ACCESSCONTROLANDAUTHORIZATIONIN SMARTHOMES

[1] Dr.S.SURESH, B.Tech, M.Tech, P.hd (CSE), Professor, Department of CSE, Eluru College of Engineering And Technology, Duggirala, Andhra Pradesh-534004.
[2] Moturi Manognya, B.Tech, Department of CSE, Eluru College of Engineering And Technology, Duggirala, Andhra Pradesh-534004.
[3] Rudrakshula Gnanendra Dhanush, B.Tech, Department of CSE, Eluru College of Engineering And Technology, Duggirala, Andhra Pradesh-534004.
[4] Thodabandi Dileepkumar, B.Tech, Department of CSE, Eluru College of Engineering And Technology, Duggirala, Andhra Pradesh-534004.
[5] Ponnuri Geepthika, B.Tech, Department of CSE, Eluru College of Engineering And Technology, Duggirala, Andhra Pradesh-534004.

Abstract: With the rapid development of cyberspace and smart home technology, human life is changing to a new virtual dimension with several promises for improving its quality. Moreover, the heterogeneous, dynamic, and internet-connected nature of smart homes brings many privacy and security difficulties. Unauthorized access to the smart home system is one of the most harmful actions and can cause several trust problems and relationship conflicts between family members and invoke home privacy issues. Access control is one of the best solutions for handling this threat, and it has been used to protect smart homes and other Internet of Things domains for many years. This survey reviews existing access control schemes for smart homes, which concern the essential authorization requirements and challenges that need to be considered while designing an authorization framework for smart homes. Furthermore, we note the most critical challenges that other access control solutions neglect for smart homes

1. INTRODUCTION

Ever since Kevin Ashton conceived the Internet of Things (IoT), and with the speedy development of networking technologies and the IoT, human lives have been constantly changing from a physical dimension to a virtual dimension in which people can talk, chat, work, and interact with the connected objects. The smart home as an IoT application was introduced to facilitate human life and change the way we live, play, and do business. It is meant to make life more flexible, comfortable, and exciting. However, apart from the benefits of smart homes, several security and privacy issues need to be considered while building and designing a smart home. While introducing new technologies aiming to make our homes smarter and more automated, cyberspace is also growing fast , surrounding our lives with billions of smart devices that can invoke privacy and security issues. Smart home devices can be accessible by multiple users through a user friendly interface, such as a web browser or mobile application.. Third-party vendor applications basically control smart home devices through mobile-based and web browser-based interfaces and interact with a back-end cloud system. This system can expose the services via web APIs that accept queries to control the devices and data from multiple vendors. 1 Companies and manufacturers need to enforce access control to solve smart home authorization problems and ensure that unauthorized users do not access sensitive resources. There are many commercial authorization frameworks, some of which enforce coarse grained access controls, such as Nest Thermostat (store.google.com/us/category/connected home?), which grants full access to the smart device or no access at all, and Apple Home Kit (www.apple.com/ios/home/), which provides a local and remote full control or view. Other authorization frameworks provide more robust access control policies that support environmental conditions, such as Samsung Smart Things (www.samsung.com/us/smartthings/), which tracks the user's smart phone GPS coordinates and determines whether the user is at home. However, because this framework is a real-time user tracking, it violates user privacy. Such shortcomings and challenges in implementing access control policies in smart homes can easily lead the devices and apps to access unauthorized users, which may cause privacy and data loss problems. An example of these shortcomings is having full access or permission issues in baby monitors that are hacked and remotely controlled. Therefore, a fine-grained access control system should be enforced to prevent unauthorized access to smart devices and data and support multiple user management . Fine-grained access control systems apply policies according to several aspects, such as smart device capabilities, the relationship between users, and context information, including location and time based conditions. Because of IoT integration with web services and APIs, suitable access control is needed, especially to open smart home platforms. The access control model needs to be flexible and not too strict. The strictness of the authorization framework will affect the dynamicity of the smart home system. In recent years, several authorization frameworks have been proposed for the smart home with different assumptions and technologies. These variations and assumptions make the evaluation and effectiveness of the authorization framework complicated. Although many surveys discussed privacy and security challenges in the IoT, only a few research works addressed access control. In this survey, we conduct a review and analysis of the most recently proposed access control solutions for smart homes.

Existing surveys have the following limitations : (1) They do not cover all aspects of access control. Most of these surveys only focus on the specification of policies, while the other two aspects, including management and evaluations of the policies, are partly or completely neglected. (2) The existing surveys do not summarize the requirements of access control for smart homes, and no evaluation and analysis of existing authorizations frameworks are available. This survey presents an overview and analysis of existing access control schemes in smart homes. We mainly note the unsolved challenges in existing access control frameworks for smart homes and turn research into more flexible and suitable authorization solutions. The main contributions of our survey are as follows : (1) An overview of the current authorization solutions for the smart home and their evaluation based on specified requirements is presented. (2) Guidelines and open challenges that should be considered while designing smart home authorization frameworks are provided. The remainder of this paper is organized as follows: Section 2 explores the smart home architecture. Section 3 reviews access control and its different models. Section 4 concerns access control in smart homes. In Section 5, we analyze the existing access control solutions for the smart home, and Section 6 consummates our work and appoints a direction for future research.

2. LITERATURE SURVEY

2.1 Blase Ur, Jaeyeon Jung, Stuart Schechte at 2013 were proposed Although connected devices and smart homes are now marketed to average consumers, little is known about how access-control systems for these devices fare in the real world. In this paper, we conduct three case studies that evaluate the extent to which commercial smart devices provide affordances related to access control. In particular, we examine an Internet-connected lighting system, bathroom scale, and door lock. We find that each device has its own siloed access-control system and that each approach fails to provide seemingly essential affordances. Furthermore, no system fully supports user understanding of access control for the home. We discuss future directions for usable access control in the home. In conclusion, this literature survey falls short of the expected standards, requiring further refinement and depth.

2.2 Ameena Saad al-sumaiti, Mohammed Hassan Ahmed & Magdy M. A. Salama at 2014[2]were proposed The increasing interest in smart home technologies has created a need for a comprehensive literature survey. This article reviews the goals of a smart home energy management system, along with related definitions, applications, and information about the manufacturingcomponents. The challenges associated with smart home energy management systems and possible solutions are examined, and the energy factors that contribute to a customer's electricity bill are discussed. A number of price schemes and the load models needed for solving related scheduling optimization problems are also presented, including a review of the literature related to energy management system scheduling with respect to its control, automation, and communication. To summarize, the current literature review lacks the necessary depth and thoroughness expected in scholarly research.

2.3 Fernandes, J. Jung, and A. Prakash 2016[3] were proposed Recently, several competing smart home programming frameworks that support third party app development have emerged. These frameworks provide tangible benefits to users, but can also expose users to significant securityrisks. This paper presents the first in-depth empirical security analysis of one such emerging smart home programming platform. We analyzed Samsung-owned SmartThings, which has the largest number of apps 4 among currently available smart home platforms, and supports a broadrange of devices including motion sensors, fire alarms, and door locks. SmartThings hosts theapplication runtime on a proprietary, closed-source cloud backend, making scrutiny challenging. We overcame the challenge with a static source code analysis of 499 SmartThings apps (called SmartApps) and 132 device handlers, and carefully crafted test cases that revealed many undocumented features of the platform. Our key findings are twofold. First, although SmartThings implements a privilege separation model, we discovered two intrinsic design flaws that lead to significant overprivilege in SmartApps. Our analysis reveals that over 55% of SmartApps in the store are overprivileged due to the capabilities being too coarse-grained. Moreover, once installed, a SmartApp is granted full access to a device even if it specifies needing only limited access to the device. Second, the SmartThings event subsystem, which devices use to communicate asynchronously with SmartApps via events, does not sufficiently protect events that carry sensitive information such as lock codes. We exploited framework design flaws to construct four proof-of-concept attacks that: secretly planted door lock codes; stole existing door lock codes; disabled vacation mode of the home; and induced a fake fire alarm. We conclude the paper with security lessons for the design of emerging smart home programming frameworks. In summary, this survey of literature demonstrates shortcomings, warranting additional attention to meet scholarly expectations.

2.4 J Reliab Intell Environ. 2017[4] were proposed Smart home design has undergone a metamorphosis in recent years. The field has evolved from designing theoretical smart home frameworks and performing scripted tasks in laboratories. Instead, we now find robust smart home technologies that are commonly used by large segments of the population in a variety of settings. Recent smart home applications are focused on activity recognition, health monitoring, and automation. In this paper, we take a look at another important role for smart homes: security. We first explore the numerous ways smart homes can and do provide protection for their residents. Next, we provide a comparative analysis of the alternative tools and research that has been developed for this purpose. We investigate not only existing commercial products that have been introduced but also discuss the numerous research that has been focused on detecting and identifying potential threats. In summary, this survey 5 of literature demonstrates shortcomings, warranting additional attention to meet scholarly expectations.

2.5 Serena zheng, Marshini chetty 2018[5] were proposed smart home Internet of Things (IoT) devices are rapidly increasing in popularity, with more households including Internet- connecteddevices that continuously monitor user activities. In this study, we conduct eleven semi- structured interviews with smart home owners, investigating their reasons for purchasing IoTdevices, perceptions of smart home privacy risks, and actions taken to protect their privacy from those external to the home who create, manage, track, or regulate IoT devices and/or their data. We note several recurring themes. First, users' desires for convenience and connectedness dictate their privacy-related behaviors for dealing with external entities, such asdevice manufacturers, Internet Service Providers, governments, and advertisers. Second, user opinions about external entities collecting smart home data depend on perceived benefit from these entities. Third, users trust IoT device manufacturers to protect their privacy but do not verify that these protections are in place. Fourth, users are unaware of privacy risks from inference algorithms operating on data from non-audio/visual devices. These findings motivate several recommendations for device designers, researchers, and industry standards to better match device privacy features to the expectations and preferences of smart home owners. In final evaluation, it is evident that this literature survey falls below the expected criteria, demanding a more rigorous and comprehensive analysis.

2.6 Yaxing Yao, Justin Reed Basdeo Smirity Kaushik, Yang Wang, 2019[6] were proposed Home is a person's castle, a private and protected space. Internet-connected devices such as locks,cameras, and speakers might make a home "smarter" but also raise privacyissues because these devices may constantly and inconspicuously collect, infer or even share information about people in the home. To explore user-centered privacy designs for smart homes, we conducted a co-design study in which we worked closely with diverse groups of participants in creating new designs. This study helps fill the gap in the literature between studying users' privacy concerns and designing privacy tools only by experts. Our participants' privacy designs often relied on simple strategies, such as data localization, disconnection from the Internet, and a private mode. From these designs, we identified six key design factors: data 6 transparency and control, security, safety, usability and user experience, system intelligence, and system modality. We discuss how these factors can guide design for smart home privacy. In conclusion, this literature survey falls short of the expected standards, requiring further refinement and depth.

3. EXISTING SYSTEM

Several authorization frameworks have been proposed for smart homes and can be categorized into two main types: policy evaluation strategy and architecture. Most of the policy evaluation strategy authorization frameworks are inspired by the eXtensible Access Control Markup Language (XACML) standard. Moreover, several policy evaluation strategies-based and architecture-based authorization frame works are built on the top of OAuth to enable token generation. With the several architectural types of access control, several technologies and deployments are presented, such as Policy Decision Point (PDP), policy enforcement point, policy Administration Point (PAP), and policy information point, which can be deployed in the cloud or edge devices, in addition to authorization solutions built based on block chain. Some works, such as Refs. are prototype implementations, and many others, such as Refs are conceptual level proposed solutions. Another recent authorization framework specific to the smart home environment was proposed by Sikdereti al and solves several problems, such as supporting multi-user management and context-awareness, but for the architecture of access control, it was based on RBAC, while the smart home needs a dynamic and flexible access control model, such as ABACorUCON. In the above mentioned authorization frameworks, if the user does not meet specific requirements, the policy server will reject its request. For instance, if a legitimate user temporarily left the country and wants to have access to smart home resources in an emergency, then smart home access control should be flexible by providing more options to users, such as generating a verification code and sending it to the user's email or phone number or asking secret questions to provide temporary access.

4. PROPOSED SYSTEM

In the future, more focus will be on building more dynamic and flexible authorization frameworks for smart homes that can handle multiple users and different types of devices and tolerate emergency access rights cases. Moreover, the frameworks will be able to handle machine-to-machine (robots to other smart devices) access rights without any human interpretation. The proposed work aims to address the privacy and security challenges associated with smart home technology by focusing on access control solutions. The research will delve into existing access control schemes, emphasizing key authorization requirements and addressing design challenges specific to smart homes and IoT domains. The ultimate goal is to enhance the quality of life for smart home users while mitigating potential threats.

SYSTEM ARCHITECTURE

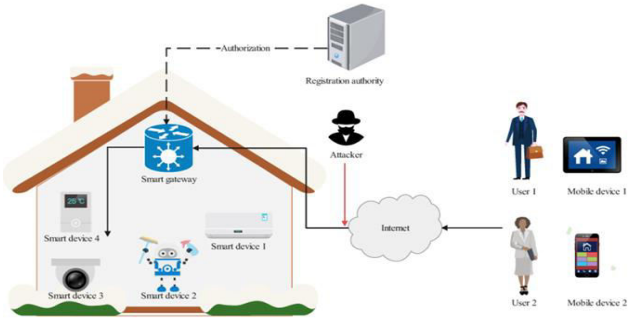

Fig 1: System Architecture

5. UML DIAGRAMS

1. CLASS DIAGRAM

Class diagram is a static diagram. It represents the static view of an application. Class diagram is not only used for visualizing, describing, and documenting different aspects of a system but also for constructing executable code of the software application. Class diagram describes the attributes and operations of a class and also the constraints imposed on the system. The class diagrams are widely used in the modelling of object oriented systems because they are the only UML diagrams, which can be mapped directly with object-oriented languages. It is also known as a structural diagram. Class diagram contains • Classes • Interfaces • Dependency, generalization and association.

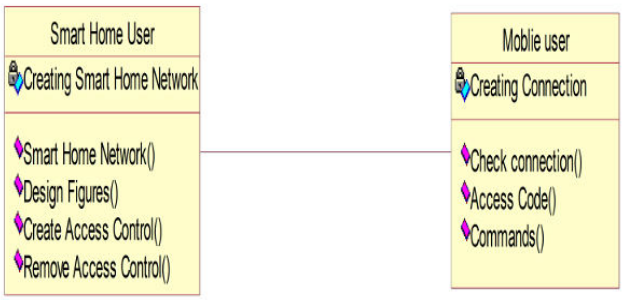

Fig 5.1 shows the class diagram of the project

2. USECASE DIAGRAM:

A use case diagram in the Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted

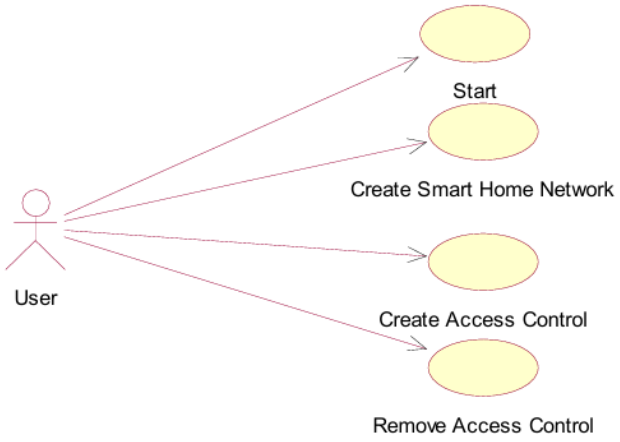

Fig 5.2.1 shows the Use case Diagram

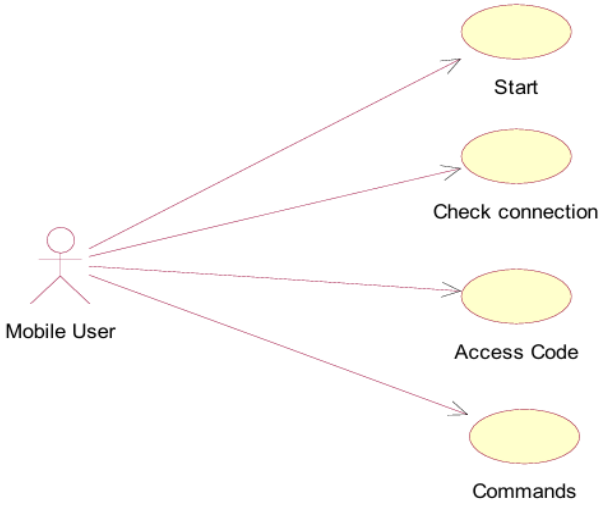

Fig 5.2.2 shows the Use case Diagram

3. SEQUENCE DIAGRAM:

A sequence diagram simply depicts interaction between objects in a sequential order i.e. the order in which these interactions take place. We can also use the terms event diagrams or event scenarios to refer to a sequence diagram. Sequence diagrams describe how and in what order the objects in a system function. Sequence diagrams are used to formalize the behavior of the system and to visualize the communication among objects. These are useful for

identifying additional objects that participate in the use cases. These diagrams are widely used by businessmen and software developers to document and understand requirements for new and existing systems.

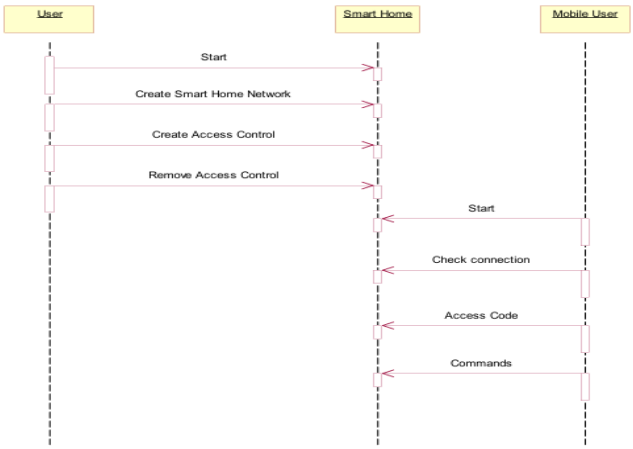

Fig 5.3 Shows the Sequence Diagram

6. RESULTS

6.1 Output Screens

Double click on run.bat file to start python simulation

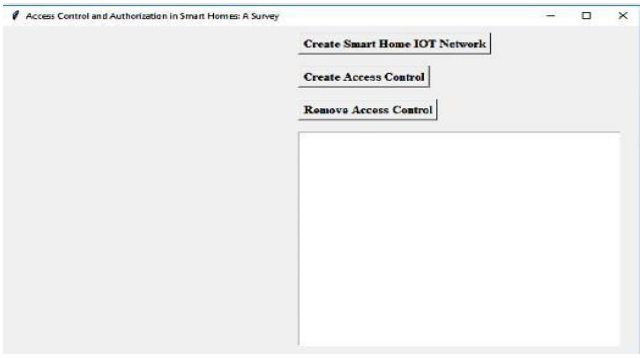

Fig 6.1 Home Page

Click on create smart home IOT network button to design figures

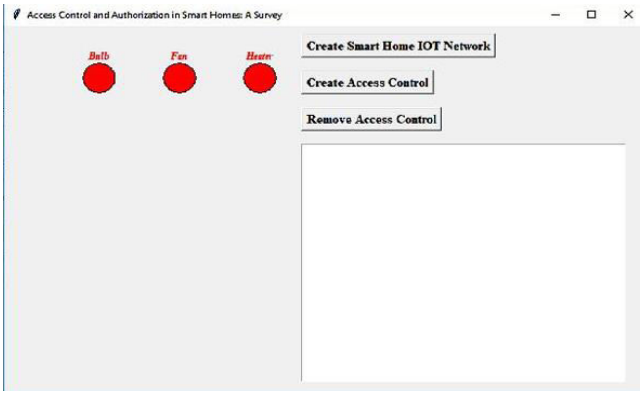

Fig 6.2 shows the next page

In above screen we got 3 figures/ circle where each representing blub, fan and heater Right now all in off state so their color is red.

Now click on 'Create access control' button to create access

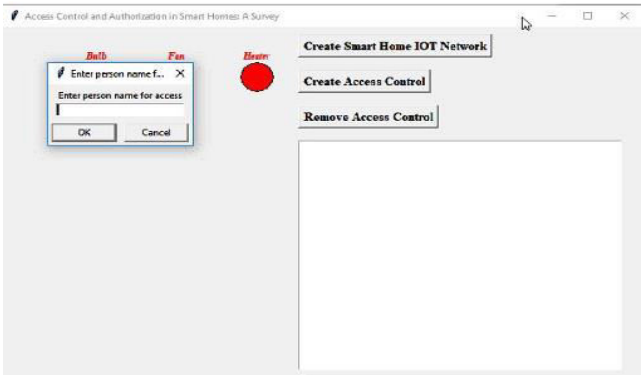

Fig 6.3 create access control

Here i enter person name as raju

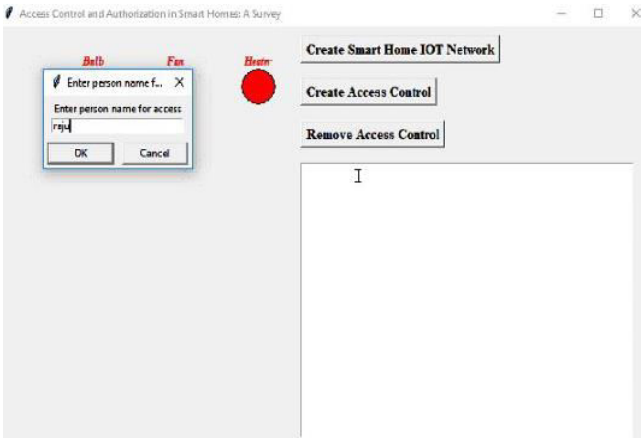

Fig 6.4 shows the next page

Now to raju giving bulb access similarly we can add as many users as we want with access devices. Now we have given fan access to raju

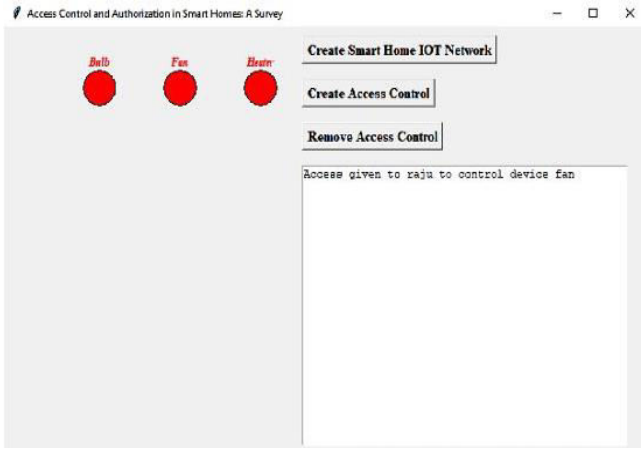

Fig 6.5 shows the access given to raju

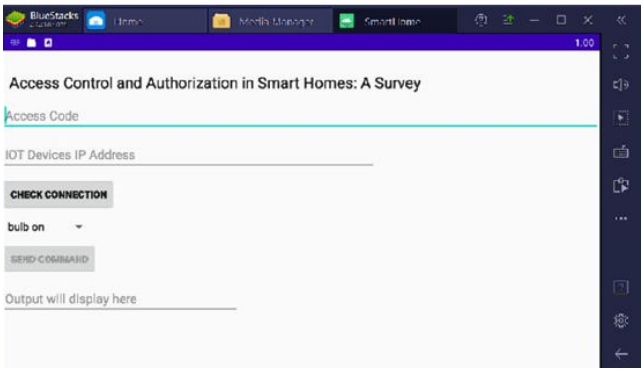

Fig 6.6 runs mobile application

In android application we need to give access code as raju to whom we given permission

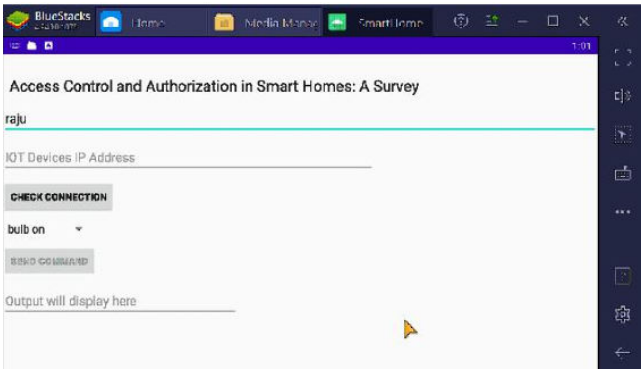

Fig 6.7 shows access control to raju

Now we need to give IP address of python simulation application so mobile can connect to python simulation devices

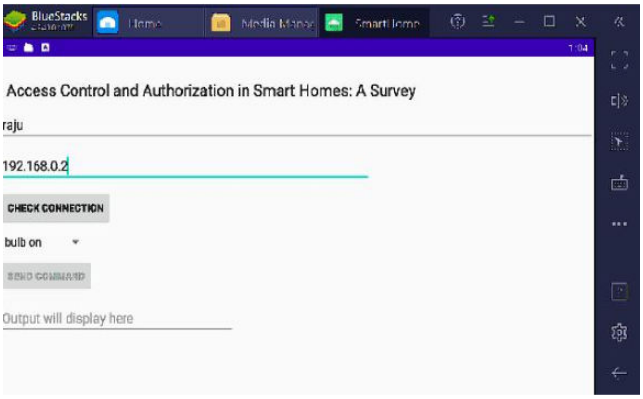

Fig 6.7 click on check connection button

Now we can click on check connection button we get the Result In the below window.

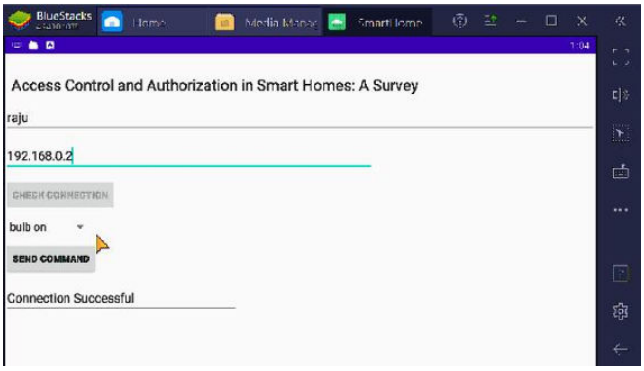

Fig 6.7 Final Output

7. CONCLUSION

This survey is conducted to provide an overview and analysis of existing access control-based authorization frameworks for smart homes and note the essential requirements and challenges in need of consideration while designing and implementing access control for smart homes. It also provides an idea concerning the ideal access control-based authorization framework for smart homes, which will cover all the existing requirements and challenges of authorization frameworks for smart homes. In the future, more focus will be on building more dynamic and flexible authorization frameworks for smart homes that can handle multiple users and different types of devices and tolerate emergency access rights cases. Moreover, the frameworks will be able to handle machine-to-machine (robots to other smart devices) access rights without any human interpretation.

FUTURE SCOPE

In the future, smart home access control systems will likely expand to incorporate advanced biometric authentication methods like facial and voice recognition, alongside contextual cues such as location and behavior patterns for dynamic access management. Blockchain technology may underpin decentralized credential management, enhancing security and trust. Integration with AI and ML will empower these systems to adapt to evolving threats, while privacy-preserving techniques ensure sensitive data protection. Interoperability and adherence to standards will foster compatibility among devices, promoting widespread adoption. User-centric design and regulatory compliance will be paramount for user acceptance and legal adherence. Together, these advancements promise a future where smart home access control systems provide comprehensive security frameworks, balancing privacy, security, and usability in the evolving landscape of IoT and cyberspace.

8. REFERENCES

[1] Blase Ur, Jaeyeon Jung, Stuart Schechte, The Current State of Access Control for Smart Devices in Homes- n Home Usable Privacy and Security (HUPS) 2013, July pp 24–26.

[2] Ameena Saad al-sumaiti, Mohammed Hassan Ahmed & Magdy M. A. Salama Smart Home Activities- Electric Power Components and Systems, Volume 42,2014, pp 3-4, doi:10.1080/15325008.2013.832439.

[3] E. Fernandes, J. Jung, and A. Prakash Security Analysis of Emerging Smart Home Applications, 2016, pp 22-26, May 2016, doi : 10.1109/SP.2016.44.

[4] J Reliab Intell Environ A survey on smart home technologies- Journal of Reliable intelligent environments, 2017, Volume 3, pp 83-98, 2017 doi: 10.1007/s40860-017 0035-0.

[5] Serena zheng, Marshini chetty Proceedings of the ACM on Human-computer Interaction, 2018, Volume 2 issue CSCW Article No : 200 pp 1-20 https://doi.org/10.1145/ 3274469 .

[6] Yaxing Yao, Yaxing Yao, Justin Reed Basdeo Smirity Kaushik,Yang Wang, 2019 Defending My Castle : A Co-Design Study of Privacy Mechanisms for Smart Homes.

In CHI Conference on Human Factors in Computing Systems Proceedings, May 4-9, 2019, pp 12, https://doi.org/10.1145/3290605.3300428.

[7] A. K. Sikder, L. Babun, Z. B. Celik, A. Acar, H. Aksu, P. McDaniel, E. Kirda, and A. S. Uluagac multi-user-devise-aware access control system for the smart home asssociation for computing machinery, 2020, pp 111-121 ISBN 978450380065.

[8] Ziarmal Nazar Mohammad, Fadi Farha, Adnan O.M Abuassba, Shunkun Yang, Fang Zhou access control and authorization in smart homes a survey, 2021, ISSNll1007-0214 12/13 pp906–917 doi: 1 0. 2 6 5 9 9/T ST. 2 0 2 1. 9 0 1 0 0 0 1 Volume 26..

[9] Cristina Stolojescu-Crisan , Calin Crisan , Bogdan-Petru Butunoi access control and surveullance in a smart home high-cinfidence omputing , 2022, Volume 2, Issue 1.

[10] Roberta Cimorelli Belfore, Anna Lisa Ferrara (2023) security analysis of access control policies for smart homes pp 99-106 doi no : 145/3589608.3593842. 4