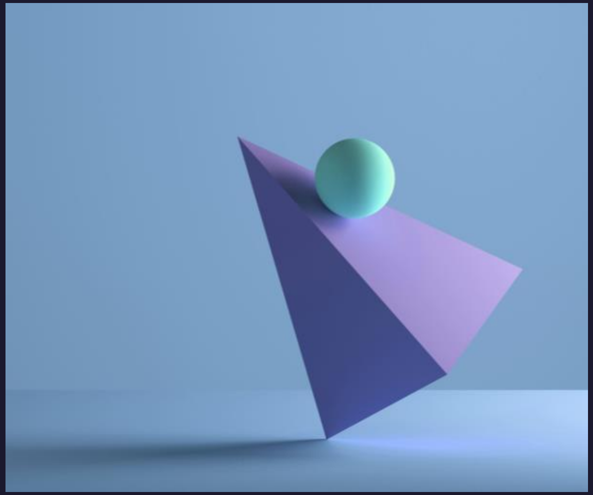
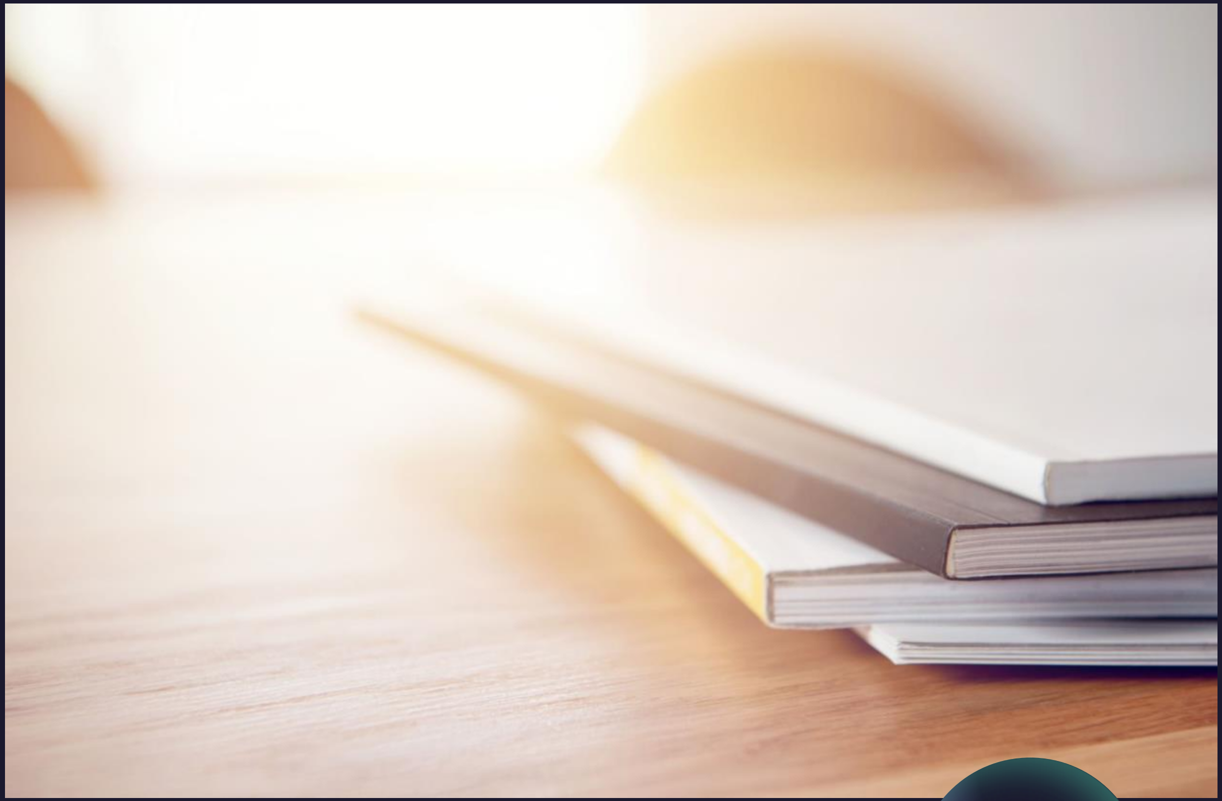
Internet of Things in Healthcare: Case Study in Care Homes

Authors

Tochukwu Emma-Duru
Email: Tochukwu.emma-duru@hud.ac.uk
Violeta Holmes
Email: V.Holmes@hud.ac.uk



About the Presenter



Tochukwu Emma-Duru

Is a Computer Scientist and is pursuing her PhD in Computer Science and Informatics at the University of Huddersfield. She has interest in the Internet of Things (IoT) and its security at the edge.

Outline of the presentation

- ❑ Motivation
- ❑ Related work
- ❑ Security issues in IoT - Security at the edge in healthcare
- ❑ Methodology
- ❑ Experimental set-up (architecture of the system)
- ❑ Obtaining sensing data and communication to cloud ThingSpeak
- ❑ Creating secure website – 2FA
- ❑ Conclusion and Future work

Motivation

- Since the adoption of the Internet of Things in the Healthcare sector, focus is mostly in hospitals with lesser attention given to care homes.
- Pressure sores are predominant in service users who have got low mobility, having pressure sensors in place to enable staff monitor these service users and the pressure the exact in real time would help reduce the development of these pressure sores.
- Also this research is aimed at providing a secured system for care homes by providing a two factor authentication for a safe login and also using edge devices to monitor the network against intrusion.

Related work

- Much research is being carried out in the use of IoT and its security in the healthcare sector with the main focus on hospitals, and not necessarily in care homes, and this is what this research focuses on.
- In care homes recently, IoT is being deployed like using sensor mats to detect falls, wearable devices to monitor the patients' vitals, temperature sensors, humidity sensors, and a few others.
- Many care homes still implement the traditional method of storing patients’ data and monitoring sensors via their care plans and daily logbooks.
- Real-time monitoring of patients’ vitals and information in care homes is not common.
- It is mostly their personal records and information that can be accessed online, and it is mostly managers, nurses and senior carers who have access to these.
- Most existing research focuses on highlighting the trends and current challenges and proposing more solutions which IoT can offer the health sector in general.

Security issues in IoT

- The more devices become a part of the Internet framework, the more global exposures would give rise to more security vulnerabilities giving room for attackers and cybercriminals to exploit these security flaws.
- IoT devices can be exposed to these security risks due to inadequacies in their systems design, which may lack security features such as authentication and authorization and have deficient communication media.
- Hackers can attack IoT devices due to the default software configuration, inconsistent software updates and the extended distance between the patch release and its installation. Security in IoT is crucial and needs to constantly be maintained to protect the billions of devices connected to the Internet.
- Some of the main security issues in IoT include Botnet, Malware attacks, Man-in-the-Middle attacks, and Denial of Service attacks

Methodology

- A combination of qualitative and quantitative research was applied to enable the design of such IoT systems for healthcare applications.

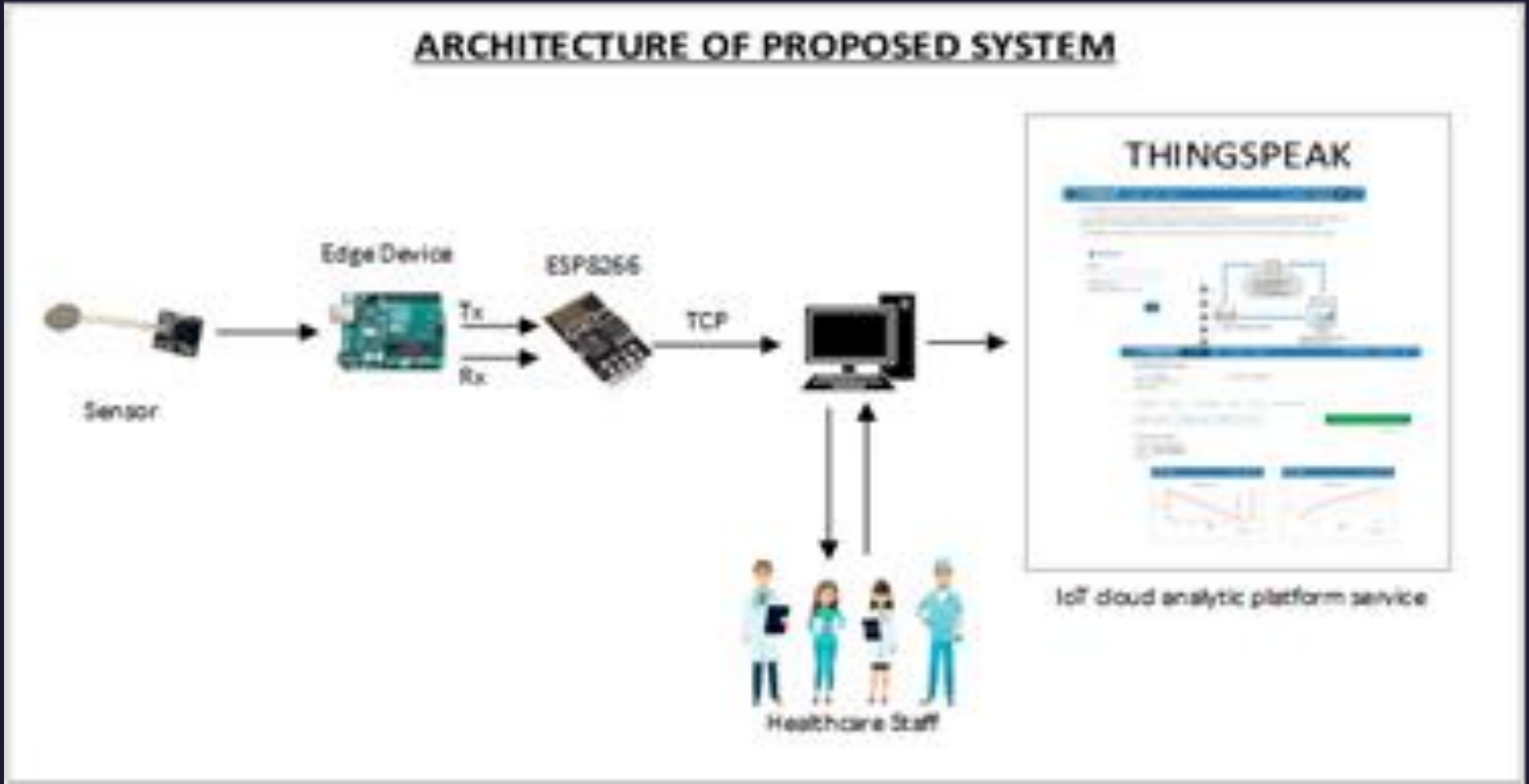
- The qualitative research involved carrying out a survey for nurses and carers in care homes to understand the gap in knowledge on the adoption of IoT in the homes and what kind of system that would be designed for more security.

- With the information gathered from the survey, experiments were performed to design the system required to monitor patients prone to developing sores in real-time. A secured system using edge devices to monitor and detect intrusion by deploying machine learning would be developed in the future.

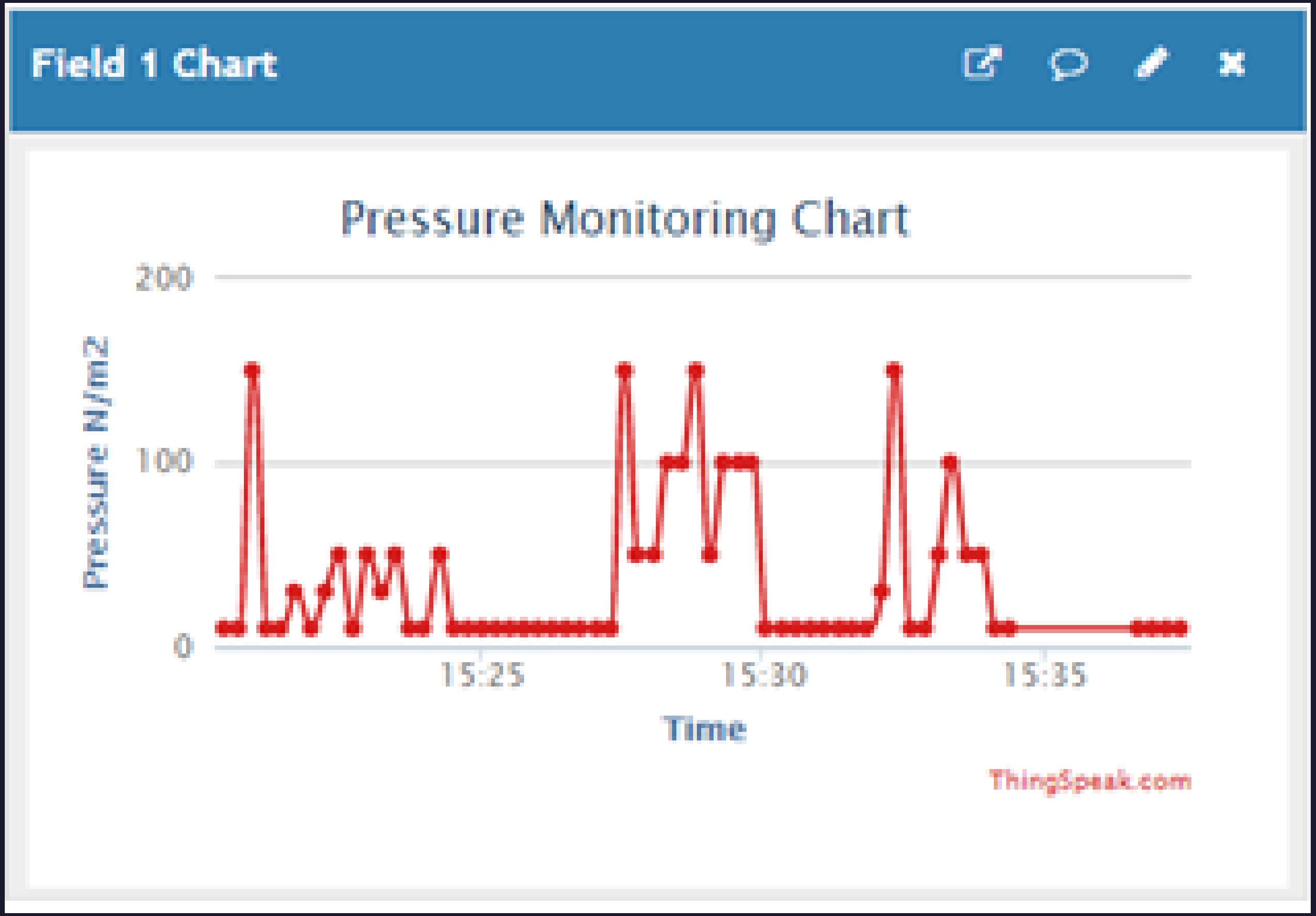
Experimental set-up

- The IoT based system would enable the healthcare staff to monitor patients' vitals in real-time on ThingSpeak, provide a more secure webpage using the 2FA secured method.

- The system consists of the pressure sensors, LED, Arduino UNO, Esp8266 and ThingSpeak network cloud platform. Below is the architecture setup of the system:


ARCHITECTURE OF PROPOSED SYSTEM
Edge Device
ESP8266
Tx
Rx
TCP
Sensor
THINGSPEAK
IoT cloud analytic platform service
Healthcare Staff

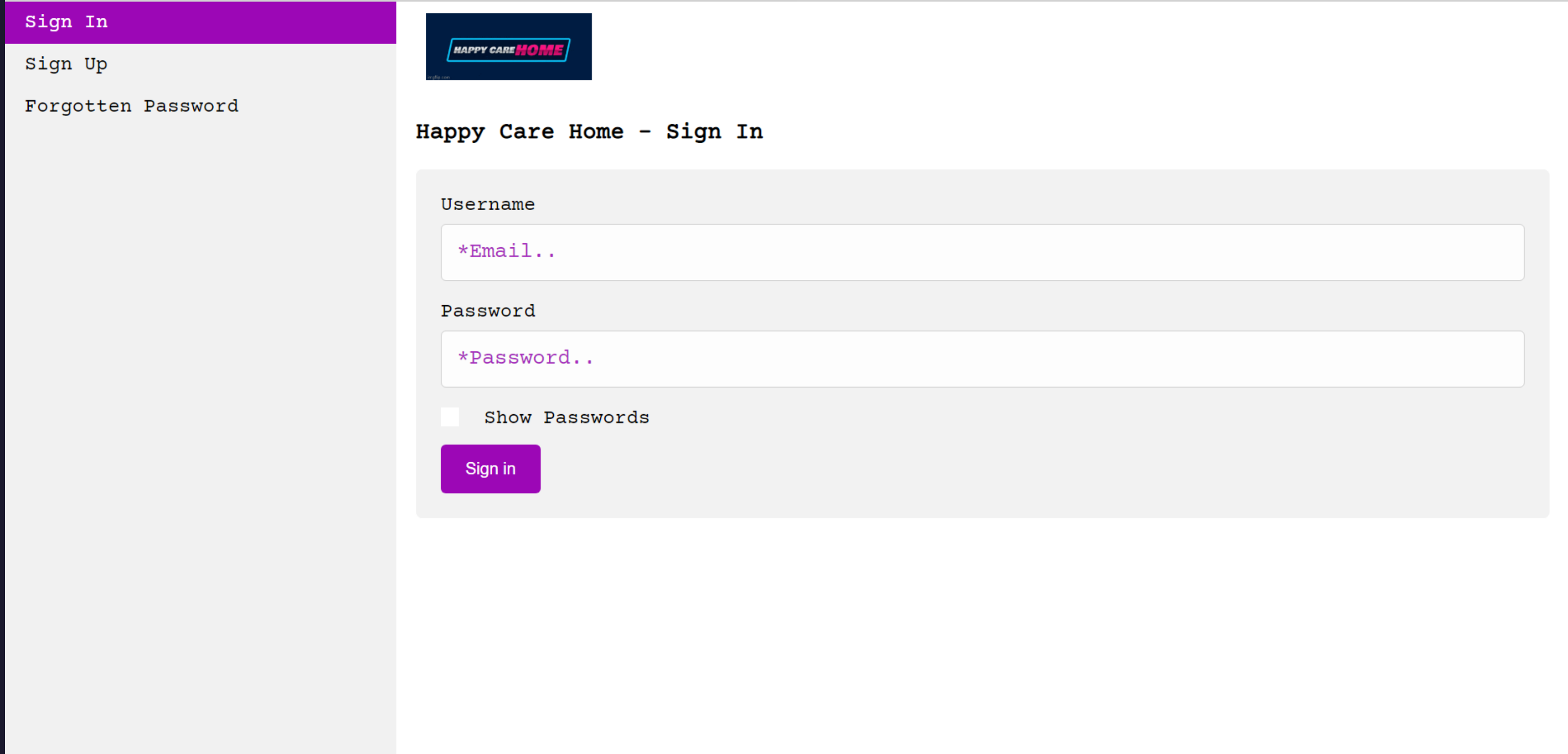
Obtaining sensing data and communication to cloud ThingSpeak



- The pressure sensor reads when pressure is exerted on different body parts and passed through to the edge device and the cloud network.
- To provide a more secure system, a two-factor authentication (2FA) system would be deployed.
- Staff would be required to input a passcode while logging into the platform through a webpage.
- The Field 1 Chart shows the results from pressure that was monitored in real-time from ThingSpeak

Creating secure website

- A website with the 2FA for staff log in before they can get access to the system.
- The 2FA was implemented for the front end users (nurses and carers) as well as the admin who has access to the back-end administration.
- Figure shows the secured 2FA log in page



Happy Care Home - Sign In

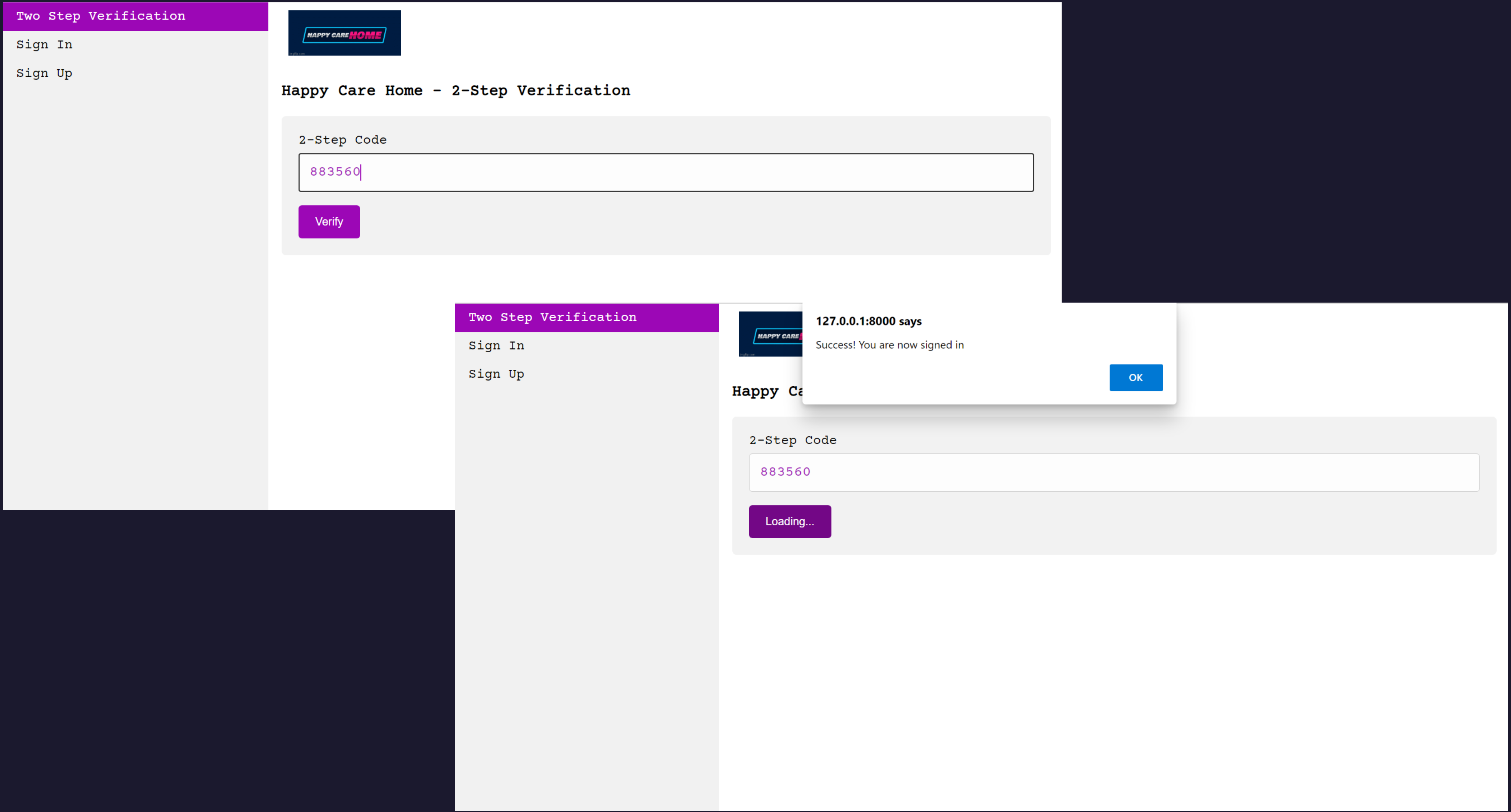
Username

*Email..

Password

*Password..

□ Show Passwords



Happy Care Home - 2-Step Verification

2-Step Code

883560

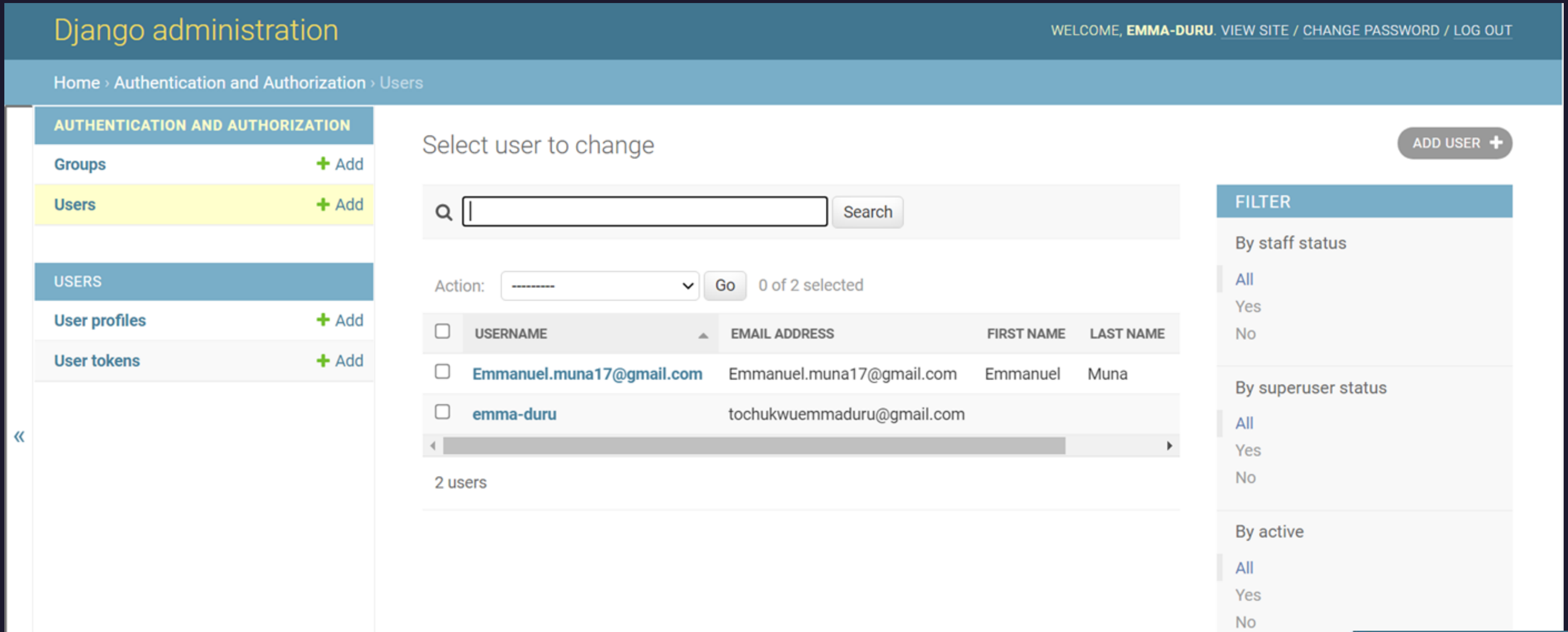
Happy Ca

127.0.0.1:8000 says

Success! You are now signed in

2-Step Code

883560



Django administration

WELCOME, **EMMA-DURU**. VIEW SITE / CHANGE PASSWORD / LOG OUT

Home › Authentication and Authorization › Users

AUTHENTICATION AND AUTHORIZATION

- Groups + Add
- Users + Add

USERS

- User profiles + Add
- User tokens + Add

Select user to change

ADD USER +

Search

Action: --------- Go 0 of 2 selected

□	USERNAME	EMAIL ADDRESS	FIRST NAME	LAST NAME
□	Emmanuel.muna17@gmail.com	Emmanuel.muna17@gmail.com	Emmanuel	Muna
□	emma-duru	tochukwuemmaduru@gmail.com		

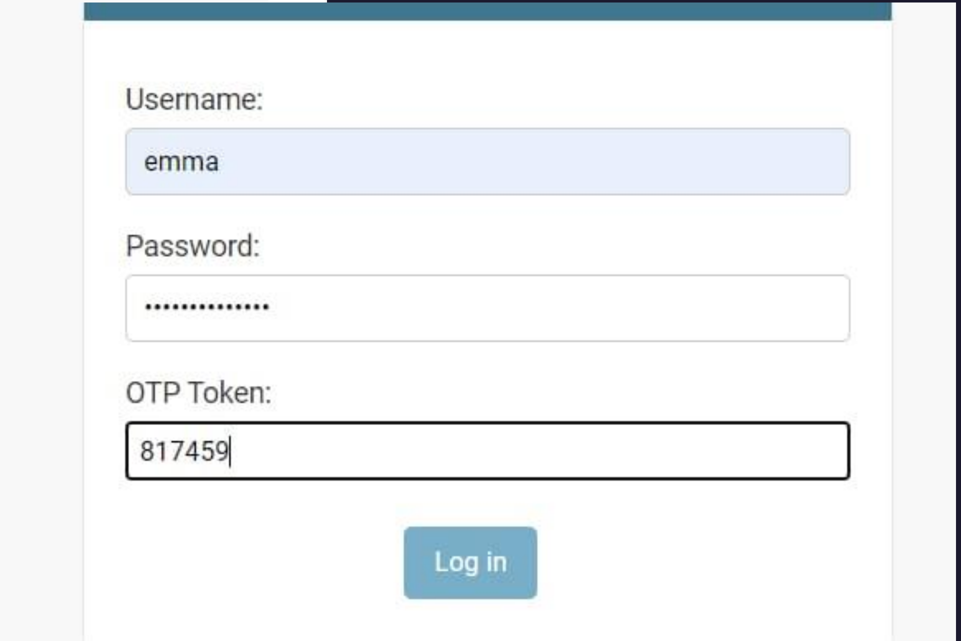
2 users

FILTER

By staff status
- All
- Yes
- No

By superuser status
- All
- Yes
- No

By active
- All
- Yes
- No



Username: emma

Password: ••••••••••••••

OTP Token: 817459

Log in

Conclusion and Future work

- There is a need for a safe IoT system for storage, transfer, and easy retrieval of patients’ data on the cloud.
- The proposed IoT system is designed to fill this need.
- The system will enable a transfer of data from the IoT based sensors, such as pressure sensors, to the cloud (TTN and ThingSpeak) and will have strong security features.
- Two-factor authentication (2FA), which was implemented is proving to be one of the safest security features to ensure data protection and security and prevent unauthorized access.
- The staff will be able to access the cloud platform, record the data on the system and retrieve real-time information on patients’ data.
- In addition, the proposed system would involve analysis of the data on the ThingSpeak platform and using machine learning algorithms in MATLAB to run simulations and train machine learning models to detect safety breaches.
- Future work would be focused on evaluating the effectiveness of the proposed system in a case study that will involve a monitoring of pressure to prevent pressure sores.
- The effectiveness of the system will consider the safe communication of the sensors data, storage, and retrieval of the information on a cloud and safe access to the data by the home care staff.