Internet of Things in Healthcare: Case Study in Care Homes

Tochukwu Emma-Duru
School of Computer and Engineering
University of Huddersfield
Huddersfield, United Kingdom
e-mail: Tochukwu.emma-duru@hud.ac.uk

Violeta Holmes
School of Computer and Engineering
University of Huddersfield
Huddersfield, United Kingdom
e-mail: V.Holmes@hud.ac.uk

***Abstract*— The Internet of Things (IoT) involves the interconnection of devices and humans to the Internet. IoT is rapidly being adopted in different sectors of life, including the health sector. Numerous sensing devices are used to gather patients' information, generating a large volume of data. The traditional applications and algorithms are not efficient in processing and managing the patients' data, which presents a challenge. Much research on the Internet of Things in healthcare focuses mainly on hospitals with little focus on care homes. This research uses care homes as a case study as these are regarded as the homes of service users for an extended period of time, much longer than the time they spend in hospitals. This research proposes a system that would enable healthcare staff to monitor the pressure sores in service users with low mobility and provide them with a secured system against attacks from cyber criminals. The system implements the use of sensors to monitor pressure exerted from bedridden service users in real-time using ThingSpeak, provides a secure system by implementing two-factor authentication (2FA) for caregivers for safe login, transmitting data securely over a safe network using raspberry pi 4 as the edge devices, and applying machine learning to help monitor the network for intrusion detection from hackers. With the current gap in research in care homes, this paper emphasises the need for the adoption of real-time monitoring and having a secured system framework for care homes to improve their services provided.**

Keywords – Internet of Things, IoT Security, Edge devices, Esp8266, Embedded Systems, Bedsores, IoT Healthcare.

I. INTRODUCTION

A. Importance of IoT In Healthcare

The Internet of Things (IoT) is a concept that is believed to be the future of the Internet. It is the interconnectivity of devices with humans, thereby linking the virtual world with the physical world and is seen as a massive network of things: people-to-people, people-to-devices, devices-to-devices [1]. Communication in IoT thrives from the constant advancements in Wireless Sensor Networks (WSN), Radio Frequency Identification (RFID), Mobile Communication, Cloud technology, among a few others. IoT has hugely helped advance people's standard of living and made life easier as devices and the different sectors of life are adopting smart technology. With the rapid adoption in the utilization of IoT applications, CompTIA predicted that roughly 50.1 billion devices would be connected to the Internet by 2020 [2] of which the number of devices connected to the internet has increased. The Internet of Things has in recent years become the key focus of research as millions of devices are becoming intelligent and being used in different fields such as healthcare, business, security, schools, asset tracking, agriculture, automobiles, smart cities, smart homes, smart metering [3].

The architecture of an IoT system is made up of a variety of layers built with sensors and actuators embedded as part of their structure. While the sensors gather information from its surroundings and process this data to produce useful information, actuators, on the other hand, adjust or modify the condition of their environment based on the information received from the sensors. Some examples include transceivers, thermometers, thermostats, cloud administrations, etc. With the accelerating growth and rapid adoption and use of these smart devices, the security of the sensitive data being shared, the applications and platforms on which they are used becomes top priority to avoid data being compromised. From a functionality and implementation point of view, the IoT systems architecture should be built with a very high and secure level of cryptographic abilities to ensure data authentication, integrity, confidentiality, and validation. Systems having these security features would be protected against all forms of attacks from hackers and cybercriminals that target vulnerable systems with low security.

The constant expansion and growth of the Internet of Things has led to the emergence of Edge Computing. Quite a high number of IoT edge devices that are used very often have high vulnerabilities, and users of these devices are advised to use the inbuilt security features in each device to avoid cyber-attacks [4]. This paper presents an overview of the IoT systems architecture, IoT enabling technology, and its security at the edge. We focus on the application of IoT in healthcare by monitoring pressure sores in patients with low mobility.

The rest of this paper is organized as follows: Section II discusses the literature review of IoT security in healthcare. Section III is the methodology. Section IV addresses the experimental setup. Section V presents the conclusion and future work.

 ISBN: 978-1-61208-893-8

B. Monitoring Pressure Sores

Pressure sores, also called bedsores, are known as injuries to the skin and the underlying tissues due to continuous pressure being applied on the skin for a prolonged period, which results in a shortage of blood flow. This pressure occurs most of the time around parts of the body that are quite bony and prone and faced with continuous friction, immobilization, and malnourishment [5]. Pressure sores have long posed a massive burden in healthcare [6]. People at risk of developing pressure sores are mostly the elderly, disabled patients in wheelchairs, and bedridden patients in hospitals and care homes. In care homes, high profile beds are used especially for patients that are prone to bedsores. Pressure relief cushions are used in chairs and wheelchairs as well to help relieve pressure when sitting.

While in bed, hourly repositioning is done for patients to relieve pressure on the sides laid. It is also done when patients sit in their recliners and wheelchairs; these actions are known as pressure relief mechanisms. Patients are assisted to stand up for a few minutes and if they can, take a short walk to help relieve the pressure that has built up while they were seated for a while. Barrier creams are also regularly applied to the pressure points to protect the skin and act as a barrier. Moody et. al. [7] proposed a platform that shows the pressure distribution map of the body, collects information from sensors embedded in the patient's bed, has the data analysed to create a timestamp, and has the actuators readjust its surface profile to make sure pressure is distributed all over the body.

Different solutions have been proposed to reduce bedsores, like smart beds, sensors, and artificial intelligence to monitor the whole body lying in bed or sitting in a chair. Nair et al. [8] proposed a smart air mattress that can inflate and deflate, thereby relieving the body pressure. Benet et al. [9] also proposed an algorithm that automatically detects parts of the body that have been relieved by pressure points from under a supine subject without assumptions or input by users.

II. 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 as carried out by [10], but there has been little research on implementing a more secured IoT system. Most care homes do not implement two-factor authentication (2FA) to ensure a more secure system, and it is just staff login details that grant them access to the system. This is not very safe and can be very detrimental should a third party hack the system and steal or alter patient's information; that is what this research is focusing on, providing a 2FA system for more security and providing a more secure system while transmitting these patients' data using edge devices. [11] presented the main problems facing narrowband IoT (NBIoT) currently and presented some solutions to help tackle these challenges. [12] addressed the important areas of IoT technologies for smart sensors, big data analytics and advanced health care systems. They used various case studies to identify possible perspectives by highlighting ongoing research issues like interoperability, scalability, security, and device-network-human interfaces. [13] focused on the applications and networks of IoT devices in healthcare, attacks on these devices, the security requirements for the IoT systems, and the organizational approach towards the development and implementation of IoT security. [14] investigated the current IoT security and privacy requirements and provided a new framework that sorts out all aspects of these security and privacy measures, requirements, and recommendations in healthcare. [15] shed light on the importance of IoT-based elderly healthcare systems and their classification by reviewing different research studies focused on developing and utilising these systems. This research also addressed the security and architecture of IoT systems in healthcare and how they are implemented in the home and hospital. [16] designed a system for smart homes to assist care for people with special needs for a prolonged period. The system tracks and analyses how residents behave at different time intervals and provide caregivers with reports and alerts. [17] proposed a novel healthcare IoT system model that provides information on the current health status of patients. Using a Raspberry Pi 3, patients can get an immediate response about hospitals close to them and if the physicians are available to see them. [18] proposed a multi-agent approach to advanced continuous threat detection using machine learning for predictive analysis in identifying security vulnerabilities and patterns to make predictions and recognize outliers.

A. IoT Systems

The IoT systems involve simple, smart devices ranging from wearables to more complex systems such as the recently developed self-driving cars. These devices aim to bring more comfort to the lives of people. IoT systems have improved the quality of life of people greatly. It has made room for everything around us to be automated. Every sector of life uses IoT to improve the services they provide [19]. A combination of all these smart systems gave rise to smart

 ISBN: 978-1-61208-893-8

healthcare, smart transportation, smart homes, and smart industries.

B. Security Issues in Internet of Things (IoT)

With the security of the IoT being a top priority, many researchers propose different solutions using different technologies to help reduce cyberattacks [20]. Many research projects have been carried out to address the modelling of the system, its design, setup and the IoT enabling technologies that allow for the proper functioning of the system and, most importantly, its security. The continuous integration of IoT and its applications has drawn attention to several security issues which should be addressed. 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. Hewlett Packard, in a survey, stated that a high percentage of IoT devices that are often used are vulnerable and defenceless to attacks [21]. 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.

Some of the main security issues in IoT include Botnet, Malware attacks, Man-in-the-Middle attacks, and Denial of Service attacks [22]. 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 [23]. Security in IoT is crucial and needs to constantly be maintained to protect the billions of devices connected to the Internet.

The design of the IoT system should involve the following security features:

- Confidentiality
- Integrity
- Authenticity
- Authorization
- Availability

C. Edge Devices in Healthcare

IoT in healthcare consists of edge devices used to sense and process data. These edge devices connect a very high number of sensing devices that are smart [24]. They come between the source of information and the cloud [25]. Edge devices provide healthcare with smart systems that allow for speedy health diagnosis and help in providing precise, effective treatments. IoT sensors and its healthcare applications have greatly changed and improved the healthcare approach, with the number of IoT healthcare devices estimated to be more than 162 billion in the year 2020 [26]. The structure of Edge-based IoT healthcare has aided remote monitoring with the help of smart sensors for patients. Data obtained from sensors are sent over to the edge devices for prepossessing before they can be trained using machine learning to also help in monitoring illnesses in real-time and treat these diseases. Solutions for remote monitoring of patients in real-time and the secured transmission of their health reports have for many years been the main area of research for health researchers [27]. [28] suggested the use of computers and microcontroller-based monitoring systems like the electrocardiogram (ECG) and heartbeat sensors to monitor the heartbeat and notify high heart rate. Because of their limited resources, Edge devices are quite vulnerable to different types of threats that could affect their performance. Hence, the cryptographic algorithms should be deployed to increase security.

D. Embedded Devices and Edge devices in IoT

Edge Computing means data being processed at the edge of a network as close to the source of data as possible. It is the expansion of the Internet of Things that led to Edge Computing. Commonly, edge devices are regarded as microcontroller-based systems [29]. As data is being collected from various IoT Edge devices, it is first pre-processed before it is sent to the cloud. Unlike the centralized cloud computing, edge computing is a distributed architecture even though it is based on cloud technologies. With traditional cloud computing being centralized and having all its computation and storage done in a single data centre, it faces some limitations with the continuous emergence of new technology that needs low latency, real-time response and decision making. This is where edge computing comes into play as it is used to improve cloud computing [30]. Data generating devices are considered edge devices. Edge devices in the IoT context are mostly microcontroller-based systems that are resource-constrained and are short of memory and computing power, and they could also be remotely located, meaning they need to optimize their power consumption as they rely on small batteries. Some embedded devices in IoT include Raspberry pi, Jetson Nvidia, etc.

Edge devices directly interact with the physical environment by using RFID tags, sensors, actuators, and embedded devices. The edge layer, which is a critical component of IoT application, is a major target to attackers as they try to gain access to the whole system in the bid to take it down. Figure 1 below shows the architecture of edge devices.

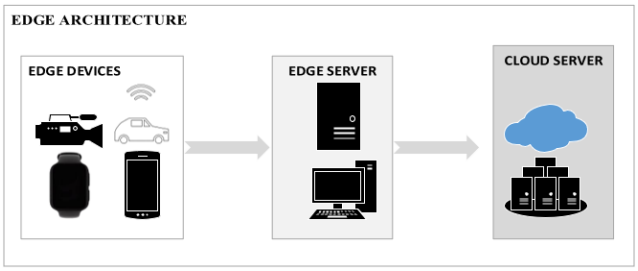

Figure 1. Edge Architecture

E. Security at the Edge in Healthcare

Statistics published a few years back showed that one sector that faced the highest level of threat was the health sector [31]. Security and privacy are major concerns to the security of patient's data. The slightest form of attacks on both patients' personal data, tampering with their medication

 ISBN: 978-1-61208-893-8

file, can be catastrophic to the patient and life-threatening [32]. Because of these security concerns, ongoing research on data security concentrates mainly on developing and implementing encryption, authentication, and solutions for wearable and implantable devices [33]-[35]. [36] evaluated a case study for patient biosignal data and designed a structure that uses edge devices to process the data sent to the cloud and enhance the processing and response time while maintaining a very high-level accuracy and data privacy.

F. Artificial Intelligence (AI) Tools For IoT Security in Health Care

Artificial Intelligence is a combination of different technologies. AI in healthcare deploys different software and algorithms to emulate human intelligence to process complex medical data and carry out analysis, tasks, reasoning, detecting patterns and solve problems with no direct human input [37]. AI has brought a massive change in diagnosing diseases, patient care and medical analysis [38]. Since its adoption in healthcare, AI has proven to be the most efficient technology used to process big data and enabling results analysis in real-time [39]. Some of the AI tools for security in healthcare are Machine Learning, Deep Learning, Big Data, Cloud Technology [40] and Blockchain. Based on research conducted, many papers use deep neural networks to tackle privacy and security in healthcare systems [41].

- Machine Learning is an aspect of artificial intelligence that uses intelligent software to enable machines to work effectively. Training models in machine learning are Supervised and Unsupervised. Some of the ML algorithms are Decision Trees, support vector machine (SVM), K-Nearest Neighbour (KNN), Logistic Regression (LR), Naives Bayes, Discriminant Analysis. Popular software used for ML is MATLAB.
- Deep Learning can be defined as learning by example using neural network architecture. It is a specialized ML technology where computer models are trained to classify data given such as images, sounds and texts and, with a result, achieve a high level of accuracy.
- Big Data is a huge amount of data gathered from billions of IoT devices. Analysts expend these gathered data, and valuable information retrieved and conveyed to organizations. This valuable dataset can affect an organisation's decision-making strategies, hence the need to employ advanced technology to help manage the high volume of data.
- Cloud Technology can be used to store data that is easily accessed over the Internet or network. Cloud Computing works with smart devices such as sensors and allows this sensing data to be saved and used for intelligent monitoring and actuation.
- Blockchain technology allows the storage and exchange of data based on peer-to-peer (P2P) network. Blockchain is open-ended and its operation is decentralised.

III. METHODOLOGY

The research adopted in this investigation consists of investigating IoT, edge computing, security in IoT and on edge, and experimentation to evaluate a secured IoT system. A combination of qualitative and quantitative research will inform the design of such IoT systems for healthcare applications.

A. Qualitative Research

A survey was carried out in care homes, and this was aimed at nurses and carers who work with elderly patients who are prone to developing pressure sores. This survey aimed to identify the gap in knowledge in the use and adoption of IoT in healthcare to help reduce the occurrence of bedsores and the need for IoT systems and security. The following information was gathered to help gain a better understanding of the current situation;

- The time intervals that service users are turned to prevent sores from developing
- If pressure sores are monitored in real-time
- How the patients' data are viewed and logged
- Security measures currently in place
- The security measure that they would be applied to prevent attacks and detect intrusion.

Below shows some feedback from the survey conducted:

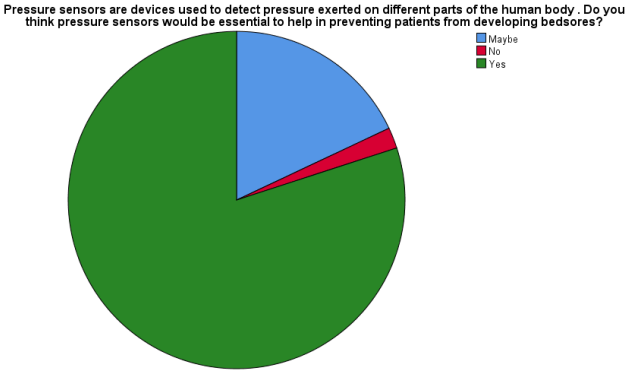

Figure 2a. Adoption of pressure sensors monitoring

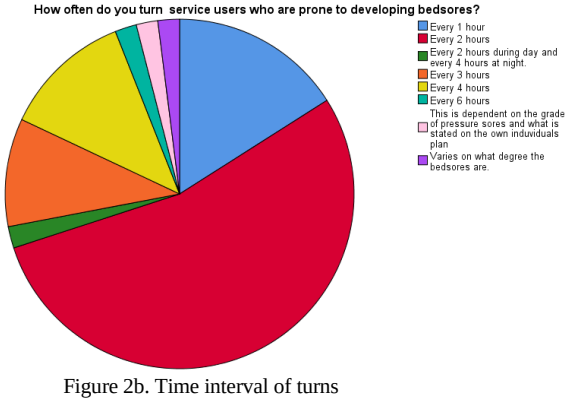

Figure 2b. Time interval of turns

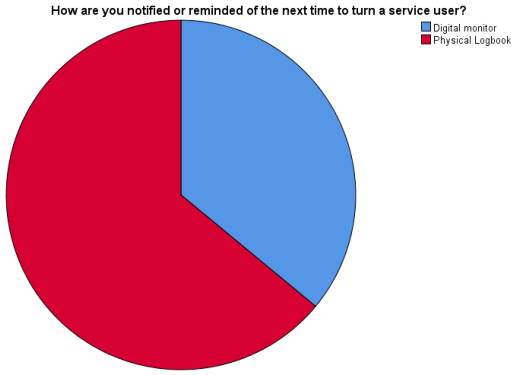

Figure 2c. Paper-based reminder of turn times

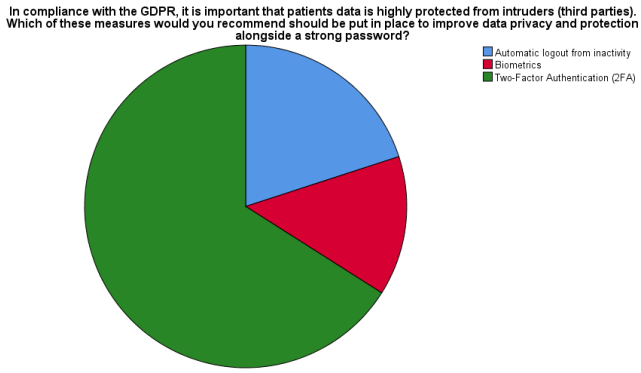

Figure 2d. Preference of the Two-factor authentication implementation

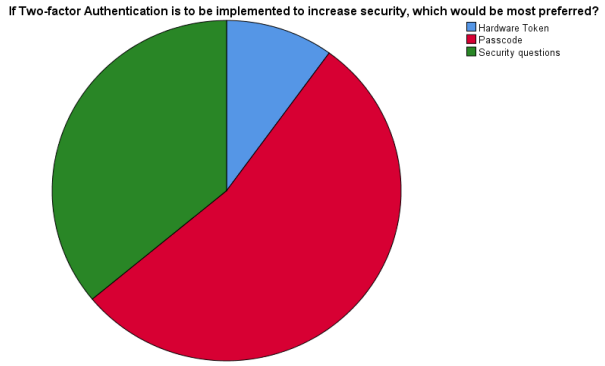

Figure 2e. Preference of the passcode for the two-factor authentication

Many healthcare staff are used to the traditional method of periodically checking on the patients and turning them. Many times, these patients are turned even before the next expected reposition time. Moreover, with this constant turn, not to forget, these carers hurt their backs with the frequent bending positions while repositioning patients. An IoT system in place would save the health staff time of checking patients' position and the level of pressure being exerted by different parts of the body, but they would be able to monitor the pressure being applied on the skin in real-time.

B. *Quantitative Research*

With the information gathered from the survey, experiments would be 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.

IV. EXPERIMENTAL SETUP

The IoT based system would enable the healthcare staff to monitor patients' vitals in real-time. This system will help prevent sores from developing in these patients. Different service users are turned at different time intervals depending on the skin's vulnerability to developing sores, everyone hour, two hours, or three hours, but the most common is two-hourly turns. Certain parts of the body are more prone to sores than other parts. The pressure sores monitoring system would monitor the pressure exerted in real-time on the ThingSpeak network so the health staff can keep track of the pressure being exerted on that part of the body and reposition the patient as needed. This system is designed to gather, process, store and analyze the data.

The system consists of the pressure sensors, LED, Arduino UNO, Esp8266 and ThingSpeak network cloud platform.

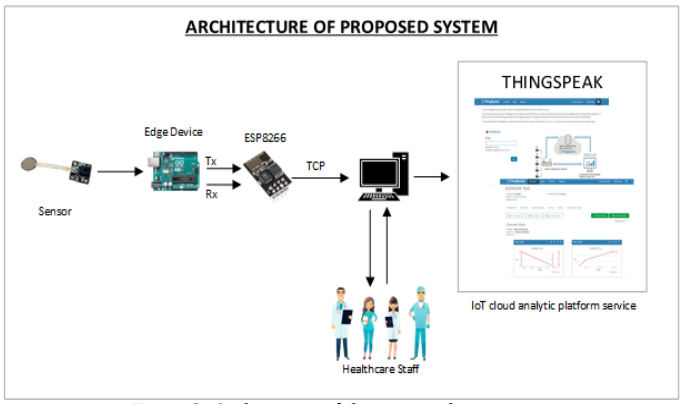

Figure 3. Architecture of the proposed system.

A. *Obtaining sensing data*

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.

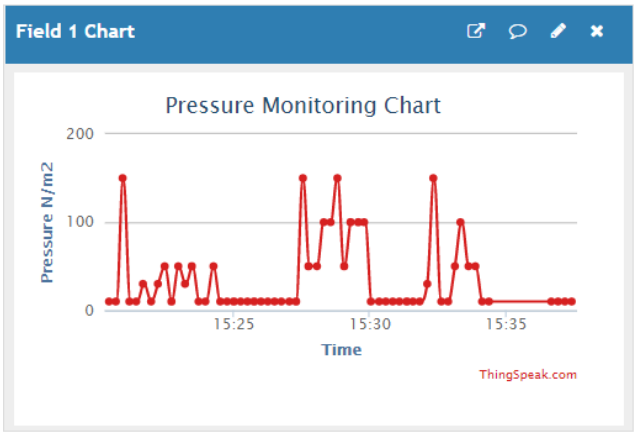

Figure 4. Real time pressure monitoring on ThingSpeak

B. *Creating a Secured Website and Implementing the Two-Factor authentication (2FA).*

A webpage was designed where the 2FA would be required to get into the system. The staff would need an authentication code to log into the system not just the traditional login method involving staff email and password. The authentication code was used based on the feedback that was received from the survey that was conducted.

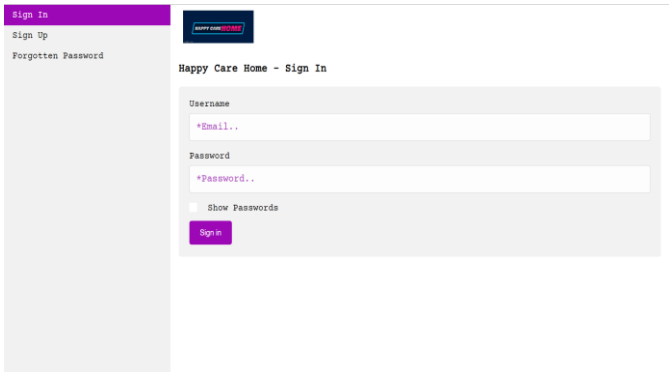

Figure 5. Staff login page

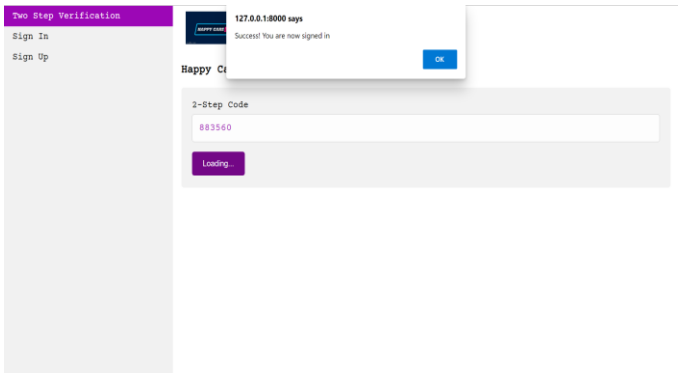

Figure 6. Authentication page

C. *Obtaining the data from ThingSpeak and applying ML*

The sensor will be connected to the edge device, which would transmit the data safely over the network through the transceiver ESP8266, acting as a gateway to ThingSpeak. ThingSpeak provides a secured Transport Layer Security (TLS) protocol. The data obtained would be used in MATLAB to train the model to detect intrusion. To test that the system is functioning, unauthorized access data would be injected into the system for intrusion detection.

V. CONCLUSION AND FUTURE WORK

In this paper we present our research on the IoT application in care homes. The care staff are still using the traditional paper-based methods of logging patients' data as evident from the survey conducted. 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.

REFERENCES

[1] A. Iwayemi, "Internet of Things: Implementation Challenges in Nigeria", American Journal Of Engineering Research (AJER), Volume-7(Issue-12), pp-105-115, 2018. Available from http://www.ajer.org.

[2] CompTIA | Sizing Up the Internet of Things. 2015 Available from https://www.comptia.org/content/research/sizing-up-the-Internet-of-things.

[3] K. Mekki, E. Bajic, F. Chaxel, and F. Meyer. "A comparative study of LPWAN technologies for large-scale IoT deployment", ICT Express. 2019;5(1):1-7

[4] M. Abomhara and G.M. Køien, "Security and privacy in the Internet of Things: current status and open issues", IEEE International Conference on Privacy and Security in Mobile Systems (PRISMS), 201433

[5] G. Brandeis, W. Ooi, M. Hossain, J. Morris, and L. Lipsitz, "A longitudinal study of risk factors associated with the formation of pressure ulcers in nursing homes", J Am Geriatr Soc, vol. 42, pp. 388-393, 1994.

[6] F. Boussu, V. Koncar and C. Vasseur, "Novel approach of ulcer prevention based on pressure distribution control algorithm", in Proc IEEE Mechatronics and Automation, pp. 265-270, August 2011.

[7] B. Moody, J. Fanale, M. Thompson, D. Vaillancourt, G. Symonds, and C. Bonasoro, "Impact of staff education on pressure sore development in elderly hospitalized patients", Arch Intern Med, vol. 148, pp. 2241-2243,1988.

[8] P. Nair, S. Mathur, R. Bhandare and G. Narayanan, "Bed sore Prevention using Pneumatic controls", 2020 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT), 2020. Available: 10.1109/conecct50063.2020.9198410

[9] S. Bennett, R. Goubran, K. Rockwood and F. Knoefel, "Monitoring the relief of pressure points for pressure ulcer prevention: A subject dependent approach", 2013 IEEE International Symposium on Medical Measurements and Applications (MeMeA), 2013. Available: 10.1109/memea.2013.6549722.

[10] G. Manogaran, N. Chilamkurti and C. Hsu, "Emerging trends, issues, and challenges in Internet of Medical Things and wireless networks", Personal and Ubiquitous Computing, vol. 22, no. 5-6, pp. 879-882, 2018. Available: 10.1007/s00779-018-1178-6 [Accessed 10 September 2021].

[11] S. Anand and S. K. Routray, "Issues and Challenges in Healthcare Narrowband IoT", in International Conference on Inventive Communication and Computational Technologies (ICICCT 2017), 2017, pp. 486 - 489.

[12] F. Firouzi, B. Farahani, M. Ibrahim and K. Chakrabarty, "Keynote Paper: From EDA to IoT eHealth: Promises, Challenges, and Solutions", IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 37, no.

 ISBN: 978-1-61208-893-8

12, pp. 2965-2978, 2018. Available: 10.1109/tcad.2018.2801227.

[13] S. El-Gendy and M. Azer, "Security Framework for Internet of Things (IoT)". 15th International Conference on Computer Engineering and Systems (ICCES), pp. 1-6, 2020. Available: doi: 10.1109/ICCES51560.2020.9334589

[14] E. Fazeldehkordi, O. Owe and J. Noll, "Security and Privacy in IoT Systems: A Case Study of Healthcare Products", 2019 13th International Symposium on Medical Information and Communication Technology (ISMICT), 2019, pp. 1-8, doi: 10.1109/ISMICT.2019.8743971

[15] M. Elkahlout, M. M. Abu-Saqer, A. F. Aldaour, A. Issa and M. Debeljak, "IoT-Based Healthcare and Monitoring Systems for the Elderly: A Literature Survey Study", 2020 International Conference on Assistive and Rehabilitation Technologies (iCareTech), 2020, pp. 92-96, doi: 10.1109/iCareTech49914.2020.00025.

[16] C. Coelho, D. Coelho and M. Wolf, "An IoT smart home architecture for long-term care of people with special needs", 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), 2015, pp. 626-627, doi: 10.1109/WF-IoT.2015.7389126.

[17] S. Yattinahalli and R. M. Savithramma, "A Personal Healthcare IoT System model using Raspberry Pi 3", 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), 2018, pp. 569-573, doi: 10.1109/ICICCT.2018.8473184.

[18] Á. MacDermott, P. Kendrick, I. Idowu, M. Ashall and Q. Shi, "Securing Things in the Healthcare Internet of Things", 2019 Global IoT Summit (GIoTS), 2019, pp. 1-6, doi: 10.1109/GIOTS.2019.8766383.

[19] K. Jaiswal, S. Sobhanayak, A. Turuk, B. SahooL, B. Mohanta and D. Jena, "An IoT-Cloud based smart healthcare monitoring system using container based virtual environment in Edge device", in Proceedings of 2018 International Conference on Emerging Trends and Innovations in Engineering and Technological Research (ICETIETR), 2021, pp. 1-6.

[20] O. Alfandi, S. Khanji, L. Ahmad and A. Khattak, "A survey on boosting IoT security and privacy through blockchain", Cluster Computing, vol. 24, no. 1, pp. 37-55, 2020. Available: 10.1007/s10586-020-03137-8.

[21] Hewlett-Packard Enterprise Development LP HP P-Class Smart Array Gen9 RAID Controllers. Citeseerx.ist.psu.edu. from http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.729.9133.

[22] S. Okul and M. Ali Aydin, "Security Attacks on IoT", 2017 International Conference on Computer Science and Engineering (UBMK), pp. 1-5. Available: 10.1109/UBMK.2017.8093577

[23] R. Gurunath, M. Agarwal, A. Nandi and D. Samanta, "An Overview: Security Issue in IoT Network". IEEE Xplore, (978-1-5386-1442-6), 2018, pp. 104-107.

[24] J. Li et al., "A Secured Framework for SDN-Based Edge Computing in IoT-Enabled Healthcare System", IEEE Access, vol. 8, pp. 135479-135490, 2020. Available: 10.1109/access.2020.3011503

[25] R. Anusuya, D. Karthika Renuka and L. L.Ashok Kumar, "Review on Challenges of Secure Data Analytics in Edge Computing", in 2021 International Conference on Computer Communication and Informatics (ICCCI -2021), Jan. 27 – 29, 2021, Coimbatore, INDIA.

[26] A. O. Akmandor and N. K. Jha, "Smart health care: An edge-side computing perspective", IEEE Consum. Electron. Mag., vol. 7, no. 1, pp. 29–37, Jan. 2018.

[27] S. Amin and M. Hossain, "Edge Intelligence and Internet of Things in Healthcare: A Survey", IEEE Access, vol. 9, pp. 45-59, 2021. Available: 10.1109/access.2020.3045115

[28] Y. Hao, Y. Miao, L. Hu, M. S. Hossain, G. Muhammad, and S. U. Amin, "Smart-edge-CoCaCo: AI-enabled smart edge with joint computation, caching, and communication in heterogeneous IoT", IEEE Netw., vol. 33, no. 2, pp. 58–64, Mar. 2019

[29] S. Shapsough, F. Aloul and I. Zualkernan, "Securing Low-Resource Edge Devices for IoT Systems", 2018 International Symposium in Sensing and Instrumentation in IoT Era (ISSI), 2018. Available: 10.1109/issi.2018.8538135.

[30] I. Sittón-Candanedo, R. Alonso, J. Corchado, S. Rodríguez-González and R. Casado-Vara, "A review of edge computing reference architectures and a new global edge proposal", Future Generation Computer Systems, vol. 99, pp. 278-294, 2019. Available: 10.1016/j.future.2019.04.016.

[31] IBM 2016 Cost of Data Breach Study United States, I. Corp,Washington, DC, USA, Sep. 2016. https://resources.idgenterprise.com/original/AST-0185855_SEL03094USEN.PDF

[32] G. Thamilarasu, A. Odesile and A. Hoang, "An Intrusion Detection System for Internet of Medical Things", IEEE Access, vol. 8, pp. 181560-181576, 2020. Available: 10.1109/access.2020.3026260.

[33] R. V. Sampangi, S. Dey, S. R. Urs, and S. Sampalli, "A security suite for wireless body area networks", 2012, arXiv:1202.2171.[Online].Available:http://arxiv.org/abs/1202.2171

[34] A. S. Sangari and J. M. L. Manickam, "Public key cryptosystem based security in wireless body area network", in Proc. Int. Conf. Circuits, Power Comput. Technol., Mar. 2014, pp. 1609_1612.

[35] W. Li and X. Zhu, "Recommendation-Based Trust Management in Body Area Networks for Mobile Healthcare", 2014 IEEE 11th International Conference on Mobile Ad Hoc and Sensor Systems, 2014, pp. 515-516, doi: 10.1109/MASS.2014.85.

[36] A. Alabdulatif, I. Khalil, X. Yi and M. Guizani, "Secure Edge of Things for Smart Healthcare Surveillance Framework", IEEE Access, vol. 7, pp. 31010-31021, 2019. Available: 10.1109/access.2019.2899323.

[37] N. Al-Milli and W. Almobaideen, "Hybrid Neural Network to Impute Missing Data for IoT Applications", 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), 2019. Available: 10.1109/jeeit.2019.8717523.

[38] W. Almobaideen, R. Krayshan, M. Allan and M. Saadeh, "Internet of Things: Geographical Routing based on healthcare centers vicinity for mobile smart tourism destination", Technological Forecasting and Social Change, vol. 123, pp. 342-350, 2017. Available: 10.1016/j.techfore.2017.04.016.

[39] C. Ieracitano et al., "Statistical Analysis Driven Optimized Deep Learning System for Intrusion Detection", Advances in Brain Inspired Cognitive Systems, pp. 759-769, 2018. Available: 10.1007/978-3-030-00563-4_74..

[40] S. Gopalan, A. Raza and W. Almobaideen, "IoT Security in Healthcare using AI: A Survey", 2020 International Conference on Communications, Signal Processing, and their Applications (ICCSPA), pp. 1-6, 2021. Available: 10.1109/iccspa49915.2021.9385711.

[41] P. Ghosal, D. Das and I. Das, "Extensive Survey on Cloud-based IoT-Healthcare and Security using Machine Learning", 2018 Fourth International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN), pp. 1-5, 2018. Available: 10.1109/icrcicn.2018.8718717.