

# Strengthening IOHT security by multi factor authentication solutions and with future directions.

MSc Research Project  
Masters in Cyber security

Pankaj Ramcharitra Yadav  
Student ID: X23205458

School of Computing  
National College of Ireland

Supervisor: Joel Aleburu

**National College of Ireland**  
**MSc Project Submission Sheet**  
**School of Computing**



**Student Name:** Pankaj Ramcharitra Yadav  
.....  
X23205458  
**Student ID:** .....  
2024  
**Programme:** Masters in Cyber Security **Year:** .....  
.....  
Practicum  
**Module:** .....  
Joel Aleburu  
**Supervisor:** .....  
**Submission Due Date:** 12/12/2024  
.....  
**Project Title:** Strengthening IOHT security by multi factor authentication solutions  
and with future directions  
.....  
6636 20  
**Word Count:** ..... **Page Count** .....

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

**Signature:** Pankaj  
.....  
12/12/2024  
**Date:** .....

**PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST**

Attach a completed copy of this sheet to each project (including multiple copies)	<input type="checkbox"/>
<b>Attach a Moodle submission receipt of the online project submission,</b> to each project (including multiple copies).	<input type="checkbox"/>
<b>You must ensure that you retain a HARD COPY of the project,</b> both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	<input type="checkbox"/>

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

<b>Office Use Only</b>	
Signature:	
Date:	
Penalty Applied (if applicable):	

# Strengthening IOHT security by multi factor authentication solutions and with future directions

Pankaj Ramcharitra Yadav

X23205458

## Abstract

The advancement of Internet of things has changed healthcare sector by providing remote monitoring, real time data collection, online treatment and better patient management. This Internet of health care things include medical devices, sensors and cloud computing for collecting and monitoring patient's health record. However, weak authentication systems are facing significantly security risks such as data breaches and unauthorized access. This research investigates the integration of multi factor authentication using AWS services such as identity and Access management (IAM) and Key management services (KMS) to enhance the data protection and security in the internet of health care things. The implementation aims to safeguard sensitive information of health care thing, build trust and improve overall security performance.

Keywords: Internet of health care things, multifactor authentication and Amazon Web Service

## 1 Introduction

The rapid growth of technologies and its advancement has given rise to a new aspect of health care sectors are called as internet of health care things. This includes combinations of sensors with the latest technology to process health records of the patients. Without involvement of internet of things in health care sectors, the patients were using traditional systems such as visiting clinics. In today's world, there are lots of patients and it's impossible for doctors to remember everyone and keeping tracks of their health record. However, after the involvement of internet of things in health care sectors it has been changed and it reduces the work load on health care sectors (Suhail Javed Quraishi et al.,)

Internet of health care things provides multiple benefits for health care professionals to monitor patient's data and also monitored their health record by themselves. The most common benefits of IOHT are to automatically collect health data of those are not able to present physically in a healthcare facility. This technology has become demanding application for healthcare professional to manage and keep track of patient's health record (Huang et al., 2023).

Internet of things are expanding in health care things with the help of medical devices and the sensors to the internet because it continuously collecting and monitoring patient's health records. However, remotely patient monitoring is the most common application of internet of things and when it collects their data and it forwards that data to a software application where health care professionals and patients can view it. Patients can take online appointment for their health concerns and their data will store automatically; this will help doctors for their next appointment. Moreover, internet of health care things will help patients those are suffering from chronic disease and professional can monitored their them even if they are at

their home. It can also help if the patients need immediate medical attention or ambulance to reach hospital and this IOHT will improve the communication between the ambulance and the patients before arriving at the hospital (Guo et al., 2024).

Internet of health care things provides numerous benefits for healthcare professional and patients with the help of internet of things wearable, but they are also associated with risk and challenge including potential hacking of systems and patients' records (Shahmiri, 2016). This wearable device and their connections are the key concept of the health care sectors. The internet of health care things is at the risk of security attack and the attacker is exploiting with the help of vulnerabilities to gain unauthorized access and this access led to data breaches (Alsubaei, F et al., 2019). The health sectors will have to face some financial losses and reputational damage. This main cause of the exploitation is that weakness in the security systems and most of them are rely on single factor authentication (Guo et al., 2024).

The improvement in the security of the health care things is an important because it contains a lot of data of health sectors and they are totally dependent on this technology. However, to protect the health care sectors is by using multi factor authentication as it provides solutions to verify the user identity with the help of different methods such as one time password or by biometrics. The multi factor authentication will add different layer of security and which make it harder for an attacker to gain unauthorized access (Jawad et al., 2022).

To overcome from security attacks, it is essential to implement strong authentication mechanism and Amazon web services provides a comprehensive security tools for safeguarding internet of health care things. With the help of AWS services such as Identity and Access Management (IAM), Key management services (KMS) and multi factor authentication in internet of health care things only authorized person can gain access to sensitive patients' data. In addition, AWS framework also includes threat detection and data encryption which will additionally layer of protection for that data that is transmitted by internet of health care devices.

By using Amazon Web service will make it strong authentication which make it more secure and trustworthy ecosystem for healthcare sectors. This will not only reduce the risk of unauthorized access but also compliance with stringent regulations like HIPAA (Health Insurance Portability and Accountability Act). As a result, AWS based multi authentication solutions play an important role in securing Internet of health care things and patients' data.

## **2 Problem Statement**

The internet of health care things includes sensors, medical devices and cloud technologies to enhance healthcare sectors by providing remote patients monitoring, real-time data and better facilities. Despite of these growth, Internet of health care things are facing security challenges such as safeguarding patient's data and preventing unauthorized access. After reviewing some literature, I have formulated the following research questions.

Secure web development – There is a lack of secure web platforms that facilitate seamless interaction between patients and doctors and current authentication depend on single factor authentication which increase the risk of unauthorized access.

Enhancing IOHT security- The internet of health care things generates a large amount of sensitive data and without robust security such as multi factor authentication, Internet of health care things (IOHT) systems remain vulnerable to data breaches and privacy violations.

**AWS Integration for Robust Security-** A lot of IOHT systems lack scalable and reliable solutions to manage authentication and data encryption. By integration of Amazon Web Service (AWS) including Identity and Access Management (IAM) and Key Management Service (KMS) provides an opportunity to implement security frameworks for Internet of health care things platforms.

I am going to develop a secure website for patients and doctors which integrated with IOHT systems to enhance the user experience and by implementing multifactor authentication using AWS service to strengthen security, protect sensitive data and build a reliable platform for future advancement in IOHT security.

### **3. Literature Review**

While doing research on Internet of healthcare things, I followed a review by Suhail Javed Quraishi and Humra Yusuf (2021) and this review shows both benefits and challenges faced in Internet of health care things during this research. There are various ways by which Internet of health care things can improve by real time patients monitoring, online appointment and access to health data. The health care methods based on internet of things has benefited by improving patient's health and there are millions of patients who are using this technology. This technology has widespread in surgical, endoscopic, orthopedic and etc. (Quraishi and Yusuf,2021).

There are various applications of Internet of things and these are successfully used in health care fields. A notable example of IOHT application is the development of a mobile based applications for the health care sectors and it uses the technology of internet of things and cloud computing. They build ECG android application and in this application the data is uploaded by the patient's end to user private centralized cloud (Junaid Mohammed Mohammad, et al., 2014). These devices are providing much effective services to healthcare professionals and to the patients. But there are some essential challenges need to address to make Internet of health care things more effective and secure. The major problem is the vulnerability of patient's data because internet of health care things is developed to collect and share patients' data with less security. This gives a chance for cyber attackers to gain unauthorized access to sensitive patient's data. There are various health care devices which have limited processing power and this cannot support advanced encryption or security protocols and this leads to exposed of patient's data for data breaches (Jawad et al., 2022).

Another problem is that managing secure access in different connected devices and there are many Internets of health care devices such as wearable devices and to remote patients monitoring. It is very difficult to consider that each and every device has strong security measures and if there will be any one unsecure device left, it will put whole network at risk. There are various devices in Internet of health care and it is very difficult to improve security of each and every device on internet of things. Many devices are there which are not updated because they are not in use for a longer period of time and if they will use these devices, it will become more vulnerable to security issues. These lack of software updates on internet of healthcare devices can lead to attacks and there will be chance of increasing risk on patient's data. Higher amount of data is generated by internet of devices and this data needs more careful management and security measures. Hospitals and health care providers must handle this data by confidentiality and also used for treatment and monitoring.

In their review, Huang, Wang and Zhang explored Internet of medical thing's structure and application for health care and explained how internet of medical things has helping in the medical field. The Internet of medical things refers to the connection of medical devices with the help of internet and allowing to their share their data. There are various devices such as wearable sensors and diagnostic tool and by the combination of these devices they form a network which helps doctors and health care professionals to monitor and treat patients. Also, researcher studied the role of internet of medical things in healthcare things and explained how it is changing the way of medical care is delivered. Internet of medical things is made of various layers that work together and there are various sensors and devices that collect health records of patients such as heart rate, body temperature and monitoring them. Once the data is collected it will send to the next layer called gateway layer and form them it will transmit to the cloud. The cloud layer stores and process the data and then it will make available for patients and for doctor professional. In the end, the application layer is located which analysed the data and used for decision making. This layer helps the doctors to get information about patient's health even if they are at their home.

The researcher explained how internet of medical things is using for remote monitoring and smart hospitals. It will help doctors and healthcare professionals to find the actual disease of the patients and also how treatment is working. With the help of these data, healthcare professionals are able to make faster decision for the patient's treatment (Huang et al.,2023). They also talked about the latest technologies that will make internet of medical things possible with the help of artificial intelligence, block chain and cloud computing. For a device authentication they proposed a scheme for the internet of medical things environment by using physical unclonable functions and this method used hybrid oscillators to ensure that no data is stored in server memory (Yanambaka, et al., 2019). With the help of artificial intelligence, professionals will analyze large amount of health data collected by internet of medical care devices. Block chain will keep patient data secure and with the help of cloud computing they will share real time data.

There are various benefits of Internet of medical things, but the researchers have noted few challenges during their research. The biggest problems is that security and privacy of the data that has been collected by these devices because medical and patient's data are so sensitive and therefore it should be protected. Also, they believe there will be some improvements in the future for security because it will make internet of medical things more useful for patients and the doctors.

The internet of things has dramatically changed the way of technology is used in various fields including health care sectors. This gives rise to the concept of smart health care or electronic health care which use the internet of things technologies to enhance the medical services and to improve the performance of overall health care sectors. This can be achieved by real time monitoring, efficient communication, data collection and reducing hospital and patient expenses (Jawad et al., 2022). The researcher has conducted a comprehensive review in these areas and this research fills the gap by offering a systematic literature review of the articles that published between 2015 and 2022 and total of 106 papers that met the inclusion criteria were analyzed (Jawad et al., 2022). The smart health care consists of advance devices such as mobiles phones and electronics to improve disease detection, treatment management and improve the quality of life of the patients. By using internet of things in health care is increasing day by day. They researchers have organized their review into three sections such as motivations, challenges and the recommendations for applying in internet of health care

thing. The motivation sections are consisting of various categories such as focusing on system functions, user needs, cost related needs and data management.

In user related motivations, health care professionals can gain access to real time patients' data which help them to early diagnosis and for treatments. Also, patients can benefit by reducing the visits to the hospital and they can receive constant monitoring which is an essential for patients those are suffering from chronic illness. Internet of things can improve the performance by monitoring and early diagnosis of diseases and cost-effective treatments. With the help of cloud computing, the Internet of health care things can share their data seamless, real-time analysis and making health care services more efficient. The large of amount of data is generated by internet of things devices is health care sectors create challenges for storage, transmission, processing and security. Innovation is required in cloud computing for managing these challenges which ensure that patient's data is protected and available.

There are various challenges related to internet of health care things and their devices such as big data handling, cloud computing, security, sensors, real time processing and technical requirements. This challenge includes problems such as performance, reliability, privacy and security (Ozdemir et al., 2017). Security and privacy are the significant challenges in internet of health care things because its focuses on preventing unauthorized access to data, privacy maintaining and protecting personal information of the patients and the hospitals. There are many studies have been pointed to security vulnerabilities such as device tampering and data breaches and there are certain measures like secure authentication and encrypted data storage are important for protecting and maintaining privacy of patient's data (Shah and Chircu, 2018). The internet of things devices such as wearables, medical sensors and other connected health care devices which are vulnerable to hacking and these devices have limited security feature which is very easy for cyber attackers to exploit this weakness to manipulate the devices or steal information.

The article Security and Privacy in the Internet of Things in health care systems: Toward a Robust Solution in Real-Life Deployment by Ibrahim Sadek, Josue Codjo, Shafiq UI Rehman, and Bessam AbdulRazak (2022) focused at the security and privacy challenges of Internet of health care things. The internet of health care things provides many benefits to health care professional and care takers to keep track of patient's health records such as vitals, lab tests, medical and prescription histories either physically or remotely with the help of mobile devices, computers or laptops (Dimitrov, D.V., 2021). The main aim of IOT systems is to record patients' data more securely and then circulate it to healthcare professionals with the help of wireless connectivity. There are lots of internet connected devices are available such as pacemakers, insulin pumps and cochlear implants and some of these devices can send information with the help of wireless connection while few of them can send and receive data. The wearable devices such as smart bracelets and smart rings are most useful for keeping record of vital signs information such as heart rate and daily activities information. The data of this device is synced for further analysis and keep track of that monitored person (Chacko, A. and Hayajneh, T., 2018). While these devices are useful of health care professionals and care taker, but they are also come with security risks such as cyber-attacks and data breaches and these attacks are harmful for patients' safety and privacy. However, the authors focus on only one possible solution of these cyber-attacks and data breaches that is the AMI Lab systems and explored how it will help to make health care sectors more secure.

The authors discussed various security issues in internet of health care things and explain various types of cyber-attacks. They also suggest various ways to improve security by using stronger methods of authentication and keeping information private. They compared the AMI lab systems with other similar systems to see whether it could be best option or not. However, this article does not show any practical example of testing of security solutions work in real health care sectors. The internet of health care things is facing many problems in terms of security and they are mainly confidentiality, integrity, privacy and the authentication between the devices and to track the flow of information. There are some helpful ideas explained by the authors, but there is more limitation because they do not test their suggested solutions in real healthcare sectors. They conducted various studies to find solutions of internet of things security Chacko, A. and Hayajneh, T. (2018). The authors only explained in theory and focused mainly on the AMI lab systems and not compare with other systems. As a result, it becomes more harder to decide whether AMI lab systems are the best solution for securing internet of things in health care.

## 4. Research Methodology

This research details the methodological approach adopted to enhance the security of Internet of health care things system with the help of multi-factor authentication (MFA) and Amazon web service. The main goal is design, implement and test multifactor authentication on healthcare platform that addresses common vulnerabilities and enhance the security of Internet of health care things.

### 4.1 Research Design

The research designed a practical experimental approach to test the effectiveness of multifactor authentication to improve the security of Internet of health care things. The design structured are as follows.

Development of a secure website for IOHT platform.

This website is developed to evaluate and simulate the real-world scenarios and the platform includes are as follows.

- Frontend- The website is developed with the help of PHP, HTML and CSS to create a user-friendly platform for health care professionals and patients.
- Backend- The MySQL is used to manage database.
- Hosting and Integration- The website is hosted on Amazon web service to enhance its security.

Implementation of Security Enhancements

The website is integrated with multifactor authentication mechanism to enhance its security such as AWS Identity and Access management (IAM) is used for role-based access controls, AWS key management (KMS) to ensure encryption of sensitive data and multifactor to provide an additional layer of authentication.

System Evaluation and comparative Analysis.

The website is tested under controlled conditions to examine its effectiveness and applicability in enhancing the security of Internet of health care things systems and the evaluation is focus on following are such as Performance assessment, Usability Analysis and security comparison. The website authentication is tested to compare the differences of



multifactor authentication and single factor authentication. It includes the measuring of unauthorized access, login success rate and the impact of multi factor authentication to prevent from data breaches and cyber-attacks. The user interface and operational work flow are analysed to access the ease of this website.

## **4.2 Experimental setup**

The experimental setup is done to find out the real-world scenario and challenges related with Internet of health care things. This setup is done through testing evaluation of the developed platform's functionality, security and performance.

### **4.2.1 Platform development**

The platform is a real-world health care application integrated with functionality that are required by health care professionals and patients and their structured and roles are as follows;

- Doctors- The doctors can access and manage patient health records more securely to monitor health records of patients that is generated by Internet of health care things systems or devices.
- Patients- The patients can view their medical history and their current health records and they can also book their appointment with health care professionals. Also, they can communicate with doctors using consultation services.

### **4.2.2 Amazon web service Integration**

To enhance the security and authentication, the platform uses Amazon web service and to ensure compliance with stringent data protection standards while providing a seamless user experience.

Identity and access management (IAM)- This implemented for providing role-based access control to manage the user permissions effectively and to make sure that doctors can only access their data which are related to them. Patients can access their health records and take an appointment with health care professional. Some advanced policies are configured to limit the actions based on their roles and responsibilities, and blocking IP address filters.

Key Management Service (KMS)- The key management service is applied to secure the sensitive data of patient's during storage and transmissions. The data is encrypted using KMS and if the data is compromised, it will remain inaccessible.

Multi-Factor authentication (MFA)- The MFA is applied for additional layer of authentication and the users are going to verify their identity with the help of knowledge factors, Possession factors and Inherence factors.

### **4.2.3 Simulated Testing Environment**

The developed website is tested to check its performance, security and scalability under real world conditions.

Simulated attacks -A various cyber-attacks are performed to determine the website resilience to security threats such as brute force attacks and phishing attempts. Also, tried login attempts by using random password to test the strength of multi-factor authentication. By creating some scenarios, tricked the users to revealing their credentials to access the website to detect and block phishing attempts.

Load testing -The platform's ability is handling large volume of traffic is tested under different conditions such as Concurrent user activity, Internet of health care things data transmission and scalability. It evaluated by sending large amount of health data to check the

Internet of health things data transmission capacity and simulated multiple logins and data access request to measure the response time.

### **4.3 Data collection**

The data collection process is used to capture quantitative and qualitative information to test the website's performance, its security and the user experience. With the help of this approach, it will ensure that platform functionalities are analysed.

#### **4.3.1 Systems Logs and Monitoring**

The systems logs and monitoring tools are most important for collecting real time data of the website operations and the data forms use for analyzing authentication and security issues. The authentication logs are tracking all user authentication to test the effectiveness of the multifactor authentication and it collects details such as total number of login attempts, successful logins, unauthorized access attempts and patterns failed while making login attempts.

#### **4.3.2 User feedback**

Collecting feedback from end users is an important step to understand its usability and security performance of the developed platforms and this feedback is collected from doctors and patients. This feedback includes the surveys and in-depth interviews to record quantitative and qualitative data.

Survey -The survey is focused on design to evaluate the user satisfaction, ease of use and to check the effectiveness of the multi-factor authentication systems. This survey includes the closed ended questions which allows the user to rate their experiences on numerical scale whether they agree or disagree and the open-ended questions enable the participants to give the detailed feedback on the features of the platform or suggest platforms.

Focus Areas- To check the user satisfaction with multifactor authentication process and ease of use and also to rate the overall experience. The questions are designed to access the platform and complete the authentication tasks for the users with limited technical expertise. Eventually, the participants giving their feedback about the safeguarding sensitive information and to protect it from unauthorized access.

Interviews- The purpose of in-depth interviews to gain a comprehensive knowledge of user that may not be captured while doing surveys. The target participants are healthcare professionals such as doctors, nurses and administrative staffs those are going to use platforms to manage patients' records, schedule appointments and to access medical records and patient those are going to interact with this platform to view their health record, booking an appointment with doctors and connecting with health care takers.

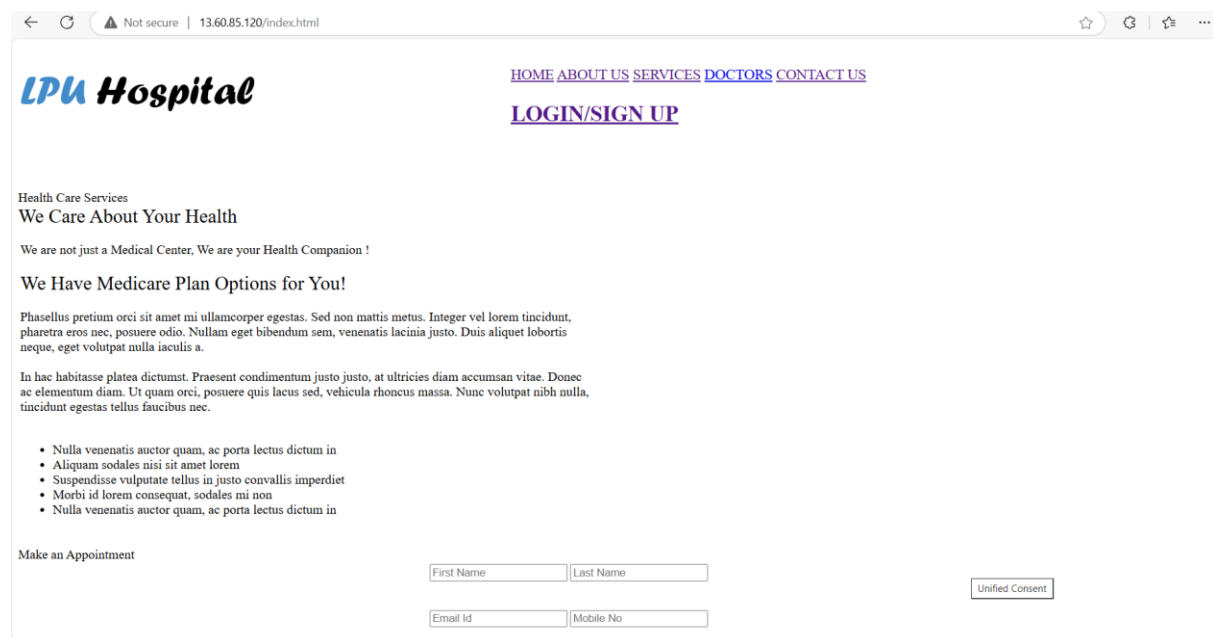
The topics covered during this interviews such as challenges in authentication and platform use, features suggestions and the overall security performance. Also, the participants discuss whether multifactor authentication has increased their confidence in the platforms to protect their sensitive data from data breaches and unauthorized access.

## **5. Design Specification**

This section outlines the design and implementation process for developing a secure healthcare website that integrated with multi- factor authentication and which uses Amazon web services. The website is built to show the need of Internet of health care things and also to maintain the ease of use and scalability of doctors and patients.

## 5.1 Website Design

The website is designed to provide secure access to health care things and also focusing on its usability, security and scalability. The website has two primary users with their different roles and responsibilities. The healthcare professionals can securely access patients' health records and manage patients' appointment and patients can view their health records and schedule their appointment with doctors when they require.



The screenshot displays a web browser window with the address bar showing "13.60.85.120/index.html". The website header features the "LPU Hospital" logo on the left and navigation links "HOME ABOUT US SERVICES DOCTORS CONTACT US" on the right. Below the navigation links is a "LOGIN/SIGN UP" link. The main content area includes the text "Health Care Services We Care About Your Health" and "We are not just a Medical Center, We are your Health Companion !". It also features a section titled "We Have Medicare Plan Options for You!" followed by a paragraph of placeholder text and a bulleted list of items. At the bottom, there is a "Make an Appointment" form with input fields for "First Name", "Last Name", "Email Id", and "Mobile No", and a "Unified Consent" checkbox.

### 5.1.1 Non-Functional Requirements

The non-functional requirements such as security, usability and scalability. The security is used to ensure data protection with the help of encryption and multi-factor authentication to it protect from cyber-attacks such as data breaches and unauthorized access. The usability is to create user-friendly interface for all users and to access all important features of that platform. The scalability allows the platform to handle multiple requests at a time and to support the integration of additional functionalities.

### 5.1.2 System Architecture

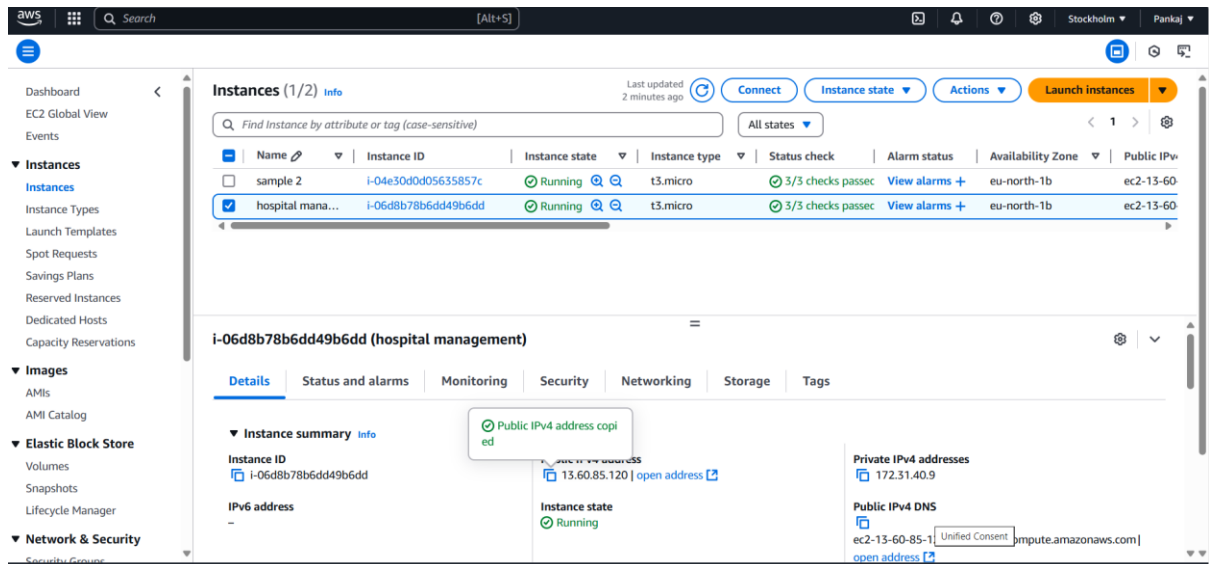
The platform's architecture consists of three core layers such as secure, scalable and efficient functionality.

1. Frontend- The website is developed using PHP, html and CSS for a responsive user interface and this allows access to two primary users with their different roles and responsibilities. The frontend is focuses on providing simplicity, so that users can easily authenticate and access required features.
2. Backend- PHP used for managing server-side logic such as user authentication, data processing, creating a secure connection and to provide role-based access control to support dynamic content.

3. Database- MySQL is for relational data storage and by hosting on amazon web service to ensure data integrity to support secure data access.

## 5.2 Deployment

The website is deployed on Amazon web service infrastructure to enhance its reliability and performance. For this website, AWS EC2 is used to host web application and the backend. The PHP web application with html and CSS file is deployed and this make that users can interact with the platform seamlessly.



```
Amazon Linux 2023
https://aws.amazon.com/linux/amazon-linux-2023

Last login: Tue Dec 10 15:41:03 2024 from 13.48.4.202
[ec2-user@ip-172-31-41-37 ~]$ sudo su
[root@ip-172-31-41-37 ec2-user]# mkdir morri2
[root@ip-172-31-41-37 ec2-user]# cd morri2
[root@ip-172-31-41-37 morri2]# wget https://github.com/kktrav/morri/archive/refs/heads/main.zip
--2024-12-10 16:35:09-- https://github.com/kktrav/morri/archive/refs/heads/main.zip
Resolving github.com (github.com)... 4.225.11.194
Connecting to github.com (github.com)|4.225.11.194|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://codeload.github.com/kktrav/morri/zip/refs/heads/main [following]
--2024-12-10 16:35:09-- https://codeload.github.com/kktrav/morri/zip/refs/heads/main
Resolving codeload.github.com (codeload.github.com)... 4.225.11.198
Connecting to codeload.github.com (codeload.github.com)|4.225.11.198|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [application/zip]
Saving to: 'main.zip'

main.zip
```

The firewall rules and security groups are setup while creating EC2 instance to control ingoing and outgoing traffic. The HTTP, HTTPs and SSH ports are opened and other ports are restricted.

The screenshot shows the AWS IAM console interface for a security group named 'i-06d8b78b6dd49b6dd (hospital management)'. It displays a table of Outbound rules. The table has columns for Security group rule ID, Port range, Protocol, Source, and Security groups. There are three rules listed, all with a source of '0.0.0.0/0' and pointing to the 'launch-wizard-2' security group. A search bar at the top left says 'Filter rules'. A 'Unified Consent' button is at the bottom right. A link '▼ Outbound rules' is at the bottom left.

Security group rule ID	Port range	Protocol	Source	Security groups
sgr-017ee867a0c3906a8	22	TCP	0.0.0.0/0	<a href="#">launch-wizard-2</a>
sgr-0a1b99c8294afc7ed	443	TCP	0.0.0.0/0	<a href="#">launch-wizard-2</a>
sgr-05ad89acacf54fdc7	80	TCP	0.0.0.0/0	<a href="#">launch-wizard-2</a>

## 5.3 Testing and Validation

Testing and validation are an important to make the platform to operate securely and efficiently. There are various testing methodologies which used to test different aspects of the platform such as functionality, performance and security,

### 5.3.1 Performance testing

To test the website performance response times and ability to handle a large of amount of data without any creating any other problem. The scenarios of testing are simulating concurrent user logins and monitoring latency. In concurrent user logins, it is tested during peak hours by doing multiple user logins at a time and this measure response time and identify bottlenecks in the authentication process. In monitoring latency, it evaluated the time taken to retrieve patient's data, process appointments and to complete authentication process in both normal and high traffic conditions.

### 5.3.2 Security testing

The security testing is done to identify and mitigate weakness present in the website.

#### 1. Validation of security mechanism

It is done to verify the encryption rules for data and to check whether it meet industry standard or not. Also, it confirms that proper implementation of amazon web service, IAM policies for role-based access control, and AWS KMS for data encryption.

#### 2. Synk Integration

This testing is done to review the vulnerabilities reported by Synk to ensure all identified issues have addressed and to validate the dependencies and configuration to meet secure coding standards. The fig shows there is a SQL injection is present in the code and it need to address.



I have fixed the code and updated it on synk to verify that SQL injection vulnerability is resolved and to ensure that all identified problems are rechecked and validated to meet the secure coding practices.

## 6. Result and Analysis

This section gives a detailed evaluation for implementing multifactor authentication and Amazon web service in the Internet of healthcare things systems. This analysis is using quantitative metrics, statistical validation and qualitative to measure the platform security.

### 6.1 Enhance security

The multifactor authentication has significantly reduced unauthorized access as compared to single factor authentication and MFA demonstrated an 85% of reduction in successful of brute force and phishing attempts. The Role based access control with AWS allows healthcare professional to access data that are related to them for example patients records and appointments.

### 6.2 Improved Data Protection

The sensitive information of patients while they are in transit or rest are encrypting with the help of AWS and to ensure that no unauthorized access can be done during testing. By using synk to Identify and resolve vulnerabilities such as SQL injection to ensure that the system was secure against common database exploits.

### 6.3 Performance metrics

The authentication response with multifactor authentication was 1.8 seconds to ensure that a secure user experience and the response during high load remains the same. The capabilities of AWS EC2 has effectively handle an increasing number of users and also a large amount of data.

## 7. Conclusion and Discussion

The integration of multi-factor authentication and Amazon web service into the internet of health care things (IOHT) platform has enhanced the security of healthcare sectors. This research focused on fixing the vulnerabilities in single factor authentication with the help of advance security solutions such as Identity and Access Management (IAM), Key management and multi-factor authentication.

## **7.1 Summary of findings**

Improved security- The use of multi-factor authentication has enhanced the website's ability to prevent it from cyber-attacks. Identity and Access Management provide role-based access controls to the users.

Data Protection- KMS provide encryption of data for both those are in process or other those at rest and this prevent risks of unauthorized access and protect sensitive data.

User-Focused Design- The website is maintaining an intuitive and user interface instead its advanced security features. Conducting surveys and interviews have showed that healthcare professionals and patients have appreciated the ease of use.

## **7.2 Discussion**

This research gives an importance of enhance security measures in Internet of health care things integrated with amazon web services to address common security challenges in health care sectors and offering them secure and user-friendly website.

Practical Application- Various simulated testing scenarios conducted to test the platform can handle real challenges in healthcare environments.

User Adoption- The feedback from users have highlighted the successful balance between security and accessibility and this balance is an important is healthcare security to adopt of new technologies.

## **7.3 limitations**

The research has achieved its primary goals, but there are many areas that require further attentions.

Scope of Testing – The testing is only focused on some threats such as phishing and brute force attacks and it should be expand to include some other threats like insider attacks or ransomware attacks.

Resource Constraints- The testing is carried out on small healthcare settings but it should be carried out in larger and complex systems to show additional insights.

## **7.4 Future Directions**

There are following areas that are recommended for further development which are follows.

Artificial Intelligence Integration- Artificial Intelligence can be used to detect an unusual behaviour or anomalies in real time to enhance the security of the platform.

Blockchain Technology- By using blockchain to secure data sharing and immutable logging that will improve transparency and performance of platform.

Advanced Security protocols- The advanced security protocols can be used in future for its additional measures such as intrusion detection systems (IDS) and encryption practices.

This research highlighted an integration of multi-factor authentication and amazon web service to improve the security and functionality of Internet of health care things systems. By fixing key vulnerabilities of website and focusing on user experience will make this platform a strong foundation for securing healthcare sectors.

## References

- [1] Bo Guo, Nur Syufiza Ahmad Shukor and Irny Suzila Ishak (2024) *(PDF) enhancing Healthcare Services Through Cloud Service*. Available at: [https://www.researchgate.net/publication/377878819\\_Enhancing\\_healthcare\\_services\\_through\\_h\\_cloud\\_service\\_a\\_systematic\\_review](https://www.researchgate.net/publication/377878819_Enhancing_healthcare_services_through_h_cloud_service_a_systematic_review) (Accessed: 28 October 2024).
- [2] Suhail Javed Quraishi and Humra Yusuf (no date) *(PDF) internet of things in healthcare, a literature review*. Available at: [https://www.researchgate.net/publication/357842774\\_Internet\\_of\\_Things\\_in\\_Healthcare\\_A\\_Literature\\_Review](https://www.researchgate.net/publication/357842774_Internet_of_Things_in_Healthcare_A_Literature_Review) (Accessed: 28 October 2024).
- [3] Parag Chatterjee, Leandro J. Cymberknop and Ricardo L. Armentano (no date a) *IOT-based decision support system for Intelligent Healthcare — applied to cardiovascular diseases | IEEE conference publication | IEEE xplore*. Available at: <https://ieeexplore.ieee.org/document/8418567/> (Accessed: 28 October 2024).
- [4] Swaleha Shaikh and Vidya Chitre (no date a) *Healthcare Monitoring System using IOT | IEEE conference publication | IEEE Xplore*. Available at: <https://ieeexplore.ieee.org/abstract/document/8300952> (Accessed: 28 October 2024).
- [5] Sudhir K. Routray and Sharath Anand (no date a) *[PDF] narrowband IOT for Healthcare, Semantic Scholar*. Available at: <https://www.semanticscholar.org/reader/ef14db158558174d95df5d276c403aed38f5d35b> (Accessed: 28 October 2024).
- [6] S.LAVANYA, G.LAVANYA and J.DIVYABHARATHI (no date a) *Remote prescription and I-home healthcare based on IOT | IEEE conference publication | IEEE Xplore*. Available at: <https://ieeexplore.ieee.org/document/8094069/> (Accessed: 28 October 2024).
- [7] Ghulam Muhammad, SK Md Mizanur Rahman, *et al.* (no date) *Smart health solution integrating IOT and cloud: A case study of voice pathology monitoring | IEEE Journals & Magazine | IEEE Xplore*. Available at: <https://ieeexplore.ieee.org/document/7823340/> (Accessed: 28 October 2024).
- [8] Yang Yang *et al.* (2018c) *Privacy-preserving smart IOT-based healthcare big data storage and self-adaptive access control system, Information Sciences*. Available at:



<https://www.sciencedirect.com/science/article/pii/S0020025518300860> (Accessed: 28 November 2024).

[9] Fizar Ahmed (no date b) *(PDF) an internet of things (IOT) application for predicting ...* Available at:

[https://www.researchgate.net/publication/316177658\\_An\\_Internet\\_of\\_Things\\_IoT\\_Application\\_for\\_Predicting\\_the\\_Quantity\\_of\\_Future\\_Heart\\_Attack\\_Patients](https://www.researchgate.net/publication/316177658_An_Internet_of_Things_IoT_Application_for_Predicting_the_Quantity_of_Future_Heart_Attack_Patients) (Accessed: 28 October 2024).

[10] AmmarAwadMutlag *et al.* (2018) *Enabling technologies for fog computing in healthcare IOT Systems, Future Generation Computer Systems*. Available at:

<https://www.sciencedirect.com/science/article/pii/S0167739X18314006> (Accessed: 28 October 2024).

[11] Junaid Mohammed *et al.* (no date) *Internet of things: Remote patient monitoring using web services and cloud computing | IEEE conference publication | IEEE xplore*. Available at: <https://ieeexplore.ieee.org/document/7059670/> (Accessed: 29 October 2024).

[12] Ee-May Fong and Wan-Young Chung (no date) *(PDF) Mobile Cloud-Computing-based healthcare service by ...* Available at:

[https://www.researchgate.net/publication/259246800\\_Mobile\\_Cloud-Computing-Based\\_Healthcare\\_Service\\_by\\_Noncontact\\_ECG\\_Monitoring](https://www.researchgate.net/publication/259246800_Mobile_Cloud-Computing-Based_Healthcare_Service_by_Noncontact_ECG_Monitoring) (Accessed: 30 October 2024).

[13 ] Kornelia Batko and Ślęzak Andrzej (no date) *(PDF) the use of Big Data Analytics in Healthcare*. Available at:

[https://www.researchgate.net/publication/357644264\\_The\\_use\\_of\\_Big\\_Data\\_Analytics\\_in\\_healthcare](https://www.researchgate.net/publication/357644264_The_use_of_Big_Data_Analytics_in_healthcare) (Accessed: 30 October 2024).

[14] Huda Hussein Mohamad Jawad, Zainuddin Bin and Bilal Bahaa Zaidan (no date) *(PDF) A systematic literature review of enabling IOT in Healthcare: Motivations, challenges, and recommendations*. Available at:

[https://www.researchgate.net/publication/364276967\\_A\\_Systematic\\_Literature\\_Review\\_of\\_](https://www.researchgate.net/publication/364276967_A_Systematic_Literature_Review_of_)

Enabling\_IoT\_in\_Healthcare\_Motivations\_Challenges\_and\_Recommendations (Accessed: 01 November 2024).

[15] Chenxi Huang *et al.* (2023) *Internet of medical things: A systematic review*, *Neurocomputing*. Available at:  
<https://www.sciencedirect.com/science/article/pii/S0925231223008421> (Accessed: 02 November 2024).

[16] Venkata Prasanth Yanambaka *et al.* (no date) (PDF) *PMsec: Physical unclonable function-based robust and lightweight authentication in the internet of medical things*. Available at:  
[https://www.researchgate.net/publication/334152897\\_PMsec\\_Physical\\_Unclonable\\_F  
unction-  
Based\\_Robust\\_and\\_Lightweight\\_Authentication\\_in\\_the\\_Internet\\_of\\_Medical\\_Things](https://www.researchgate.net/publication/334152897_PMsec_Physical_Unclonable_Function-Based_Robust_and_Lightweight_Authentication_in_the_Internet_of_Medical_Things) (Accessed: 02 November 2024).

[17] Faisal S. Alsubaei *et al.* (no date) (PDF) *IOMT-SAF: Internet of medical things security assessment framework*. Available at:  
[https://www.researchgate.net/publication/336340918\\_IoMT-  
SAF\\_Internet\\_of\\_Medical\\_Things\\_Security\\_Assessment\\_Framework](https://www.researchgate.net/publication/336340918_IoMT-SAF_Internet_of_Medical_Things_Security_Assessment_Framework) (Accessed: 03 November 2024).

[18] Hai Ziwei *et al.*, “The applications of internet of things in smart healthcare sectors: A Bibliometric and deep study,” *Heliyon*,  
<https://www.sciencedirect.com/science/article/pii/S2405844024014233> (accessed Nov. 4, 2024).

[19] FATIMA ALSHEHRI and GHULAM MUHAMMAD (no date) *IEEE Xplore Full-text PDF*: Available at:  
<https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10363200> (Accessed: 04 November 2024).

[20] S. M. RIAZUL ISLAM *et al.* (no date) [PDF] *the internet of things for health care: A comprehensive survey* | *semantic scholar*. Available at:  
[https://www.semanticscholar.org/paper/The-Internet-of-Things-for-Health-Care:-A-Survey-  
Islam-Kwak/cddb22908f28a1636cbbdeb3a4f0e00f9cef05a9](https://www.semanticscholar.org/paper/The-Internet-of-Things-for-Health-Care:-A-Survey-Islam-Kwak/cddb22908f28a1636cbbdeb3a4f0e00f9cef05a9) (Accessed: 05 November 2024).

[21] Rushabh Shah and Alina Chircu (no date a) *IOT AND AI IN HEALTHCARE: A SYSTEMATIC LITERATURE REVIEW*. Available at: <https://www.semanticscholar.org/paper/IOT-AND-AI-IN-HEALTHCARE:-A-SYSTEMATIC-LITERATURE-Shah-Chircu/45f1aa37b38efca0cc36b6d7b58d56bc1b5c7951> (Accessed: 08 November 2024).

[22] Shahmiri, S. (2021a) *Wearing your data on your sleeve: Wearables, the FTC, and the privacy implications of this new technology*, *Globethics Library Homepage*. Available at: <https://repository.globethics.net/handle/20.500.12424/3993744> (Accessed: 09 November 2024).

[23] Ibrahim Sadek *et al.* (2022a) *Security and privacy in the internet of things healthcare systems: Toward a robust solution in real-life deployment*, *Computer Methods and Programs in Biomedicine Update*. Available at: <https://www.sciencedirect.com/science/article/pii/S2666990022000222> (Accessed: 11 November 2024).

[24] Dimitar V Dimitrov (no date) *Efficient data handling for massive internet of medical things: Healthcare Data Analytics [1 ed.] 3030666328, 9783030666323, dokumen.pub*. Available at: <https://dokumen.pub/efficient-data-handling-for-massive-internet-of-medical-things-healthcare-data-analytics-1nbsped-3030666328-9783030666323.html> (Accessed: 12 November 2024).

[25] Anil Chacko and Thaier Hayajneh (no date a) *(PDF) security and privacy issues with IOT in Healthcare*. Available at: [https://www.researchgate.net/publication/326568227\\_Security\\_and\\_Privacy\\_Issues\\_with\\_IoT\\_in\\_Healthcare](https://www.researchgate.net/publication/326568227_Security_and_Privacy_Issues_with_IoT_in_Healthcare) (Accessed: 12 November 2024).

[26] L. Minh Dang, Kyungbok Min, *et al.* (no date) *(PDF) a survey on internet of things and cloud computing for Healthcare*. Available at: [https://www.researchgate.net/publication/334457075\\_A\\_Survey\\_on\\_Internet\\_of\\_Things\\_and\\_Cloud\\_Computing\\_for\\_Healthcare](https://www.researchgate.net/publication/334457075_A_Survey_on_Internet_of_Things_and_Cloud_Computing_for_Healthcare) (Accessed: 14 December 2024).

[27] Srinivas Jangirala *et al.* (no date) *Cloud centric authentication for wearable healthcare* ... Available at:  
[https://www.researchgate.net/publication/324609384\\_Cloud\\_Centric\\_Authentication\\_for\\_Wearable\\_Healthcare\\_Monitoring\\_System](https://www.researchgate.net/publication/324609384_Cloud_Centric_Authentication_for_Wearable_Healthcare_Monitoring_System) (Accessed: 15 November 2024).

[28]Ahmet Turan Ozdemir, Cihan Tunc and Salim Hariri (no date a) *(PDF) Autonomic Fall Detection System - Researchgate*. Available at:  
[https://www.researchgate.net/publication/320365999\\_Autonomic\\_Fall\\_Detection\\_System](https://www.researchgate.net/publication/320365999_Autonomic_Fall_Detection_System) (Accessed: 16 November 2024).