4.0" and the Internet of Things (IoT), offer creative marketing strategies and novel customer reviews by leveraging robust connectivity and implementing next-generation embedded systems. Those systems create, analyze, and transmit massive volumes of security-critical and privacy-sensitive data, making them easy prey for hackers. Cyber attacks on IoT equipment are extremely dangerous though they may inflict direct harm and even endanger people's lives.

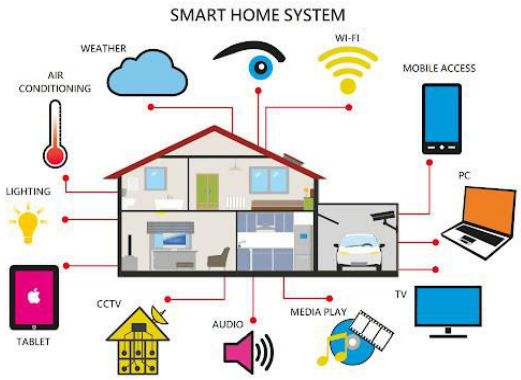
III. SMART HOME

In today's world, the smart home is a significant application. In smart homes, smart gadgets such as doorbells, thermostats, locks, digital appliances, lighting, and freezers are installed and programmed. They may be operated remotely by homeowners using user-friendly interfaces like internet browsers or phone apps. Machine-to-machine or human-to- machine connections are possible within the smart homes. A smart fridge, as a sample of machine-to-machine communications, may automatically communicate with a smart phone and provide a notice if anything in the refrigerator is getting low, like as milk or fruit. Due to its multi-user and multi-device nature, the smart home application poses a number of issues.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 11, Issue 1, January 2022 ||

| DOI:10.15680/IJIRSET.2022.1101012 |



IV. SMART HOME ELEMENTS

The smart home components, also known as nodes, generally categorized into three elements:

- **Application nodes:** Users may transmit orders to actual equipment from these nodes, which could be smart phones, laptops, or robotic systems.
- **Intermediate nodes:** This is a type of wireless internet access technology that links application nodes to physical equipment so that users may transmit commands back and forth.
- **Physical nodes:** These include smart household appliances such as smart bulbs, fans, heaters, refrigerators, and more. Application nodes provide orders to this technology, which it subsequently executes to turn on or off.

V.PROPOSED WORK

The ease with which this equipment may be accessed raises a security concern. Additionally, there are access restrictions in place to ensure that this device is not accessible by various family members, house employees, or youngsters. For instance, children must have access to television for a period of time, and guests must have access to air conditioning for a period of time, among other things. As a result, controlling this access may be a challenge, hence several access control mechanisms such as role-based, category-based, and others have been implemented.

We developed two Android and Python applications to implement this task. The Python application acts as a simulation, receiving orders from the Android app and then executing these instructions to turn on or off the light source.The Android application will establish a connection with the Python program and deliver requests to it. Here, we show several images that symbolize smart equipment, and that they will change its color to red or green depending just on orders they provide.

The essential modules make up the Python application:

- **Design a Smart Home Network:** This module generates various figures that will be displayed in the simulation.
- **Create Access Control:** With this component, a user can grant a certain user access to a specific equipment.
- **Remove Access Control:** The proprietor has the ability to revoke access to any user at any moment.

The modules that make up an Android application are as follows:

- **Check connection:** Android will use this component to verify the connection between itself and the Python simulation.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 11, Issue 1, January 2022 ||

| DOI:10.15680/IJIRSET.2022.1101012 |

- **Access Code:** To use this component, the user must first input their name, after which the programme will verify whether or not the user has access.
- **Commands:** To use this module, a user may pick a bulb on or off command, transmit it to the simulation programme, and the command will be performed based on access permissions.
-

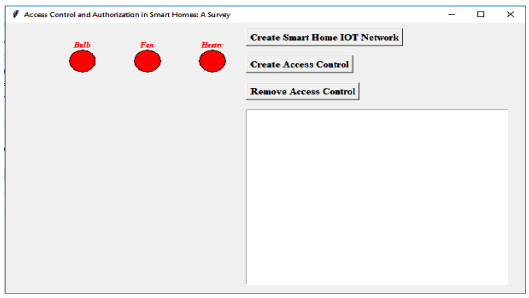


Fig1: We have three figures/circles in the upper screen, each symbolizing a light, a fan, and a heater.

Each of them are currently in the off state, therefore their color is red. Now giving bulb accesssimilarly we can add as many users as we want with access devices.

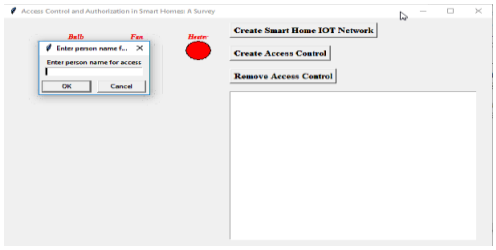


Fig2: To create access control, select the 'Create access control' option.

Now run mobile application.

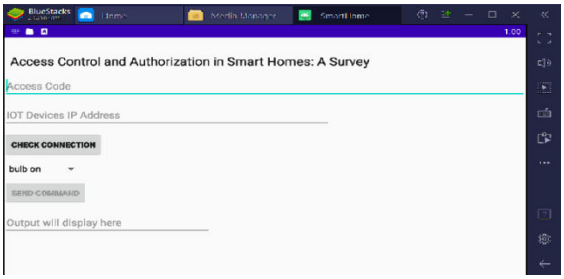


Fig3: Mobile Application

In an Android application, users must provide an access code to those to whom we have granted access.
Now we need to give IP address of python simulation application so mobile can connect to python simulation devices.
Now click on check connection button. Connection success and now select any command form drop down list.
Selecting bulb on .

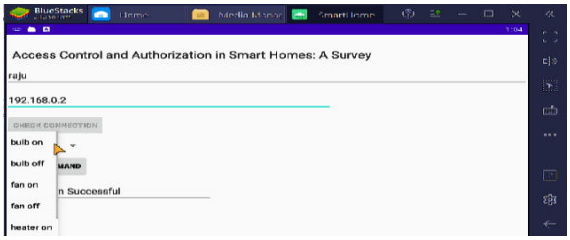


Fig4: Selecting bulb on

Now click on send command.
Bulb on command successful.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 11, Issue 1, January 2022 ||

| DOI:10.15680/IJIRSET.2022.1101012 |

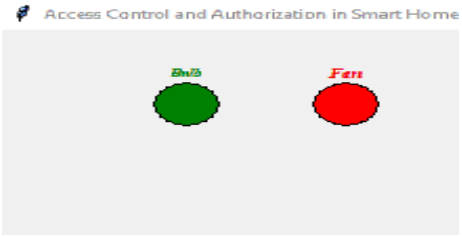


Fig5: Bulb on command successful

We haven't allowed the heater access yet. As a result, the heater is turned on and you have no access.

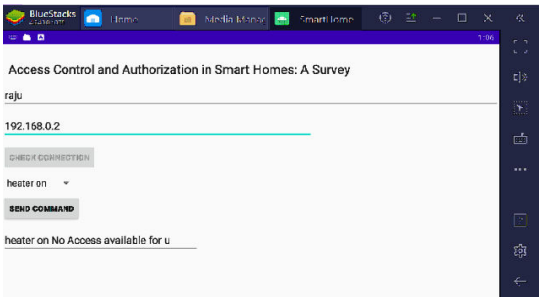


Fig6: Heater on No Access Available

ADVANTAGES

- All of your home gadgets may be controlled from one location.
- Household components may be controlled remotely.
- Increasing the amount of safety in your house.

VI. CONCLUSION

This research is being done to give an evaluation and review of existing access ownership authorization schemes for smart homes, as well as to identify the key characteristics and obstacles to be considered when developing and executing smart home security controls. This also offers a notion for the perfect access control-based authorization framework for home automation, which would address all of the present authorization framework needs and constraints. Furthermore, the frameworks will be able to handle access rights between machines (robots and other electronic objects) without the need for human interpretation

REFERENCES

[1] K. Ashton, That “Internet of Things” thing, RFID Journal,vol. 22, no. 7, pp. 97–114, 2009.
[2] H. Liu, H. S. Ning, Q. T. Mu, Y. M. Zheng, J. Zeng, L. T.Yang, R. H. Huang, and J. H. Ma, A review of the smart world, Future Generation Computer Systems, vol. 96, pp.678–691, 2019.
[3] A. K. Sikder, A. Acar, H. Aksu, A. S. Uluagac, K. Akkaya,and M. Conti, IoT-enabled smart lighting systems for smart cities, in Proc. IEEE 8th Annu. Computing and Communication Workshop and Conf (CCWC), Las Vegas,NV, USA, 2018, pp. 639–645.
[4] Y. D. Huang, Y. T. Chai, Y. Liu, and J. P. Shen, Architecture of next-generation e-commerce platform, Tsinghua Science and Technology, vol. 24, no. 1, pp. 18–29, 2019.
[5] H. S. Ning, H. Liu, J. H. Ma, L. T. Yang, Y.L. Wan, X. Z.Ye, and R. H. Huang, From internet to smart world, IEEE Access, vol. 3, pp. 1994–1999, 2015.
[6] J. H. Liu, Y. Yu, J. W. Jia, S. J. Wang, P. R. Fan,H. Z. Wang, and H. G. Zhang, Lattice-based double authentication-preventing ring signature for security and privacy in vehicular Ad-Hoc networks, Tsinghua Science and Technology, vol. 24, no. 5, pp. 575–584, 2019.
[7] A. K. Sikder, L. Babun, H. Aksu, and A. S. Uluagac, Aegis: A context-aware security framework for smarthome systems, in Proc. 35th Annu. Computer Security Applications Conf., San Juan, PR, USA, 2019, pp. 28–41.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 11, Issue 1, January 2022 ||

| DOI:10.15680/IJIRSET.2022.1101012 |

[8] B. Zhao, P. Y. Zhao, and P. R. Fan, ePUF: A lightweight double identity verification in IoT, Tsinghua Science and Technology, vol. 25, no. 5, pp. 625–635, 2020.
[9] F. Farha, H. S. Ning, S. K. Yang, J. B. Xu, W. S. Zhang,and K. K. R. Choo, Timestamp scheme to mitigate replay attacks in secure ZigBee networks, IEEE Transactions on Mobile Computing,doi:10.1109/TMC.2020.30 06905.
[10] M. C. S´anchez, J. M. C. de Gea, J. L. Fern´andez-Alem´an, J.Garceran, and A. Toval, Software vulnerabilities overview:A descriptive study, Tsinghua Science and Technology, vol.25, no. 2, pp. 270–280, 2020.
[11] L. Babun, A. K. Sikder, A. Acar, and A. S. Uluagac,IoT Dots: A digital forensics framework for smart environments, arXiv preprint arXiv:1809.00745, 2018.
[12] R. H. Weber, Internet of Things–New security and privacy challenges, Computer Law & Security Review, vol. 26, no.1, pp. 23–30, 2010.

.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.569

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details