ASHESI UNIVERSITY

PRIVACY-BY-DESIGN FOR INTERNET OF THINGS(IOT): IMPLEMENTING USER AUTONOMOUS OPTIONS IN A SMART HOME SCENARIO

CAPSTONE REPORT

B.Sc. Electrical Engineering

Joachim Edward Asare

2020

ASHESI UNIVERSITY

PRIVACY-BY-DESIGN FOR INTERNET OF THINGS(IOT): IMPLEMENTING USER AUTONOMOUS OPTIONS IN A SMART HOME SCENARIO

THESIS CAPSTONE PROJECT

Capstone Project submitted to the Department of Engineering, Ashesi University, in partial fulfilment of the requirements for the award of Bachelor of Science degree in Electrical Engineering.

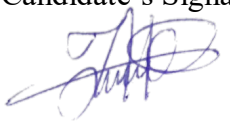
Joachim Edward Asare

2020

DECLARATION

I hereby declare that this capstone is the result of my own original work and that no part of it has been presented for another degree in this university or elsewhere.

Candidate's Signature:



Candidate's Name:

Joachim Edward Asare

Date: 11th May, 2020

I hereby declare that the preparation and presentation of this capstone were supervised in accordance with the guidelines on supervision of capstone laid down by Ashesi University.

Supervisor's Signature:

……

Supervisor's Name:

……

Date:

Acknowledgements

To all the people whose encouragement and academic advice helped me undertake this project, I would like to declare my earnest appreciation. First, I wish to express my sincere gratitude to my supervisor, Mr. Francis Gatsi, for his inspiration, guidance and direction throughout my research and writing of this thesis. His patience to review every detail of this thesis was one I could not do without.

I also wish to show my gratitude to Ashesi University for the opportunity given me to have an impactful undergraduate engineering study. Not forgetting the amazing Engineering Department faculty whose feedback were instrumental in discovering flaws as well as areas to develop upon in this work. Lastly, I wish to thank all my classmates of the 2020 Engineering Class for being very contributive towards this project.

Abstract

In traditional Internet of Things (IoT) systems, users are unable to authorize and/or deauthorize the collection of user data. Hence, the problem of the absence of user autonomy in IoT systems. The project aims to tackle this problem by suggesting a human-centered privacy-by-design option in the design and implementation of IoT systems. It aims to prioritize the need for the privacy of the user in designing IoT systems. It proposes to do this through the provision of user autonomous commands that enable the user to opt out of the collection of a particular data type and restore the collection of that data type at will. A Smart Home was built and designed, as the IoT system, for the proof of concept. Various data types were collected at the edge level and three of them (audio, image and temperature) were selected to be transmitted to a remote NoSQL database. Through the user web application, the user was able to authorize and/or deauthorize the transmission of data types by choice. In addition, the user was given access to view a user-friendly presentation of the cloud database, to validate the execution of their autonomous actions taken. This was demonstrated in several use case scenarios. The results shown from this research illustrate that user autonomous actions for privacy can successfully be implemented in the design of IoT systems.

Table of Contents

Table of Figures

List of Tables

Chapter 1: Introduction

Internet of Things (IoT) forms a major part of the evolution of the internet age in the 21st Century. The first usage of the term was by Kevin Ashton during a presentation on the introduction of Radio Frequency Identifier (RFID) in 1999 [1]. Since then, the term has been adopted and modified to describe a breakthrough in data collection, data processing and connectivity. IoT describes an interconnection of physical objects including sensors, mechanical and digital machines, objects and people to transfer, receive and process data over a network. There are four major components of a complete IoT system: sensor devices, network connectivity, data processing and a user interface.

IoT systems have a wide range of applications. For example, there are IoT applications adopted in transportation systems. Products such as 'Dash' or 'The Automatic app' use an in-car adapter connected to sensors to collect data such as mileage, fuel cost, efficiency, GPS location, hours driven and ignition [2]. This allows the driver to receive real-time information from the vehicle. In most cases, this data is processed to perform some form of automated output such as providing tips for fuel efficiency based on the data collected. Now, delivery firms can offer their clients real-time tracking of their deliveries. Here, a location sensor or tracker is attached to the products; real-time data of the products' precise location is collected and processed over a network such as the internet; and clients can monitor the movement of their goods via a user application interface. IoT systems led to the conception and innovation of smart homes. Today, one can control lighting and other home appliances while away from home with the help of IoT systems. It interconnects objects at home via a network and allow for automation. A simple smart home system can include a fire or smoke detector that detects fire and automatically calls the local Fire service to the precise location of the fire and/or turns on overhead fire sprinklers to quench the fire

without human intervention. In this smart home, the fire detector, telephone and sprinklers have been given a communication platform to perform specific tasks depending on data collected. This data is processed by the fire detector device in a digital system design with logic to control connected devices to the network.

Based on the above applications, advantages of IoTs are conspicuous. IoT systems are undeniably taking a forefront in the advancement of people, mechanical and digital machines, computing devices and objects [3]. Internet of Things enables industries to automate processes and reduce cost of human labor. It enables greater quality and more efficient Machine to Machine (M2M) communication. In cases where physical objects are connected and automated over a wireless network without human intervention, time is significantly saved and hence, productivity is improved. Also, through real-time collection and storage of data, such as with a video surveillance IoT system, monitoring is highly improved as compared to systems where humans are needed to do same. Furthermore, energy and money are saved as well. For example, embedding IoT in a power system would lead to the judicious use of electrical power and hence, less energy cost. Indeed, the merits of IoT are enormous and extend across all sectors (energy, transportation, healthcare, finance etc.) [4].

On the other hand, as any emerging major technological advancement, there are crucial challenges that IoT systems currently face. These challenges can be classified into four broad areas: compatibility, complexity, naming and identity management, and privacy and security [5]. With the absence of a standardized IoT system, most manufacturers provide their own network or hardware technological preferences. This usually results in incompatible integrations with other IoT systems. There is the need for IoT interoperability and universal standardization for all IoT elements. Moreover, designing IoT systems are sometimes complex due to the connection of a

myriad of diverse objects over a complex network. Some sensor devices may, by default, have bugs in their firmware that need to be explored and corrected. In applications where automation is made, precision and accuracy are sometimes difficult to achieve through computer programming [5]. In addition, effective naming and identity management systems in IoT systems have also been a challenge [6]. With the increasing number of objects or elements in a system, such management systems are required to dynamically assign and manage a unique identity to each element.

Privacy and Security have been the most alarming challenge in recent times. There have been several concerns for IoT privacy and security in recent years. For example, in March 2018, a woman in Portland complained that her Amazon Echo (IoT product component for smart homes) recorded her conversations and sent them to a random contact without her request [7]. This is a total invasion of privacy. Also, this year (2020), The Washington Post published an article that lamented that companies such as Amazon and Google used their IoT devices to collect data from users without their authorization [8].

Sadly, IoT systems are also prone to network intruders due to their vulnerability in network design. Most IoT do not adhere to security standards due to the absence of no problem regulation in their development. Furthermore, for most IoT systems, the storage devices used are memory cards and these cannot store large amount of data [9]. Hence, most data are stored on remote sites and this requires a high-level security and privacy as they can be hacked.

Paramount in the challenge of privacy and security is the absence of user autonomy. IoT systems are highly focused on the systems automation and rather fail to include user autonomy to regulate and control data that is collected over the IoT network. In the case of privacy or security intrusion, the user has no opportunity to access and control data transferred over the system. For example, in the report by the Washington Post, the user's Amazon echo had a wide range of tasks

besides collection of audio data. In her case, she is unable to turn off only the audio recording feature and may have to resort to disconnecting the entire system, which is very inconvenient to the entire smart house system. Currently, there is little or no control by a user over the collection and transmission of user data over an IOT system [10]. In the case of privacy invasion or anticipated privacy invasion, there is no user autonomy control session the IoT application to interrupt data collection and restore the data collection at will [10]. The aim of this capstone project is to attempt addressing this particular problem by developing a smart home IoT-based system that gives the user some control over which type of data is collected at any moment as preferred.

Chapter 2: Literature Review

This capstone project is concerned with the problem of the absence of user autonomy in IoT systems. It would go on to develop a proof of concept on the development of design options for a human/user-centered Design for IOT privacy. The problem investigated, can be categorized under the Privacy and Security challenges of IoT. Privacy and Security is rather a broad area in the field of Internet of Things and hence, there is the need to specify the aspects that would be focused on. These consist of Data Privacy, Information Consent and the Ethical challenges.

There have been many publications on the privacy and security of Internet of Things. However, there has been very little work done on the challenge of Data Privacy and the need for the implementation of user autonomy in IoT systems. This chapter goes on to show, investigate and analyze literature publications on IoT privacy and security on a whole. It would then focus on literature publications that addressed the challenges of Data Privacy in IoT, the methodologies used, and the gaps in these research works.

2.1 Existing and supporting legislations

Data Privacy and Data Security are strongly related, however, there is a distinct difference between them. Data privacy is concerned with the authorization of the data collected and how it is defined and used [11]. It simply refers to the ethical and appropriate use of data. On the other hand, Data security is the implementation of policies, physical and logical frameworks to protect the data from unauthorized access, loss and corruption of sensitive data [12].

According to the Data Protection Commission (DPC), Data Protection is the legal protection of personal data [13]. For example, the Data Protection Act, 2012 (Act 843), of the Constitution of Ghana outlines the rights and obligations of individuals and organizations regarding the

collection, disclosure and care for personal data [14]. Though the Act does not explicitly provide regulation for IoT data privacy, its definition of personal data captures IoT data. It covers all data such as images, videos, audio and location of individuals and groups [15]. A session of the law that lists the Individual Rights to data protection, strongly insist and validate user autonomy as a requirement in IoT systems. Those relevant to user autonomy include: access to personal information collected; right to amend personal information; right to prevent processing of personal information; right to freedom from automated decision making; right to prevent processing of personal data for direct marketing purpose [16]. There are also international laws such as the General Data Protection Regulation of the European Union, Global Data Privacy Law and the International Data Privacy Law that supports the mentioned rights [17]. Current IoT systems are unable to meet these Privacy rights due to the absence of user autonomy.

2.2 Relevant publications

In the paper, 'IoT Security, Safety, Privacy and Ethics', Hany and Gary [18] discuss IoT security and privacy challenges. It highlights privacy and security threats and the need to implement ethical design in IoT systems (smart cities were used as a case study). The paper discussed the problem of privacy by classifying privacy threats under six categories: Identification, Location and Tracking, Profiling, Life-cycle Transition, Inventory Attack and Linkage. This was very informative as this approach clearly and broadly highlighted the various aspects to consider when ensuring privacy.

Identification and Location and Tracking threats would be further explored since they were most relevant to this capstone report. Identification was defined as the threat posed by associating an identifier with the private data of a user. The IoT system allows sensor devices to collect various types of data about a user and his interaction with the environment. These data are processed by

third-party administrators and hence are outside of the user's control [19]. This identification threat is mostly exploited by the third-party administrators by analyzing customer behavior and selling user data to companies for marketing. Also, in case of breaches in security such as an unauthorized access to the data collected, personal information (name, address etc.) can be accessed since identifiers are related to users. The authors of this publication recommend that attribute-based authentication is used to minimize the disclosure of data. This method allows users to be authenticated anonymously and protect their privacy.

Though this paper gave some good recommendations regarding data privacy threats, there were no experiments conducted to validate their efficiency. There was the need to include supporting evidence from a proof of concept. The suggestions are thus, open for debate. In addition, some recommendations were generalized. For example, Privacy by design was stated as a suggested Privacy-Preserving solution for IoT systems. However, the elaboration made on this failed to give a specific design approach that can be followed, implemented and outcomes measured. It merely stated IoT users should have required features that allows them to control their data.

The article informs the need for an efficient solution that tackles potential sources of privacy threats. Solutions recommended for data privacy threats summed up the need to introduce user autonomy in IoT systems. Further, this capstone project aims to meet the mentioned gaps, by providing specific privacy by design options, selecting one to be implemented and measuring the IoT system's performance after embedding that selected design option.

'Ethical Design in the Internet of Things' was an article published in the Science and Engineering Ethics journal in 2016. Its content provides an innovative approach for users to interact with IoT systems, based on the concept of Ethical Design [20]. It demonstrates the need to grant users with a more active role to address the issue of data protection and privacy.

Ethical Design is explained in this paper as IoT devices and applications designed and deployed to give users autonomy in controlling and protecting their personal data that is collected and processed over an IoT system [21]. The paper defends that users should be allowed to freely regulate, authorize or restrict the data collection in real time. It refers to these user features as ethical choices. Their research argues that business that include ethical values in their products would benefit as consumers are more willing to buy devices that would protect their data and ensure their privacy. This is meant to rebut companies that infringe on data privacy rights to make some financial gains by selling consumer personal data to other companies [22]. Ethical Design creates a new target market niche of individuals who do only benefit from the convenience of IoT but also, the trust that they have some power over their data or information.

In addition, the article highlighted the challenges and processes involved in implementing Ethical Design in IoT. It went on to discuss how these challenges can be solved. Unlike the previous publication, the research was validated by a proof of concept to demonstrate the implementation of ethical design in IoT. This was demonstrated in a separate publication, 'SecKit: A model-based security toolkit for the internet of things' [23]. In it, the Model-based Security Toolkit (SecKit), a policy-based framework software was designed to empower users to regulate personal data collected. It was developed to have a user interface that allowed users to interact with elements on the IoT network such as enabling and disabling the collection of data by some sensors.

The inclusion of a proof of concept was one of the main strengths of the paper as it validated the opportunity to implement Ethical Design in IoT systems to ensure data privacy and protection. However, there were a few weaknesses to this initiative. To begin with, the software interface of SecKit was not quite user friendly. However, there were a few weaknesses to this initiative. To

begin with, the software interface of SecKit was not quite user friendly. It can only be used by an expert in the IoT field. Specific users who do not have much knowledge regarding IoT systems technicalities would relatively find it difficult to navigate through and execute commands. A screenshot of the SecKit user interface is shown in Fig. 1 below. Moreover, the article was not able to quantitatively or qualitatively show how much data privacy and implementation has been added to the IoT. It was obvious that some data privacy and protection was included in the Ethical Design, however, the extent of its impact on this system was not given. This measurement can be made and has been proven by some other researchers [24].

Ethical Design is spearheaded by the inclusion of user autonomy in Internet of Things. The proof of concept implemented in it is similar to that of this capstone project. However, the capstone project proses to meet the gaps highlighted above in addition to other functionalities.

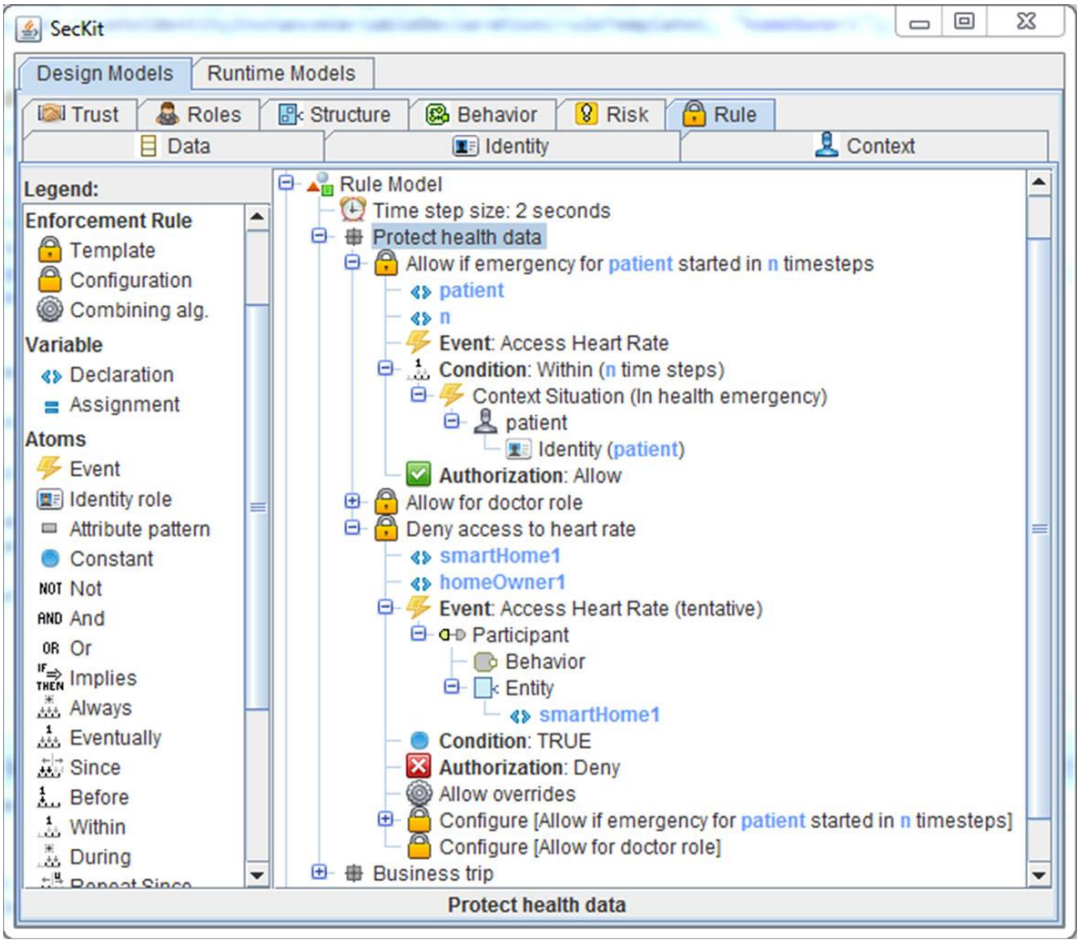


Fig.1 SecKit User Interface

Ukil, Bandyopadhyay and Pal [25] introduce the concept, Privacy Preserving Data Mining (PPDM) in this literature. PPDM was used in this paper to show how privacy breaching attacks in the development and deployment of Internet of Things can be reduced. The objective of the paper was to develop strong sensitivity detection, analysis and privacy quantification. Real sensor data was to show and quantify performance of a data privacy management method.

There were three components in the methodology employed in their work – privacy measurement, statistical compensation, privacy quantification and privacy decision. The methodology involves developing a scheme from theoretical expectations made with appropriate

assumptions. Then, sensor data are collected and interpreted into some statistical measurement. The paper was very straightforward as it went directly ahead to demonstrate how privacy can be measured. On the other hand, this straightforward approach made the paper too succinct to be understood as little explanation was given at each stage. Also, the paper appeared very technical and can only be properly interpreted by experts in the field of statistics. IoT engineers are experts who are meant to be the target audience would most probably be unfamiliar with the statistical approaches used. Hence, it makes it relatively difficult to emulate the work done.

Chapter 3: Design

3.1 Introduction

The aim of this project is to design a Privacy-by-design option to implement user autonomy in IoT Systems. To do this, a proof of concept would be developed where a typical IoT System would be embedded with a user and administrator software that allows users to exhibit some level of autonomy over the collection, analysis and transmission of their data over an IoT network. To successfully demonstrate this, there are systematic design approaches that were developed to be followed. The Design Thinking approach and Privacy-by Design Principles are incorporated in this design as the nature of the subject of this capstone research strongly requires these. This chapter explores the design phases, requirements and specifications.

3.2 Product Description

The final product system consists of a miniature smart home IoT system modeled with some sensor and data collection devices, a cloud database, where data is transmitted over a network and the software interface. The software interface would be the point of focus as the user software is supposed to provide the user with autonomy over his data collected. The block diagram interconnection of the system is shown in Fig 3.1 below.

3.3 Design Decisions

The design decision phase was categorized in three milestones: IoT System choice, Sensor devices and network choice, Software interface.

3.3.1 IoT System Choice

There was the need to select a specific type of IoT System that best demonstrates user autonomy. In this case, data should be collected from severally interconnected data inputs and transmitted unto a cloud database. Notable to the selection is a user software and administrator software system that can successfully interact with the sensor devices and mode of communication. The proof-of-concept of this capstone project proposed to illustrate a scenario where the data owner can choose to opt of one of the various types of data collected without interrupting the collection of other data and the entire operation of the system. Based on this scenario a Smart Home System, Smart Vehicle IoT System and Smart Health IoT System were considered and a choice was made on one. For example, in the smart vehicle system, where data such as acceleration, fuel level and GPS location are being collected, the user may wish to deauthorize the collection of location data due to privacy reasons. It is such scenarios that led to the choice of these three IoT System Options. A Pugh chart was used to make the final selection of the IoT system to be used.

Table 3.1 Pugh Chart for IoT system Selection

	Baseline	Weight	A	B	C
Criteria	General Purpose IoT System		Smart Home IoT System	Smart Vehicle IoT System	Smart Health IoT System
Relevance to Project Aim	0	5	+4	+4	+4
Simplicity in Construction	0	4	0	-2	0
Ease of access to Components	0	3	+1	-1	-1
Time to construct	0	3	0	-1	0
		Total	+5	0	+2

The criteria used for selection were the relevance to the aim of the capstone project, simplicity with regards to design construction, ease of access to components required and the time frame to be used for constructed. As shown in Pugh chart above, **the Smart Home IoT System** was selected to be used for the proof of concept.

3.3.2 Mode of Communication Decision:

The network choice as a mode of communication was another crucial component. For the transmission of data to be later sent unto an online database a mode of communication is needed. Examples used in IoT systems include, WiFi, Bluetooth, Zigbee and Cellular.

The criteria used for the mode of communication decision include power consumption, compatibility with wide range of sensor devices that would be used, availability of the technology, and communication range. A Pugh Chart was applied to make to show how the decision was made.

Table 3.2 Pugh Chart for Mode of Communication Decision

	Baseline	Weight	A	B	C
Criteria	Cellular		ZigBee	WiFi	Bluetooth
Versatility with wide range of sensor devices chosen	0	5	+3	+3	+1
Availability	0	3	+1	+2	+3
Data rate	0	2	0	0	-1
Communication range	0	2	+2	0	+1
Power Consumption	0	3	+2	-2	0
Cost	0	2	+1	-1	+2
Smart Phone integration	0	3	0	+3	+1
		Total	9	5	8

From the above the choice made was Zigbee at edge level. Moreover, it is widely used for smart home integration.

3.3.3 Device for collection and processing Decision

For the collection, control and processing of data a microcontroller or device with a microcontroller was needed. The decision was between Raspberry Pi 3, Arduino and NodeMCU (ESP8266) due to their ready availability and suitability for educational purposes. A pugh chart is shown below to select the most appropriate device for the research work.

Table 3.3 Pugh Chart for Mode of Communication Decision

	Baseline	Weight	A	B	C
Criteria	MSP430 Launchpad		Raspberry Pi 3	Arduino	NodeMCU (ESP8266)
Processing Speed	0	5	+5	+2	+3
Programming language suitability for automation	0	4	+4	+3	+3
Memory size for program/code file storage	0	3	+3	0	+1
Availability of Internet Gateway without external hardware	0	4	+5	0	+5
Power Consumption	0	4	+2	+4	+4
		Total	19	9	16

3.3.4 Sensor Devices Decision

The decision for sensor devices that would be used was dependent on the IoT system chosen and Communication mode being employed. Hence, upon making both decisions, it was relatively easier. The inputs include surveillance camera, audio input (baby alarm), a digital thermostat that works with a heater/cooler and the state of open and closed automated doors and windows.

3.3.5 Database Decision:

The decision for the choice of database to be used in this research work was between a structured (MySQL) and non-structured database (MongoDB). MySQL first appears to be a good choice as tables can be easily used to organize the data collected in table easy reference. However, the NoSQL database, MongDB supports both structured and unstructured data types unlike MySQL which supports only structured data. This project makes use of unstructured data

comprising of image and audio data. Hence, there is the need to employ a database that can accommodate these variety of data. In addition, MongoDB serves as a more ideal

3.3.6 Software Interface Design:

A web application was decided to be used over a mobile app application due to the cross-platform advantages it has over a mobile application. A web application would successfully run on any computer or mobile device irrespective of the operating system it works on. However, the mobile app would have to be designed to fit several distinct operating systems such as making one for Google's Android OS and another for Apple's IOS.

Although, this thesis is focused mainly on the user interface (as user autonomy session is to be included), there was the decision to include an administrator interface. In a typical scenario, it is important for the administrator to receive a feedback when the user performs an autonomous action. When this is not established, it would be difficult to differentiate between an anomaly in network data due to a technical or functional fault in the IoT system.

Hence, Administrator software interface was designed to show the following:

i. All sensors and whether they are running or not
ii. A notification session that shows that a user has made an autonomous
iii. A data analytics session that displays a graph of the rate of transmission of data across the network.

3.4 Illustration for design arrangement.

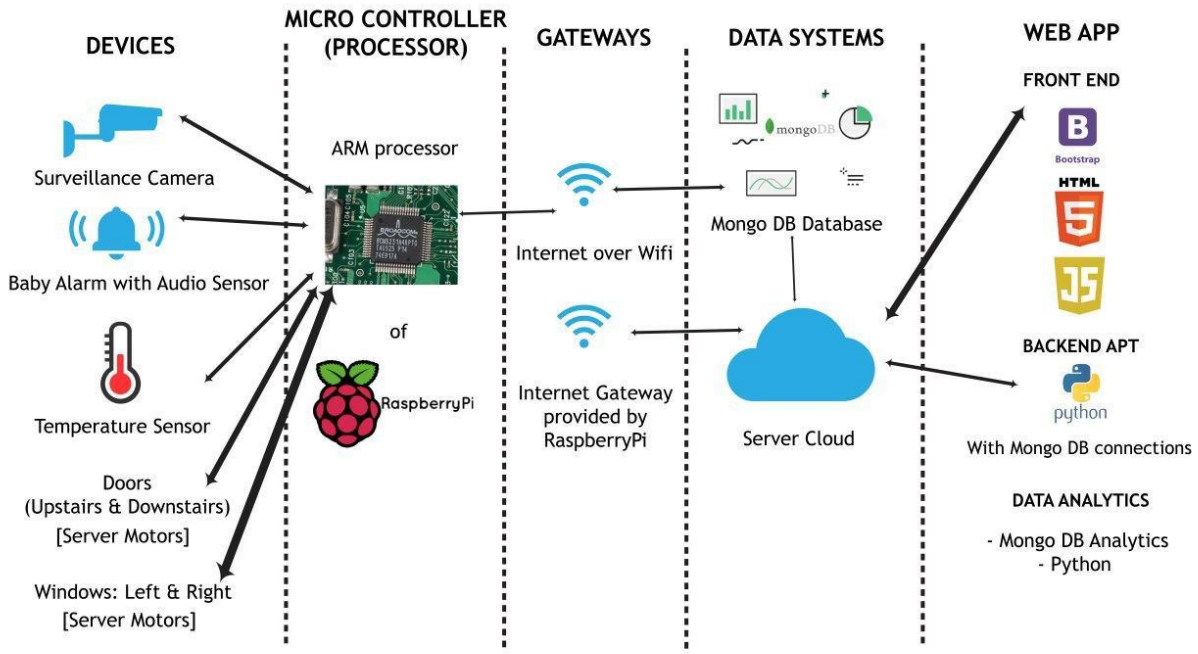


Figure 3.1 showing illustration of Smart Home System with User Autonomy Implementation

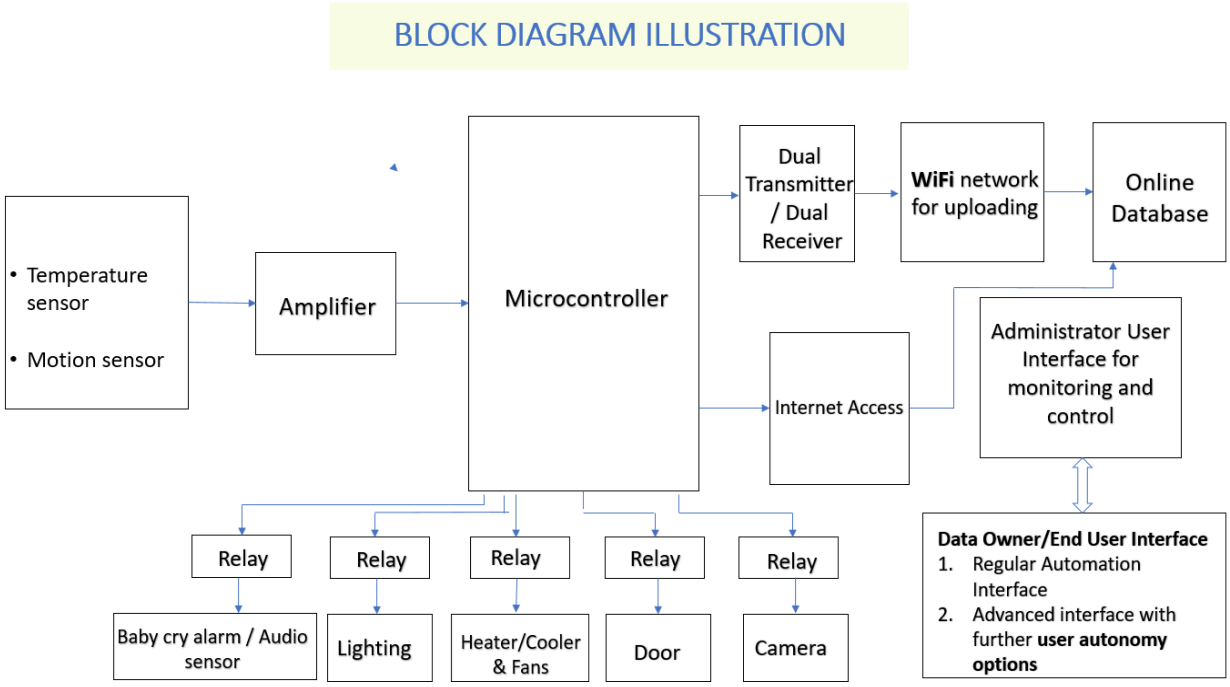


Figure 3.2 Block Diagram illustration of Smart Home System to be built

3.5 Design Requirement

Design Requirements were made to ensure design meets the aim of the capstone project satisfactorily. These requirements guided the entire implementation of the proof of concept. They are categorized into user and system requirements.

3.5.1 User Requirements:

The user must have a user-friendly interface over which he can:

- View the various Input devices on the IoT System
- View data being transmitted in real time over the IoT System's mode of communication
- Authorize the transmission of a specific type or group of data
- Deauthorize the transmission of a specific type or group of data
- View Data types for a sensor input that has been authorized or deauthorized
- Receive feedback on the performance in any sensor hardware input or network transmission, including error or fault repairs

3.5.2 System Requirements:

The table below describes the functional/technical requirements of the IoT System (input and sensor devices, network system, database system, user and administrator application software)

Table 3.4: Table of the technical requirements of the system

System Requirements	**Justification**
1 Responsiveness	User and Administrator Software interface should have the least delay as possible when a command is selected
2 Feedback	A feedback should be sent to the administrator software interface when the user authorizes or deauthorizes the transmission of data.
3 Sensitivity	Network must be very sensitivity to signals Sensor devices must be satisfactorily sensitive to collect data signals as input
4 Selectivity	User interface must present user with options to select from.
5 Accuracy	The accuracy of the system should be about 0.99.
6 Power Consumption	The system consumes minimal power hence communication and senor devices must be low-powered.

Chapter 4: Methodology

4.0 Overview

To illustrate the possibility of the inclusion of user autonomy in an IoT system, a methodology was developed and followed. A typical IoT system was chosen to meet the requirements of this objective. In this case, a Smart Home IoT scenario was chosen. Data types were chosen to be collected. Hence, a miniature Smart Home IoT system model was built. The reference model was designed, mechanical housing and framework was built, then electrical and electronic connections were made. Next, a database was created to store relevant data and data was collected and sent over the internet to the database. Most importantly, a user and administrator user interface were made, and user autonomous actions were added to the user interface. The successful implementation of user options to opt out of the collection of a data type and/or restore would be an affirmative answer to the research question of this thesis. This chapter goes on to explain the methodology involved in the proof of concept. These steps were executed under the following steps:

4.1 Smart Home Construction

4.1.1 Mechanical Framework Design and build

The concept of a miniature smart home IoT system was developed and designed using 'AutoDesk Revit' software as shown in figures 4.1 and 4.2 below. A typical home size was designed and scaled down by a factor of 689.94. Building plan drawings were made and implementation were made based on these design plans. The implementation of this framework was made using wood and plexiglass. The choice of plexiglass was used to wall the rooms of the home due to its transparent properties. This would allow visibility of the operating interior

components such as the sensors in the home. In addition, the durability, low cost, strength and of wood influenced it as the choice for the major framework of the smart home. Lastly, a cuboidal compartment was construction behind the Smart Home as an extension of the house to accommodate and conceal the major electrical and electronic components (Raspberry Pi microcontroller and power supply).

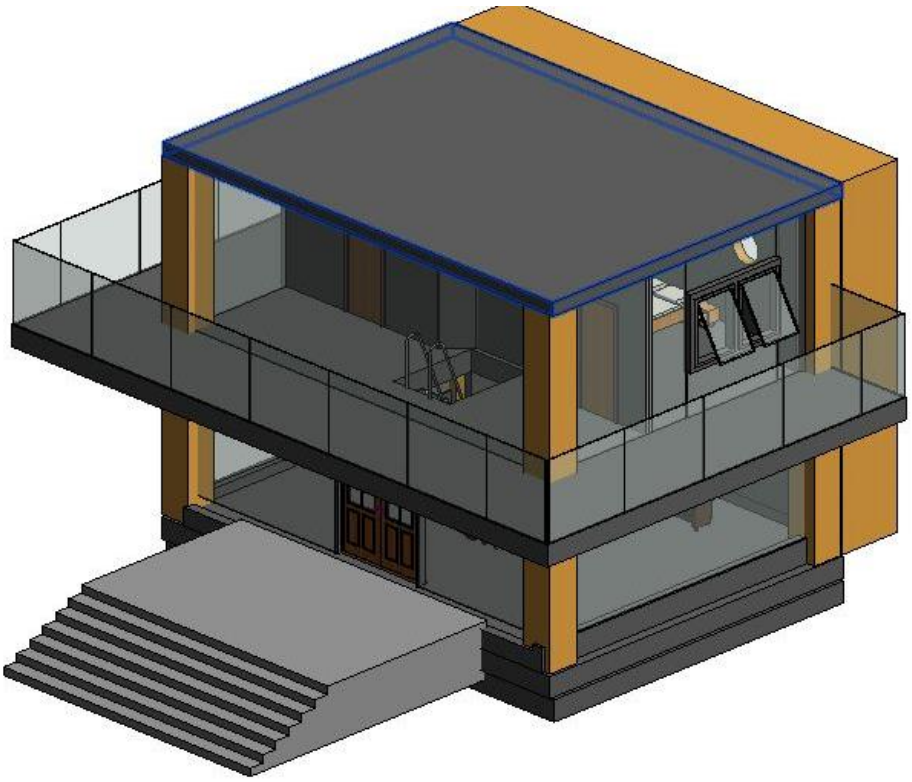


Figure 4.1 Side View of AutoDesk Revit Sketch of Smart Home

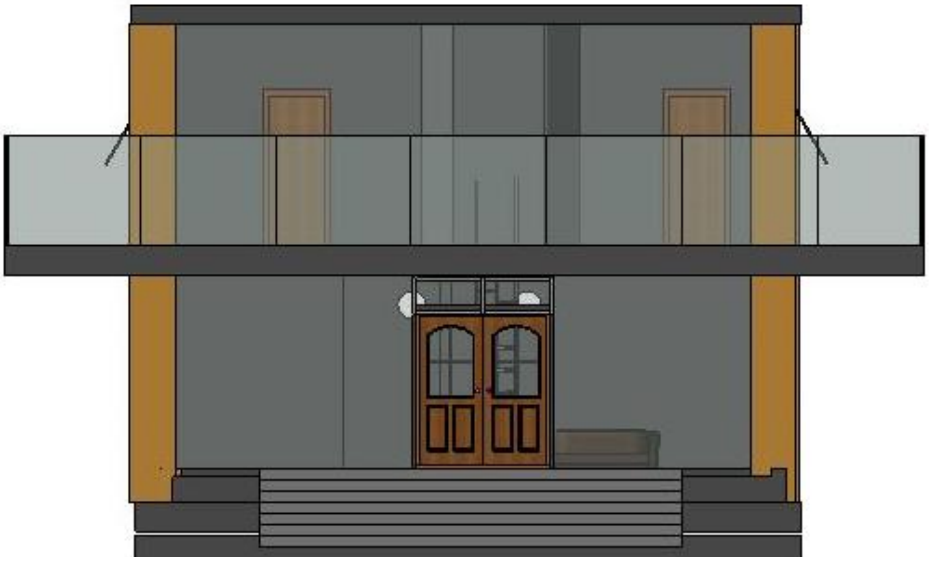


Figure 4.2 Front View of Smart Home AutoDesk Revit Design

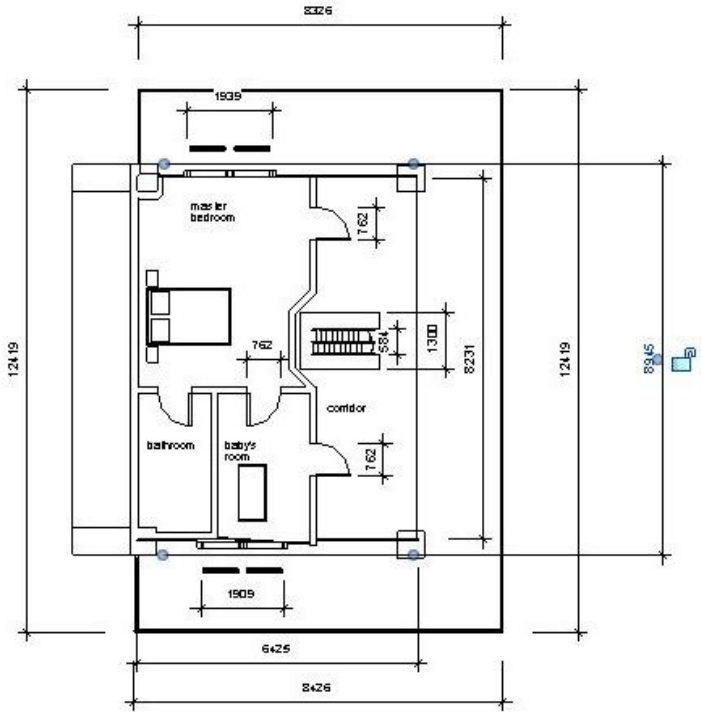


Figure 4.3 Smart Home Plan

Figure 4.4 Implementation of Mechanical Design

4.1.2 Electrical, electronics and sensor set up

Based on the choice data to be collected and used to demonstrate the privacy-by-design proof of concept, an electrical and electronic design was made. This electrical and electronic design was made to set up the sensors to be controlled by a microcontroller (in this case a Raspberry Pi) to collect relevant data from the smart home.

First, a schematic circuit diagram was drawn using Proteus software tool as show in Fig. 4.3. Based on this sketch the circuit was build. Servo motors were used for the automation of the doors and windows, an audio sensor and a buzzer, for a baby alarm by detecting baby cry (audio) and sounding an alarm. In addition, a surveillance camera that takes image data was set up by connecting a Raspberry Pi camera to the raspberry pi module. The final circuit assembly is shown in Figure 4.5 below.

The power requirements for this set up was 9V DC to the Raspberry Pi and 5V-6V DC to the sensors. A 220V/240V AC – 12 DV supply was connected to the Raspberry pi and the 5V-6V pin of the raspberry pi was connected to the sensors.

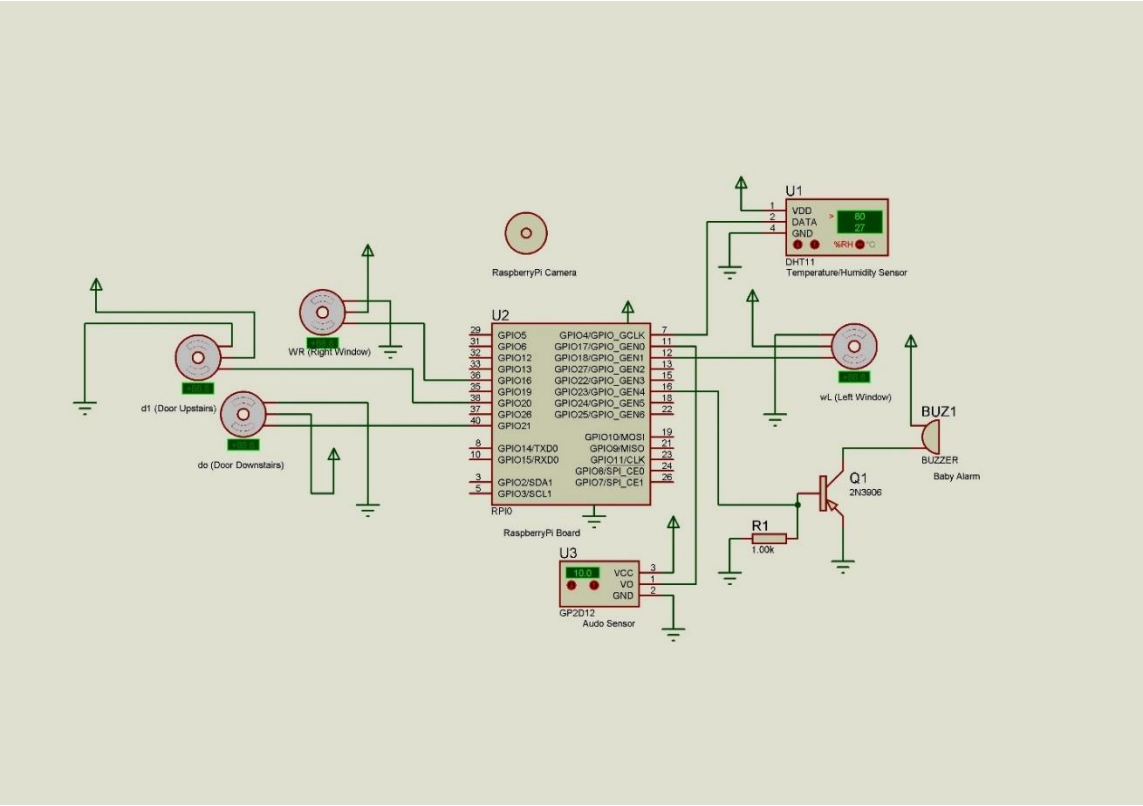


Figure 4.5 Schematic Diagram designed with Proteus

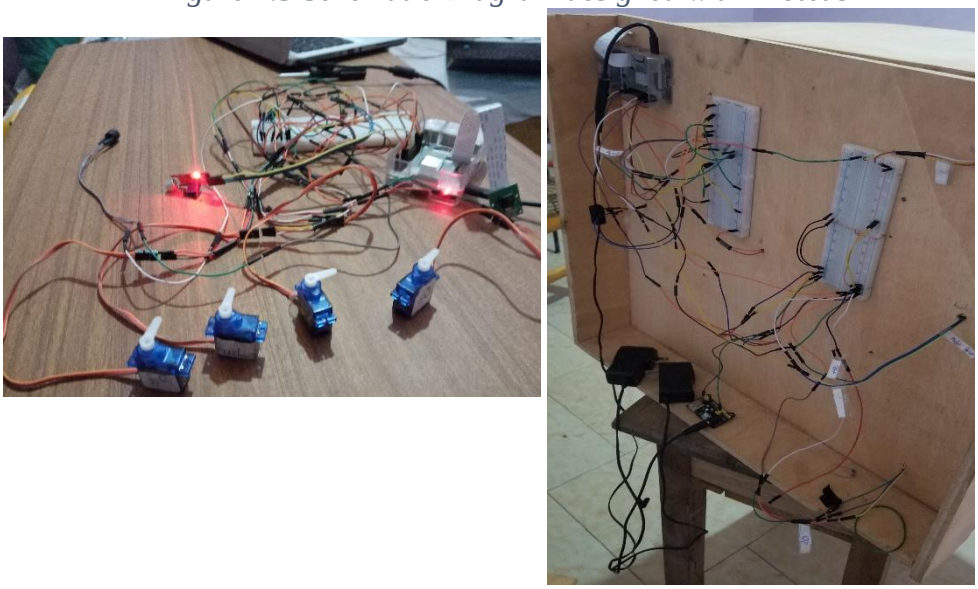


Figure 4.6 Implemented Electrical Set up

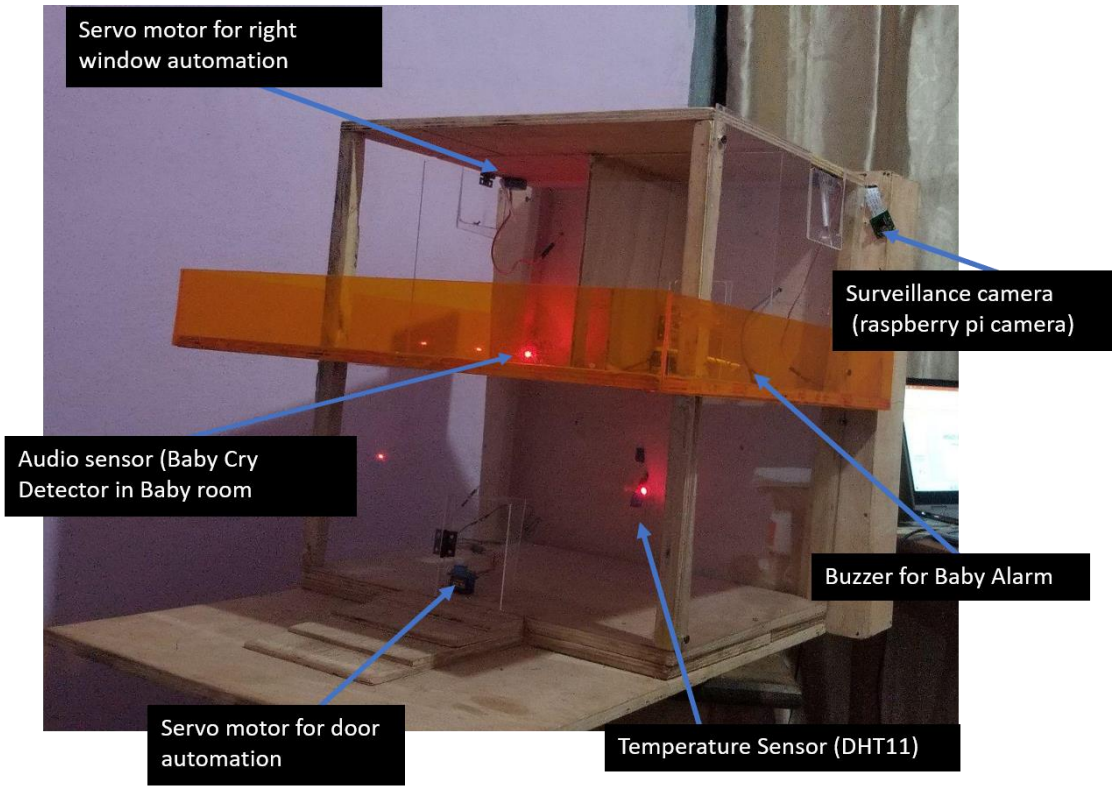


Figure 6.1 Complete Assembly

4.2 Data Collection and Storage

4.2.1 Sending Data

The data required to be sent from the Smart Home for demonstration of user autonomy are: audio data from baby alarm, images from surveillance camera, state (open or closed) of door upstairs in text , state of door downstairs , state of left window, state of right window. The audio sensor, Raspberry pi camera, and servo motors (door and window automation) are programmed in Python computer language to collect corresponding data types to the raspberry pi.

Then, an API was created using Python with MongoDB connectors. This API provides the protocol that regulates how data is collected from the sensors connected to the Raspberry pi, and

how they are to be displayed. This API is then connected to a database to store the data. A NoSQL database, MongoDB, was created to receive the various data types

4.3 Software interface

4.3.1 User Interface

The user interface is a web application developed using HTML, CSS, Bootstrap and Javascript. It was designed to have two windows. The first window is a dashboard that was split into two parts. The upper part shows the typical control buttons for an IoT page to show to main parts. Then, the lower part, has the novel inclusion of a session for performing user autonomous action. There the user can opt out and/or restore the collection of a particular data type as shown in Figure 4.8. The second window was created to provide the user with the opportunity to verify effect of his autonomous actions on the database. The second window can be accessed at the header area of the dashboard window.

At the header session, there is a button labelled ‘Details’. It was coded to serve as a hyperlink to open the second administrator web application window when clicked on. This page has a table that displays the various data types that are being stored in the database in real time. The columns are named by each data type and the rows are named by the time stamps that the data was taken. In the case where the collection of data type is interrupted, it shows as an empty area in the table.

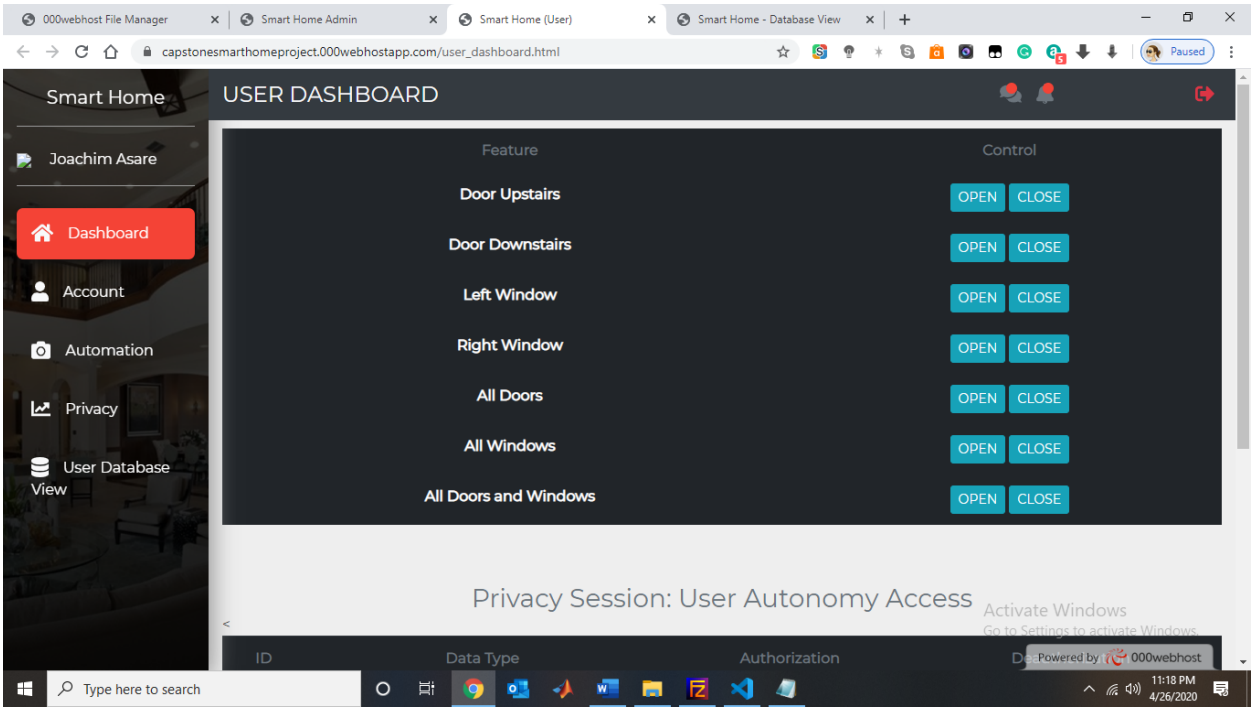


Figure 4.7: Session of User Web App Interface for Smart Home Automation commands

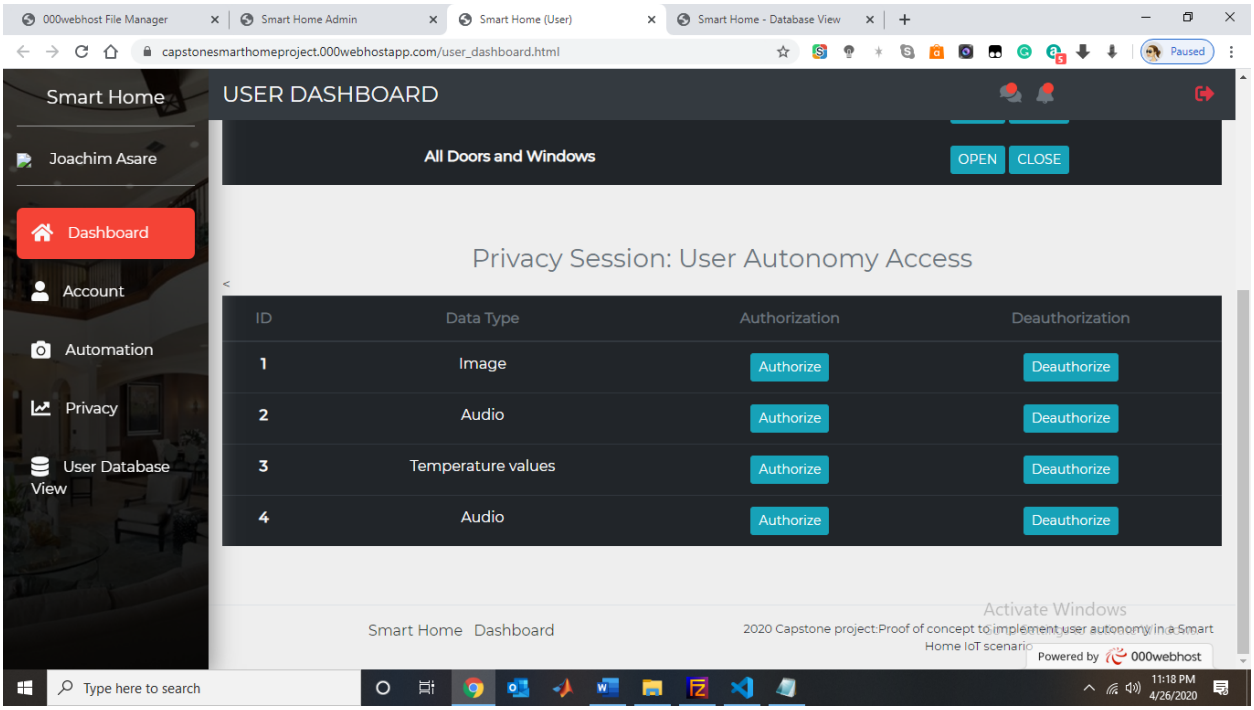


Figure 4.8 Privacy Session to allow user to have control over data transmitted to cloud database

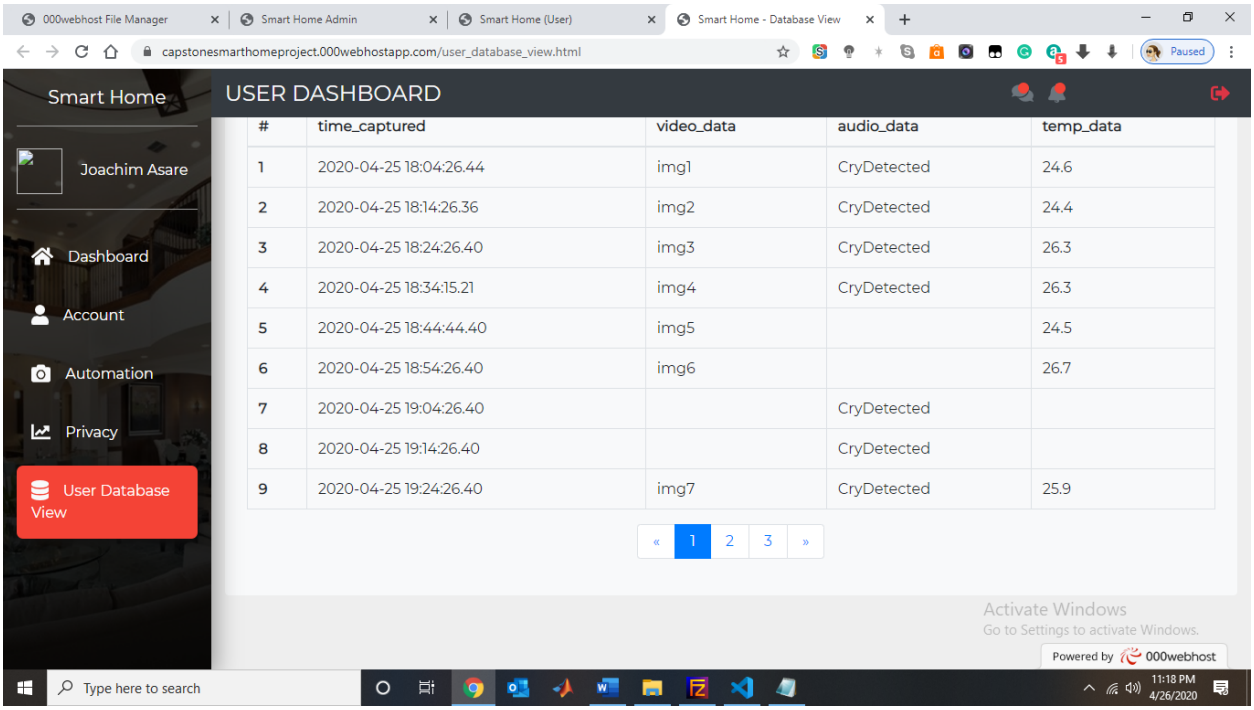


Figure 4.9 Second Web page to display MongoDB database real time logging connected to boostrap table

4.3.2 Administrator Interface

The administrator web application interface was also developed using Bootstrap and Javascript for its front-end design and Python for its back end with connections to the MongoDB Database server. It was made to have one window. The first window, which is the home page, is divided into three parts. The upper session was the home page window that displayed the list of sensor components of the Smart and indicated whether they are running or not. Secondly, the mid-session, has an analytics session that displayed a graph of the rate of transmission of the various data types. This graph was programmed back-end with Python and MongoDB Analytics and shown front-end using Javascript and Bootstrap. Lastly, the bottom session was designed to be a notification area that generated texts that indicate when a user issues or run an autonomous

action. A preview of the administrator home page developed is shown in Figures 4.9.1, 4.9.2 and 4.9.3

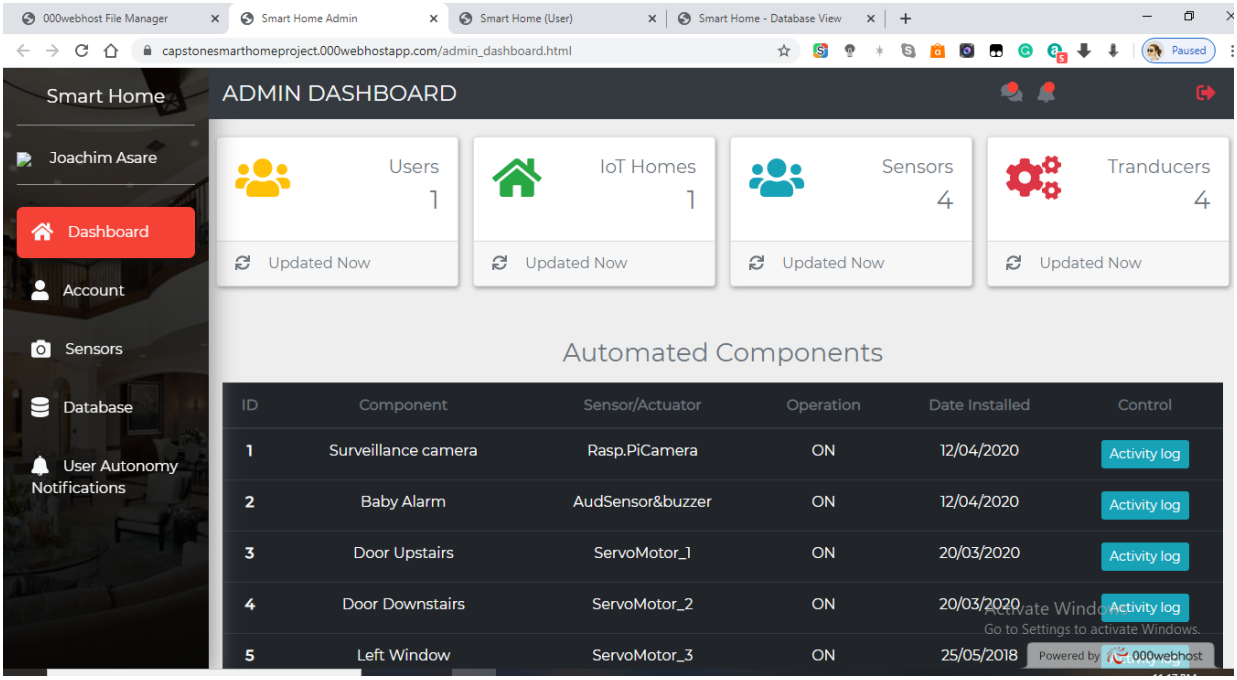


Figure 4.9.1 Top Session of Admin Webapp Interface

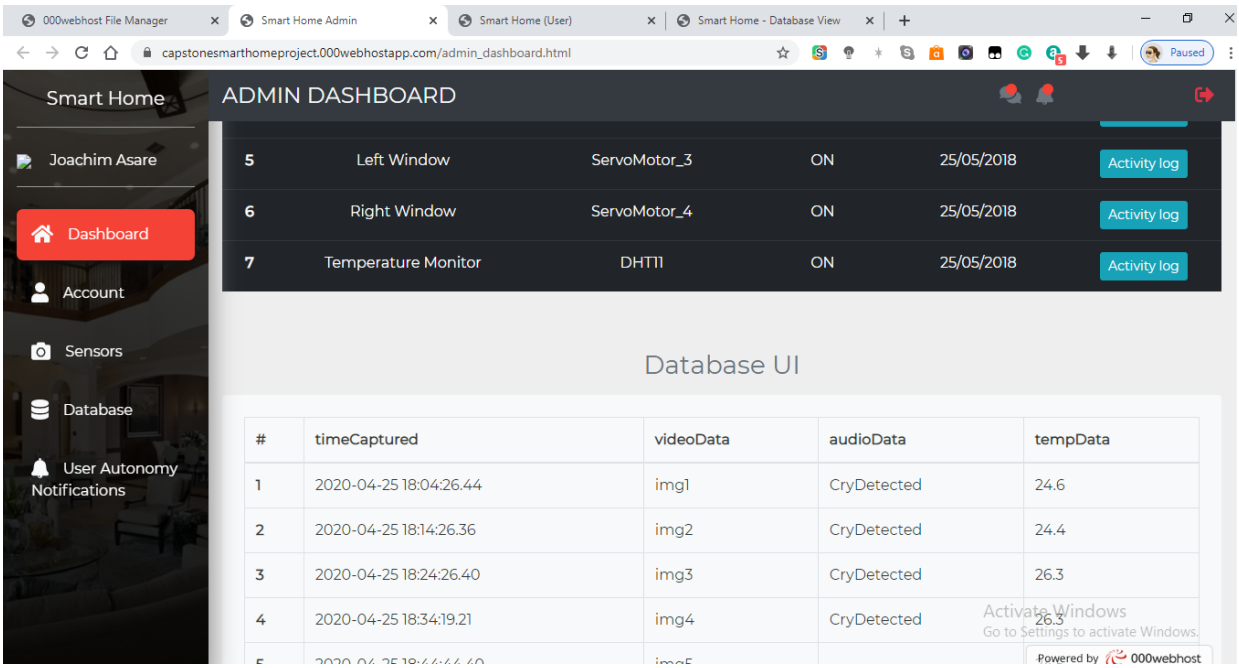


Figure 4.9.2 Middle Session of Admin Web app Interface

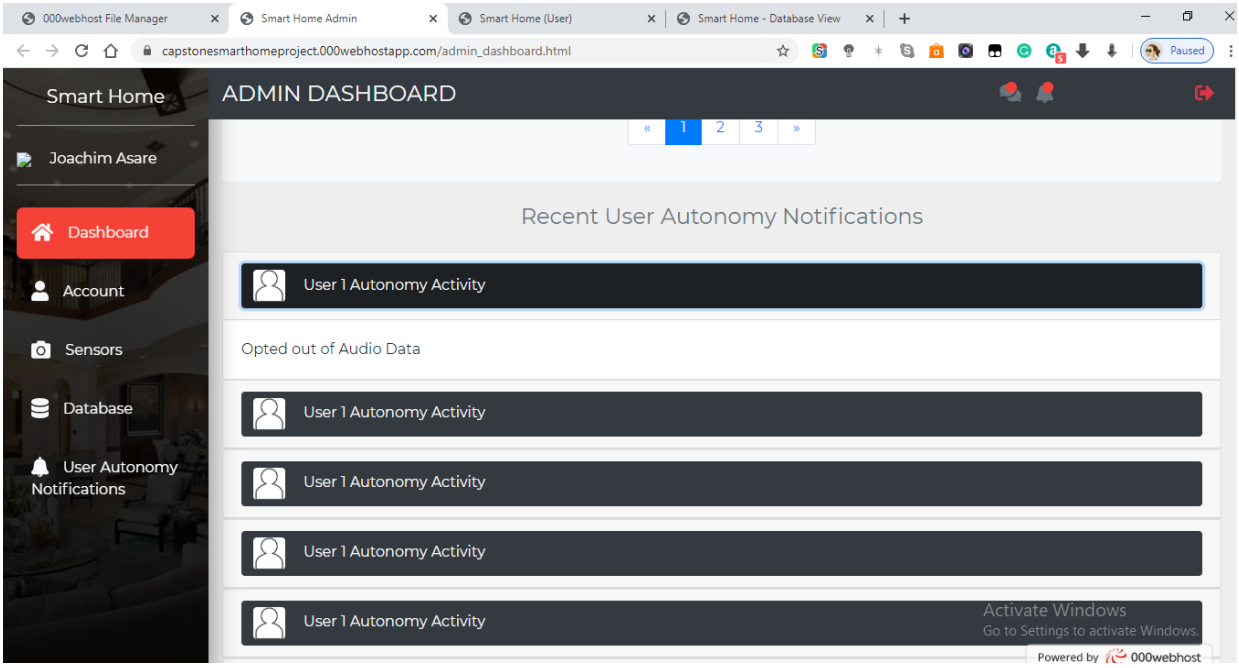


Figure 4.9.3 Bottom Session of Admin Web app Interface

Chapter 5: Results and Analysis

5.0 Overview

Chapter 5 highlights the outcomes observed from executing the methodology outlined in the previous chapter. Here, two case scenarios were used to show the result of the attempt to implement user autonomy in the smart home-based IoT system. The outcome or results of the implementation are illustrated using screenshots from the user and administrator web application interface as shown below

5.1 User Autonomy Results from Use Case Scenarios

Case 1: User **opts out** of the collection of his **audio data only for** 20 minutes.

To do this, the user logged unto his dashboard on the web app, then navigates to the 'Privacy Session: User Autonomy Access'. There, the user clicks on the 'Deauthorize' button corresponding to 'Audio' as shown in Figure 5.1. To validate the effect of the implementation of this command, the user clicks on 'User Database View' on the side navigation bar on the left of the page. This leads to a web page that shows the real time logging of data. This was viewed for 20mins and the result is shown in Figure 5.3. Also, a notification was successfully sent to the IoT administrator, as shown in Figure 5.4

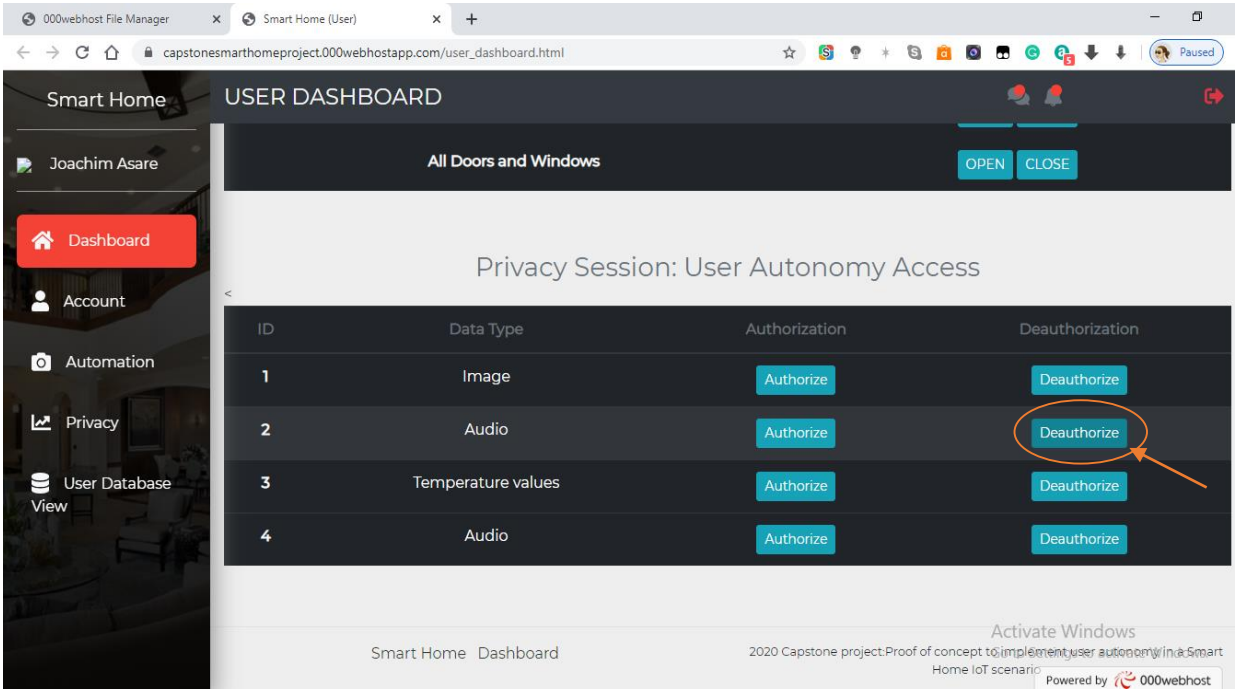


Figure 5.1 User Deauthorizes collection of audio data

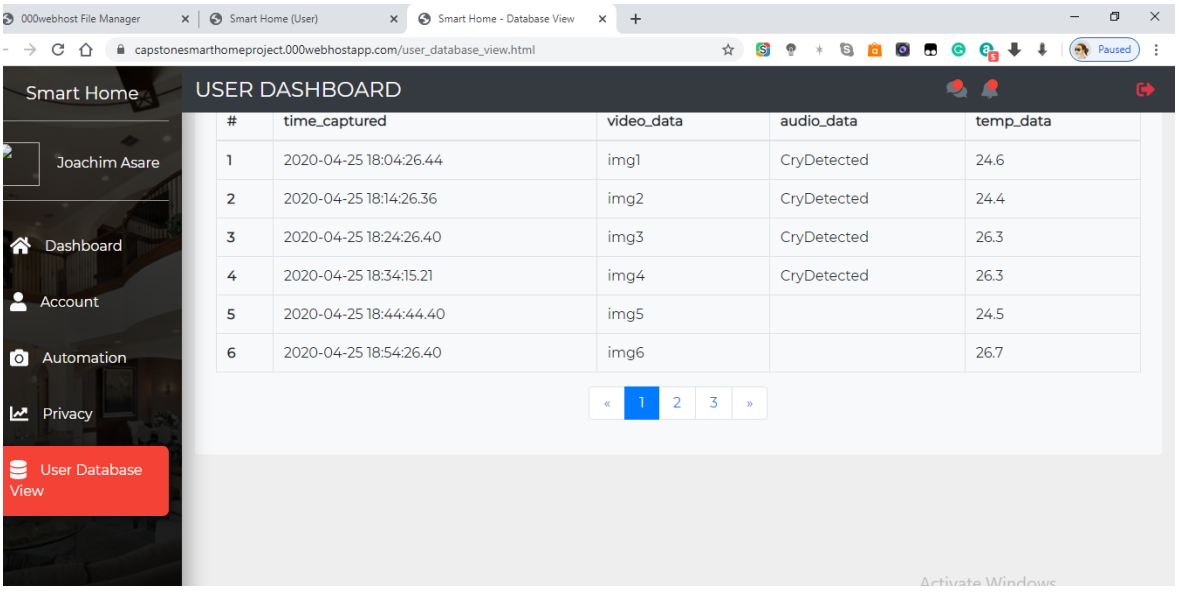


Figure 5.2 Figure Clicks on User Database View button

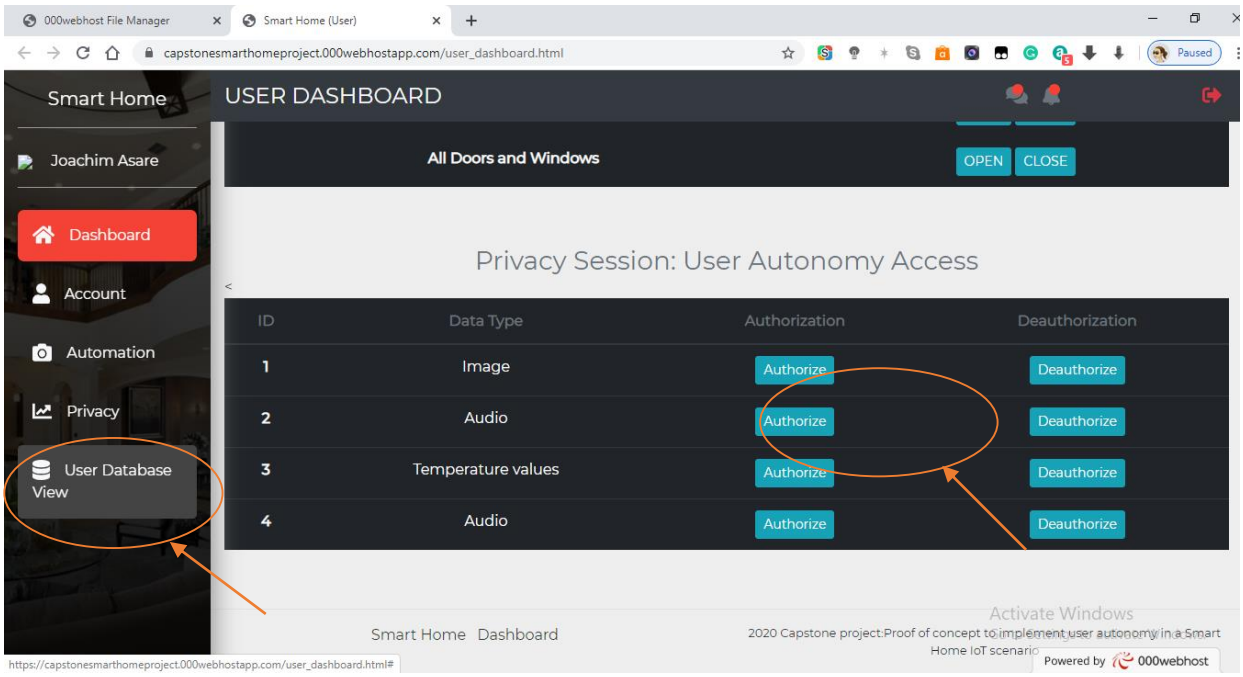


Figure 5.3 User views Audio Data not collected for the past 20 mins since it was deauthorized

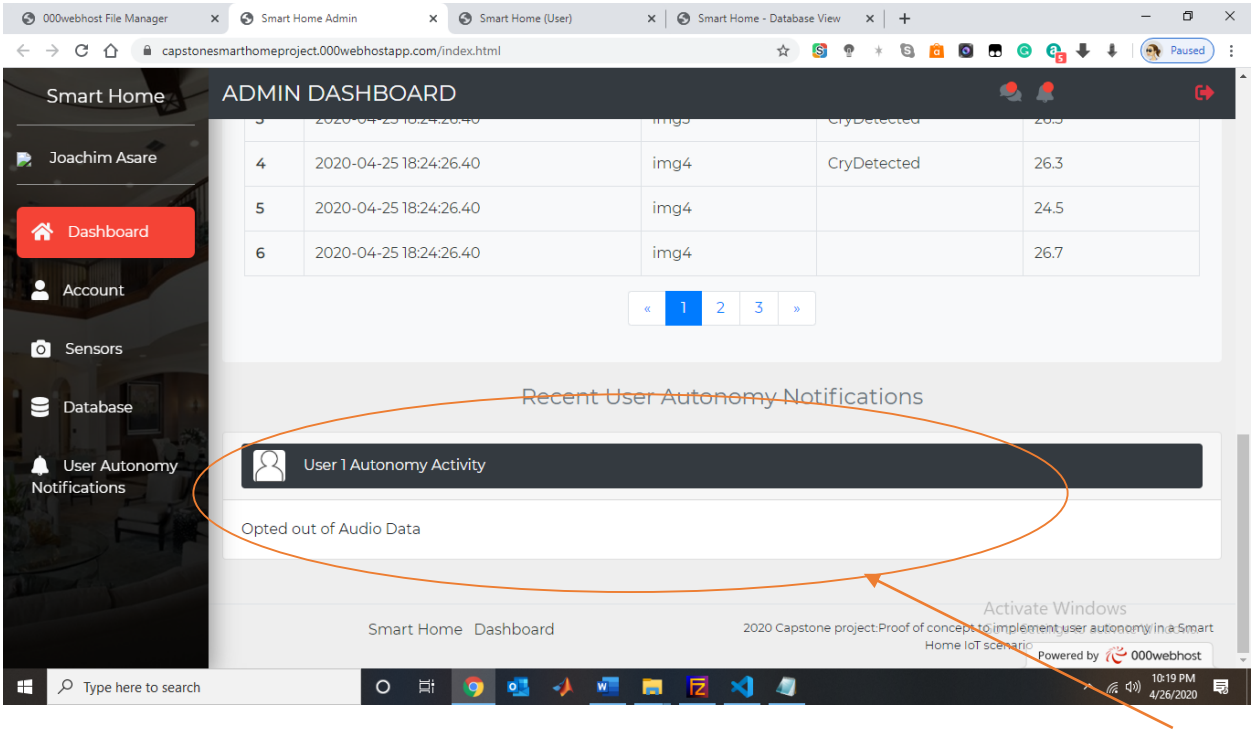


Figure 5.4 Admin successfully receives notification of user autonomy command initiated

Case 2: User opts out of the collection of Image data from his surveillance camera and temperature data while leaving other audio data collection ongoing.

This case scenario was set up to demonstrate multiple autonomous commands ran simultaneously. Therefore, in this case, image and temperature data collection are halted then then restored. In this situation, as done Case 2, audio data and temperature data are deauthorized and after 20 mins are authorized again. The results of these executions on the user, database view and admin pages are shown below. In addition, the IoT administrator web app indicated how there was reflection of these actions in the database and most importantly, notifications received on them. This is shown in Figures 5.5 to 5.9 below.

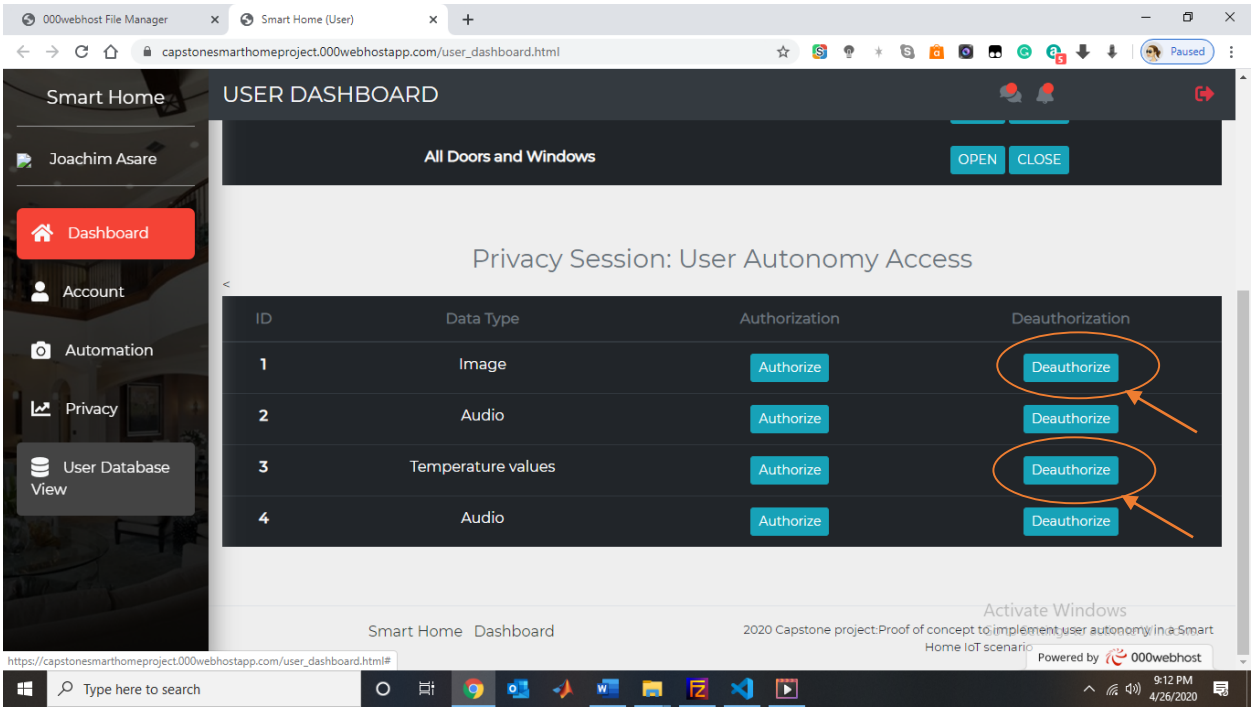


Figure 5.5 Image and temperature data are deauthorized from collection using the buttons

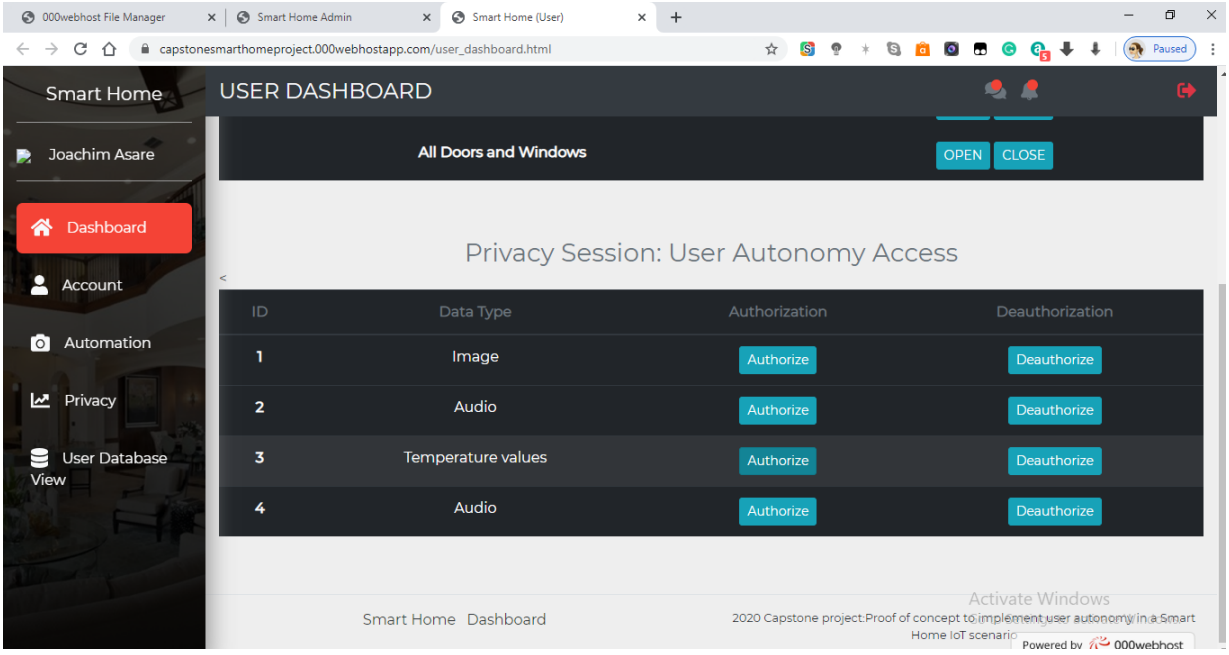


Figure 5.6 Image and Temperature data are authorized after 20mins

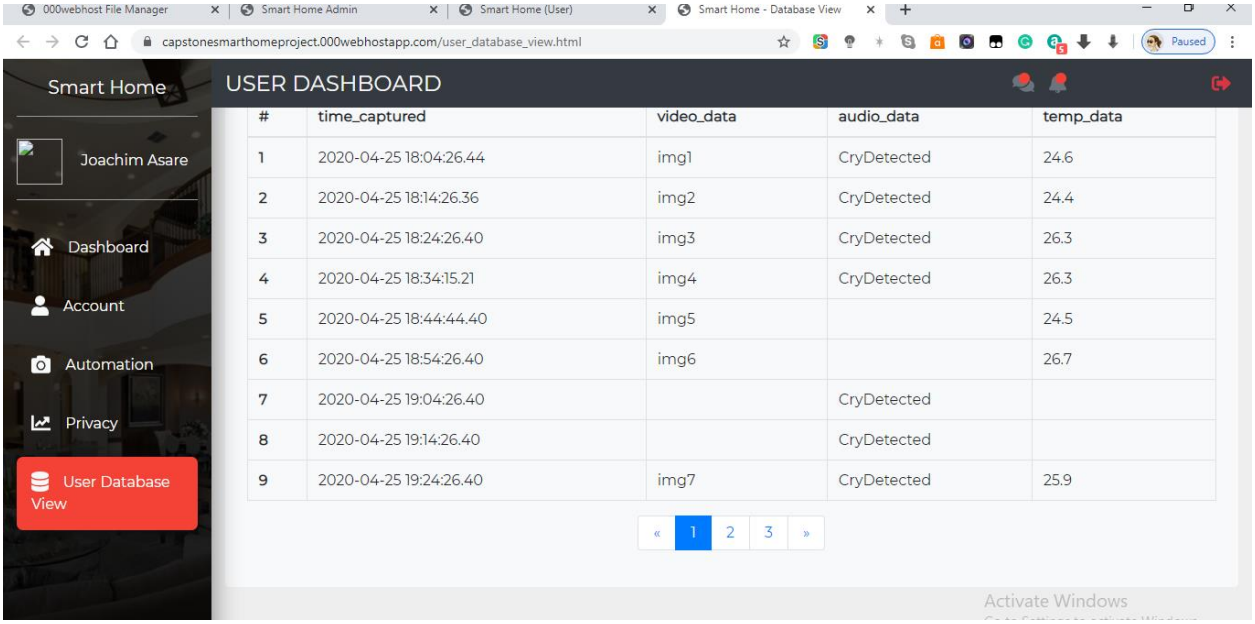


Figure 5.7 User validates deauthorization and later deauthorization after 20minutes each

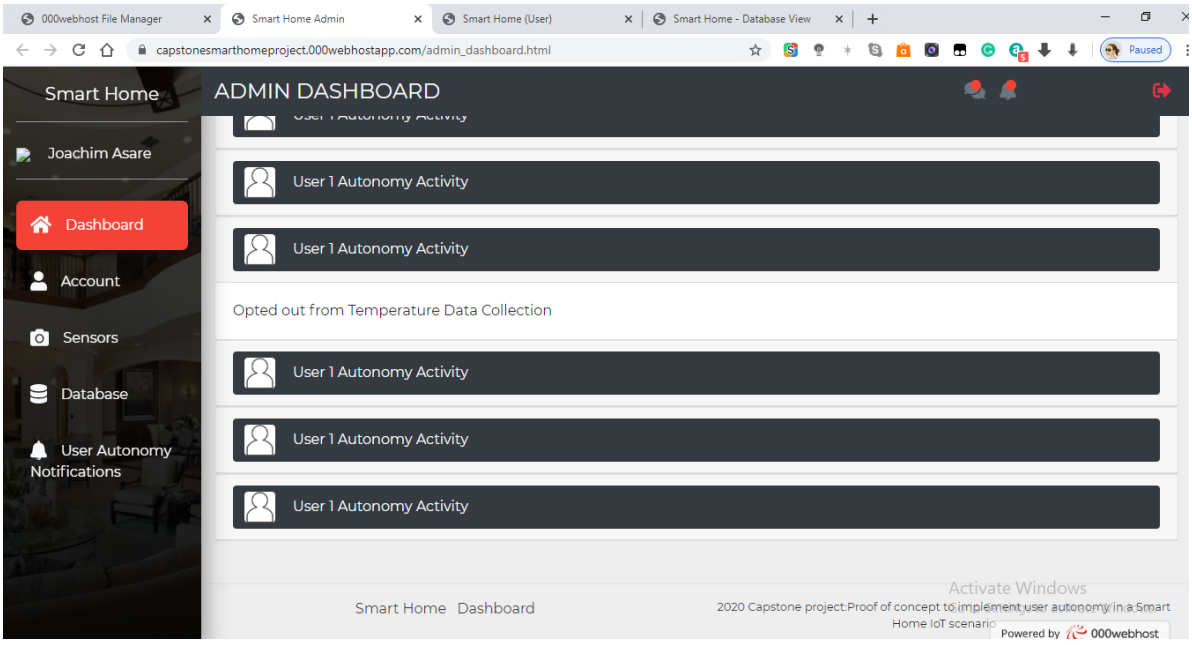


Figure 5.71 Notification received by Admin for deauthorization of Temperature data collection

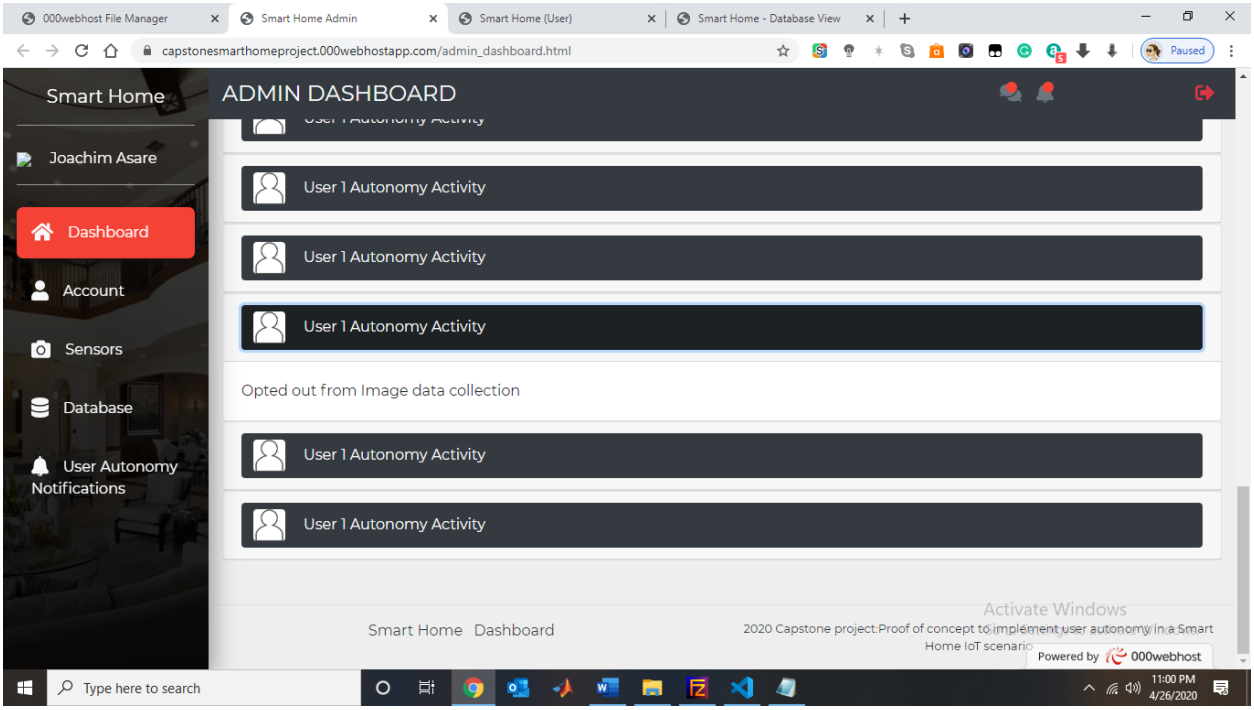


Figure 5.82 Notification received by Admin for deauthorization of Temperature data collection

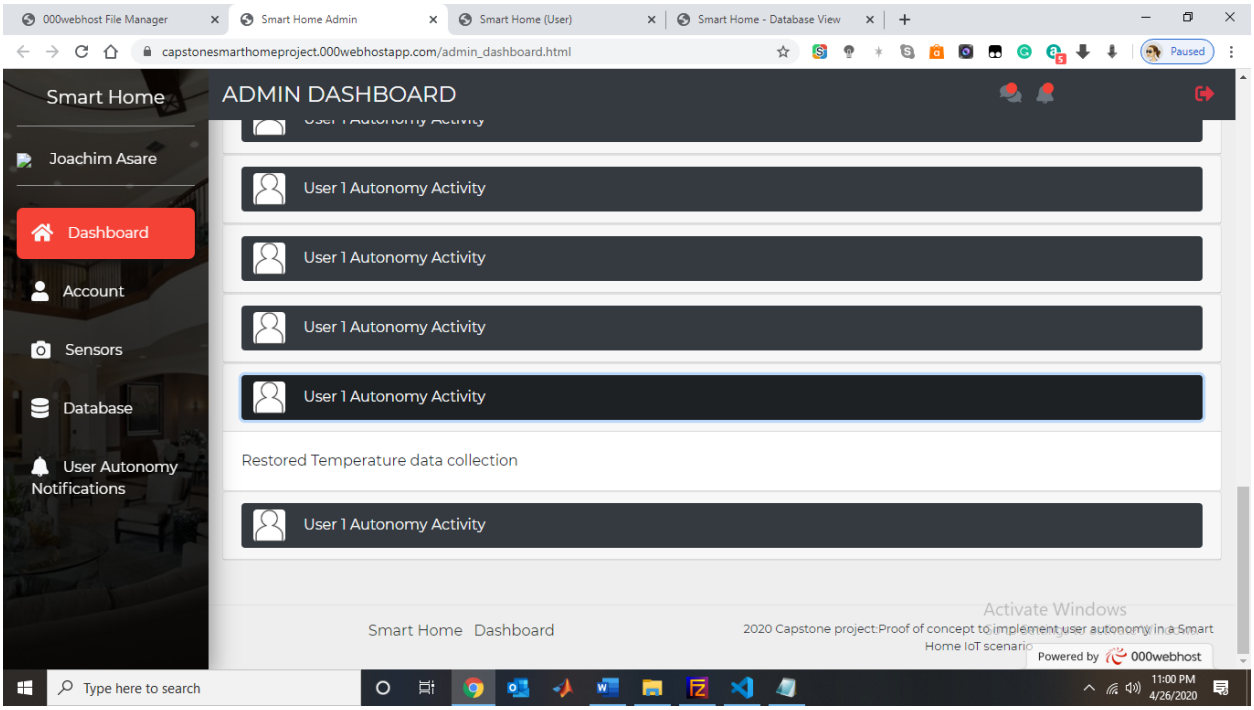


Figure 5.83 Notification received by Admin when User authorized Temperature data

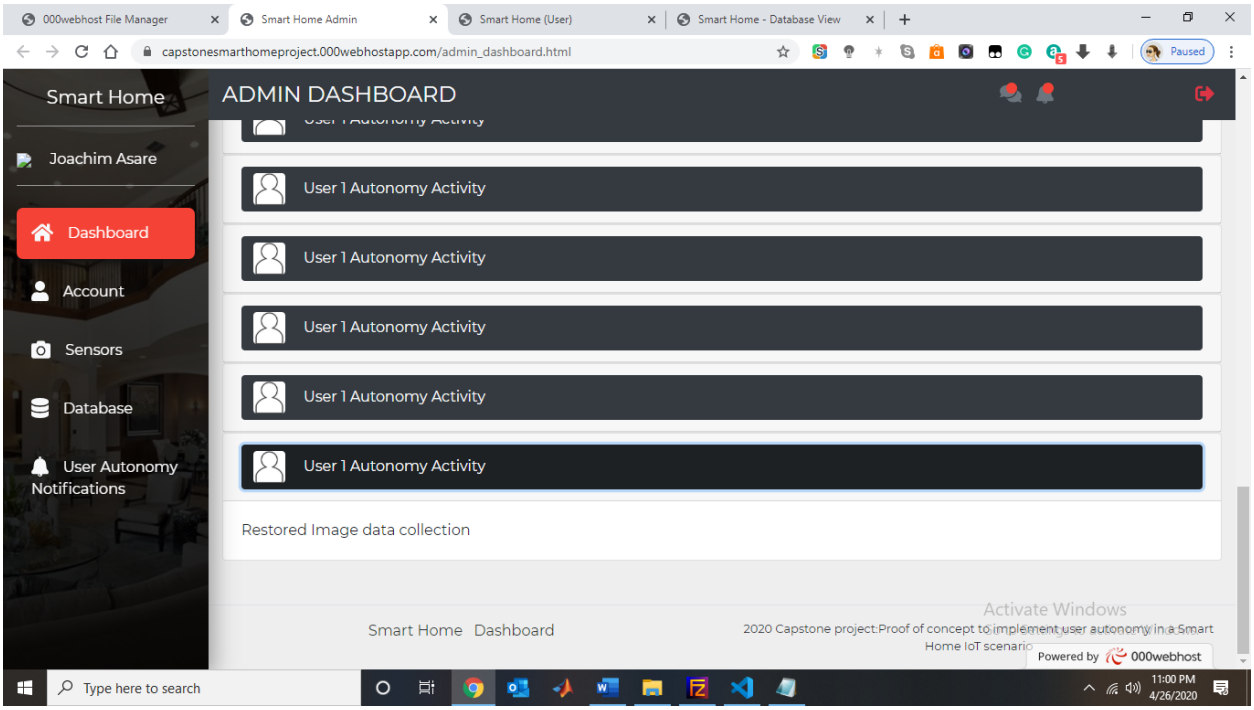


Figure 5.84 Notification received by Admin when User authorized Temperature data

Chapter 6: Conclusion & Recommendations

6.0 Overview

This chapter summaries the entire thesis including key outcomes based on the objectives and methodology used. It also discusses limitations to the such as constraints that were encountered during the work and proposes insights for future work on privacy-by-design in Internet of Things.

6.1 Summary

This research successfully met its three main objectives. First, the user was able to successfully have a session of the user web application interface to authorize or deauthorize several data types. Secondly, the user was also able to validate the result of his issued autonomy command over the user web interface as well. Lastly, an admin user interface was designed to show how the user dashboard would communicate with the IoT manager or administrator user interface. This was demonstrated when a notification description message was generated on the IoT manager or administrator dashboard each time the user performed an autonomous command.

Also, a model framework can be developed from this work to guide the implementation of privacy by design in IoT systems. This framework would inform the technical, functional and legal requirements of designing an IoT system that has the privacy of the user as a high priority. Functional and technical requirements were discussed in Chapter 3. On the other hand, the legal requirements must include requirements as shown in the example below.

6.1.1 Legal Requirements

a. The design must meet local data privacy laws such as the Data Protection Act, 2012 (Act 843) of Ghana [25].

b. The design must meet international data privacy laws such of those of the General Data Protection Regulation (GDPR) of the European Union. For example, in this research, the session on the web application that allows the user to view the data being collected meets Chapter 3, Article15 of the GDPR [26]. It states that, “The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case …” [26].

6.2 Limitations

One of the major limitations to this project was the constrained budget of $50.00 available for the research. Due to this more sophisticated and expensive components including mainstream smart objects and sensors used in ideal case Smart Home scenarios could not be used. Cheaper and more education tailored components were purchased instead. This financial constraint also influenced the choice of the IoT system. For example, to develop this proof of concept in a Smart IoT based vehicle, an On-Board Diagnostic Device would have to be attached and it costs about US$900 [27].

Notwithstanding, deployment of the Smart Home IoT system ran for over a short time of 3 hours due to limited database space 512MB of space on MongoDB Atlas for data storage. Paid storage services on the server cost US$946.79 annually [28]. Hence typical deployment of IoT systems for longer periods such as months was not demonstrated due to this constraint.

6.3 Future Work

Though the proof of concept of the implementation of user autonomy in a Smart Home IoT system was successful, it is necessary to apply this in several other diverse IoT scenarios. This is

because the data specifications such as the variety, velocity and veracity of data may differ with different IoT applications. Owing to this, the database and network requirements would vary. Therefore, there is the need to investigate and explore other design options to implement user autonomy actions and its performance across different IoT systems.

As indicated under limitations, financial constraints have a significant impact of the quality of research in this area. Based on this work, it is recommended that further research must be financially capable of simulating an ideal IoT system as much as possible. That way, results obtained would be more reliable and applicable including industrial applications that are relatively expensive to implement. Ideal world high performing IoT systems have more sophisticated and costly components such as large-scale deployable sensors and microcontrollers.

Furthermore, though the objectives of this project were met, it is recommended that the option of executing user autonomy at the edge level is explored other than executing user autonomy commands at the application layer (as done in this work). Performing thorough data and network analytics is done. This research focused more on the demonstration of user autonomy at the user interface front end. However, it would be informative to view how executing these commands would have some effect on the data and network and if so, to what extent.

References

[1] Ahmed A. & Gad-Elrab A. (2019), "Benefits and Challenges of Internet of Things for Telecommunication Networks". doi: 10.5772/intechopen.81891

[2] Jian D. and Chao S. (2013), "A study of information security for M2M of IOT - IEEE Conference Publication", *Ieeexplore.ieee.org*, 2019. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5579563&isnumber=5579079.

[3] Formisano C. et al., "The Advantages of IoT and Cloud Applied to Smart Cities," 2015 3rd International Conference on Future Internet of Things and Cloud, Rome, 2015, pp. 325-332.doi: 10.1109/FiCloud.2015.85

[4] C. B, "Semi-autonomous, context-aware, agent using behaviour modelling and reputation systems to authorize data operation in the Internet of Things - IEEE Conference Publication", *Ieeexplore.ieee.org*, 2019. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6803201&isnumber=6803102. [Accessed: 08- Oct- 2019].

[5] Mukhopadhyay S.C., Suryadevara N.K. (2014) Internet of Things: Challenges and Opportunities. In: Mukhopadhyay S. (eds) Internet of Things. Smart Sensors, Measurement and Instrumentation, vol 9. Springer, Cham

[6] Hicks, K. (2017, June 14). Smart cities: How the Internet of Things is changing urban areas. Quoted.

[7] Wolfson S. (2018). Amazon's Alexa recorded private conversation and sent it to random contact. Retrieved from https://www.theguardian.com/technology/2018/may/24/amazon-alexa-recorded-conversation

[8] Timberg, C. (2019). The Washington Post: Consumer groups accuse Amazon of illegally collecting data on children. Retrieved from https://www.washingtonpost.com/business/technology/ 2019/05/08/2af2d282-71cc-11e9-b5ca-3d72a9fa8ff1_story.html

[9] Yuchen Y., et al., "A Survey on Security and Privacy Issues in Internet-of-Things - IEEE Journals & Magazine", *Ieeexplore.ieee.org*, 2019. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7902207&isnumber=8059894. [Accessed: 13- Oct- 2019].

[10] Tian Y., et al., "SmartAuth: User-Centered Authorization for the Internet of Things", *Usenix.org*, 2019. [Online]. Available: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/tian. [Accessed: 7- Oct- 2019].

[11] Abomhara M., & Køien M., "Security and privacy in the Internet of Things: Current status and open issues," *2014 International Conference on Privacy and Security in Mobile Systems (PRISMS)*, Aalborg, 2014, pp. 1-8. doi: 10.1109/PRISMS.2014.6970594

[12] Bertino, E. (n.d.). *Data Security and Privacy in the IoT*. https://doi.org/10.5441/002/edbt.2016.02

[13] Data Protection Commission (2019). About Data Protection Commission. Retrieved from https://www.dataprotection.org.gh/about-us/the-commission

[14] *Constitution of the Republic of Ghana* [Ghana], 7 January 1993, available at: https://www.refworld.org/docid/3ae6b5850.html [accessed 1 November 2019]

[15] Data Protection Commission (2019). Data Protection for Individuals. Retrieved from https://www.dataprotection.org.gh/index.php/data-protection/data-protection-for-individuals

[16] Data Protection Commission (2019). The Data Protection Principles. Retrieved from https://www.dataprotection.org.gh/data-protection/data-protection-principles

[17] Greenleaf, Graham, Global Data Privacy Laws: 89 Countries, and Accelerating (February 6, 2012). Privacy Laws & Business International Report, Issue 115, Special Supplement, February 2012; Queen Mary School of Law Legal Studies Research Paper No. 98/2012. Available at SSRN: https://ssrn.com/abstract=2000034

[18] Atlam, H. F., & Wills, G. B. (2019). IoT Security, Privacy, Safety and Ethics. *Internet of Things*, 123–149. https://doi.org/10.1007/978-3-030-18732-3_8

[19] Mashhadi, A, Kawsar, F and Acer, U. G. "Human Data Interaction in IoT: The ownership aspect," *2014 IEEE World Forum on Internet of Things (WF-IoT)*, Seoul, 2014, pp. 159-162. doi: 10.1109/WF-IoT.2014.6803139

[20] Baldini, G., Botterman, M., Neisse, R., & Tallacchini, M. (2016). Ethical Design in the Internet of Things. *Science and Engineering Ethics*, *24*(3), 905–925. https://doi.org/10.1007/s11948-016-9754-5

[21] Maras, M.-H. (2015). Internet of Things: security and privacy implications. *International Data Privacy Law*, 5(2), pp.99–104.

[22] Neisse, R., Steri, G., Fovino, I. N., & Baldini, G. (2015). SecKit: A model-based security toolkit for the internet of things. Elsevier Computers & Security Journal. doi: 10.1016/j.cose.2015.06.002.

[23] Ukil, A., Bandyopadhyay S. and Pal A., "Privacy for IoT: Involuntary privacy enablement for smart energy systems," *2015 IEEE International Conference on Communications (ICC)*, London, 2015, pp. 536-541. doi: 10.1109/ICC.2015.7248377

[24] Ukil, A., Bandyopadhyay, S., & Pal, A. (2014, July 8). IoT-Privacy: To Be Private or Not to Be Private. Retrieved November 1, 2019, from https://ieeexplore.ieee.org/document/6849186/.

[25] Amazon (2020). LAUNCH X431 V PRO Bi-Directional Scan Tool Full System Scanner,Key Programming,Reset Functions ABS Bleeding,TPMS,EPB,SAS,DPF,BMS,ECU Coding, Injector Coding, Full Connector Kit- Free Update. Retrieved from https://www.amazon.com/LAUNCH-Diagnostic-Bi-Directional-Control-Warranty /dp/

B01GRN4BRQ/ref=sr_1_23?dchild=1&keywords=On-Board+Diagnostic+system +for+ car&qid=1587963489&s=automotive&sr=1-23

[26] Mongo DB (2020). FAQ: How much does MongoDB Atlas cost? Retrieved from

https://www.mongodb.com/cloud/atlas/faq

[27] *Constitution of the Republic of Ghana* [Ghana], 7 January 1993, available at: https://www.refworld.org/docid/3ae6b5850.html [accessed 1 November 2019]

[28] *EU General Data Protection Regulation (GDPR):* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.