National College of Ireland

Encryption of the Healthcare Data to Protect Against Various Attacks

MSc Research Project
Cloud Computing

Bharat Patil
Student ID: 21204811

School of Computing
National College of Ireland

Supervisor: Sean Heeney

National College of Ireland
Project Submission Sheet
School of Computing

Student Name:	Bharat Patil
Student ID:	21204811
Programme:	Msc in Cloud Computing
Year:	2022
Module:	MSc Research Project
Supervisor:	Sean Heeney
Submission Due Date:	14/08/2023
Project Title:	Encryption of the Healthcare Data to Protect Against Various Attacks
Word Count:	4604
Page Count:	19 LastPage

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:	Bharat Patil
Date:	18th September 2023

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST:

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

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

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Encryption of the Healthcare Data to Protect Against Various Attacks

Bharat Patil
21204811

Abstract

The rapid advancement of technology and the advent of the Internet of Things (IoT) have revolutionized various industries, including healthcare. IoT devices in healthcare systems offer promising opportunities to improve patient care, increase operational efficiency, and enhance medical research. However, the integration of these devices into critical healthcare infrastructures raises significant concerns about security and privacy. This research delves into the multifaceted landscape of security challenges posed by IoT devices in healthcare systems and explores potential solutions to safeguard patient data, maintain the integrity of medical operations, and protect against potential cyber threats.

The first part of this research involves a comprehensive review of the current state of IoT devices in healthcare systems. It examines the various types of IoT devices deployed, ranging from wearable health monitors to smart medical devices and connected medical facilities. The analysis highlights their indispensable role in real-time patient monitoring, disease management, and remote patient care. Despite their transformative potential, these IoT devices also introduce new entry points for cyber attackers to exploit vulnerabilities and access sensitive patient data. With a focus on security threats, the second section of this research identifies and categorizes potential risks associated with IoT devices in healthcare systems. It sheds light on common attack vectors such as unauthorized access, data breaches, and denial-of-service (DoS) attacks.

To mitigate the risks and enhance the security posture of IoT devices in healthcare systems, the third part of this research investigates existing security measures and best practices. Robust encryption, strong authentication mechanisms, and continuous monitoring of devices are some of the strategies adopted to protect against cyber threats. Furthermore, the research explores the significance of adherence to regulatory standards, such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR), in ensuring patient data confidentiality and integrity. This research underscores the significance of addressing security challenges associated with IoT devices in healthcare systems. While these devices hold tremendous potential for revolutionizing healthcare, their integration should be accompanied by a steadfast commitment to robust security practices. By acknowledging the risks and adopting proactive security measures, the healthcare industry can unlock the full potential of IoT devices while ensuring patient safety, data privacy, and the integrity of medical operations.

***Keywords*— Cloud Security Confidentiality, Data Classification, Machine Learning, Cryptography Algorithm.**

1 Table of Content

Contents

2 Introduction

The Internet of Things (IoT) represents a ground-breaking technological paradigm that has transformed the way we interact with the digital world and the physical environment around us. It is a vast network of interconnected devices, objects, and systems that communicate and exchange data over the internet without the need for human intervention. IoT has emerged as one of the most influential and disruptive technologies of the 21st century, reshaping industries, enhancing efficiency, and fundamentally altering how we live and work.

At its core, IoT relies on a web of interconnected "smart" devices that are embedded with sensors, actuators, and communication modules. These devices can collect, process, and transmit data, enabling them to interact with each other, gather information from their surroundings, and respond accordingly. The data generated by IoT devices is aggregated, analysed, and utilized to provide valuable insights, automate tasks, and improve decision-making processes.

2.1 General Findings

The growth of IoT can be attributed to several factors. First, advancements in miniaturization and microelectronics have allowed for the creation of smaller, energy-efficient sensors, making it easier and more cost-effective to integrate them into everyday objects and devices. Second, the proliferation of high-speed internet connectivity has expanded the reach and capabilities of IoT systems, facilitating seamless data transfer between devices and cloud-based platforms.

IoT has found applications across numerous domains, with one of the most significant being in the realm of smart homes. In smart homes, IoT devices such as smart thermostats, lighting systems, and home assistants enable homeowners to control and monitor various aspects of their living spaces remotely. This not only enhances convenience but also contributes to energy conservation and cost efficiency.

Beyond smart homes, IoT has revolutionized industries such as healthcare, transportation, agriculture, manufacturing, and retail. In healthcare, IoT-enabled medical devices facilitate remote patient monitoring, improve treatment outcomes, and optimize healthcare delivery. In transportation, IoT enables real-time tracking of vehicles, predictive maintenance, and the development of autonomous vehicles.

However, as IoT continues to grow, it brings forth several challenges, with security and privacy being paramount concerns. With the massive influx of data being exchanged between devices and stored on cloud servers, the risk of cyber threats and unauthorized access rises significantly. Ensuring robust security measures and adherence to privacy regulations becomes imperative to safeguard sensitive information and maintain user trust.

Moreover, the interoperability of various IoT devices and the standardization of communication protocols pose technical challenges that need to be addressed for seamless integration and efficient collaboration between devices from different manufacturers and ecosystems.

2.2 Research Question

As the use of IoT devices has been increasing, where in there are multiple threats of how data can be exposed. How can we make sure the data is secure/private?

2.3 Ethics Consideration

The ethical statement is included in Table 1, which contains relevant information. The study utilizes the IoT Healthcare Security Dataset supplied from the Kaggle website. The documentation pertaining to copyright concerns, Terms of Use, and Privacy Policy of the firm has been provided as follows:

- IoT Healthcare Security Dataset

- Copyright Dispute Policy
- Kaggle Terms of Use
- Kaggle Privacy Policy

Table 1: Table of Ethics Consideration Declaration

This project involves human participants	Yes / No
The project makes use of secondary dataset(s) created by the researcher	Yes / No
The project makes use of public secondary dataset(s)	Yes / No
The project makes use of non-public secondary dataset(s)	Yes / No
Approval letter from non-public secondary dataset(s) owner received	Yes / No

3 Literature Review

3.1 Security Issues of IoT in Healthcare Sector: A Systematic Review

The research article titled "Security Issues of IoT in Healthcare Sector: A Systematic Review" is a complete examination of the security concerns associated with the Internet of Things (IoT) in the healthcare industry. The researchers did a comprehensive review of the existing literature by collating papers published in reputable academic journals between the years 2015 and 2021. This enabled them to provide a concise overview of the many issues that are closely associated with the subject matter *Security Issues of IoT in Healthcare Sector: A Systematic Review* (2022).

This research emphasizes the significance of the Internet of Things (IoT) within the healthcare industry, as it offers a wide range of effective services for healthcare professionals and facilitates treatments for patients with different medical conditions. The design of the healthcare system application for the Internet of Things (IoT) encompasses several components, including devices, network infrastructure, a layered model, and Communication Application/Protocols. Nevertheless, the research also highlights that the Internet of Things (IoT) encounters many security difficulties inside its patient record hierarchy. The establishment of IoT-based systems in the healthcare industry necessitates a strong emphasis on ensuring comprehensive security and privacy measures, primarily because to the sensitive nature of private and empathetic patient data.

The authors found the following IoT security problems in the healthcare industry, which are outlined as follows:

- **Data Privacy and Confidentiality:** The study reveals that data privacy and confidentiality are the most important security concerns in the healthcare industry. The authors recommend that healthcare organizations implement robust security measures to prevent unauthorized access, disclosure, and modification of sensitive patient data.

- **Data Integrity and Availability:**The study also highlights the significance of data availability and integrity in the healthcare industry. The authors recommend that healthcare organizations implement measures to ensure that patient data is accurate, comprehensive, and accessible when required.

- **Authentication and Authorization:** The research emphasizes the significance of authentication and authorization in the healthcare industry. The authors recommend that healthcare organizations implement robust authentication and authorization mechanisms to ensure that only authorized personnel can access patient information.

- **Network Security:** In addition, the study identifies network security as a crucial issue in the healthcare industry. The authors recommend that healthcare organizations implement firewalls, intrusion detection systems, and encryption to protect their networks from unauthorized access.

- **Device Security:** Additionally, the study emphasizes the significance of device security in the healthcare industry. The authors recommend that healthcare organizations secure their IoT devices against unauthorized access with measures such as strong passwords, firmware updates, and encryption *Internet of Things Security: Challenges and Key Issues* (2021a).

- **Regulatory Compliance:** The research emphasizes the significance of regulatory compliance in the healthcare industry. The authors recommend that healthcare organizations comply with applicable regulations, such as HIPAA, to safeguard patient information.

3.2 Security and Interoperability Issues with Internet of Things (IoT) in Healthcare Industry: A Survey

The paper titled "Security and Interoperability Issues with Internet of Things (IoT) in Healthcare Industry: A Survey" provides a survey of the security and privacy issues associated with Internet of Things (IoT) in the healthcare industry. The authors have conducted a thorough literature review to identify the most significant challenges and solutions associated with the use of IoT in healthcare Abounassar et al. (2022).

The paper begins by introducing the concept of IoT and its healthcare applications. The section then discusses the various IoT devices and sensors utilized in healthcare, including wearables, smart implants, and medical imaging devices. The authors emphasize the advantages of utilizing IoT in healthcare, including enhanced patient outcomes, decreased costs, and increased efficiency.

However, the paper also focuses on the numerous security and privacy issues associated with the use of IoT in healthcare. These obstacles are as follows:

- **Data security:** Sensitive patient data collected and transmitted by IoT devices and sensors is susceptible to cyberattacks and data breaches.

- **Privacy concerns:** Patients may be concerned about how IoT devices and sensors collect and use their confidential health information.

- **Interoperability issues:** Different IoT devices and sensors may utilize different communication protocols, making their integration into a unified healthcare system challenging.
- **Trust issues:** Patients and healthcare professionals may lack confidence in the precision and dependability of IoT devices and sensors.

To address these obstacles, the authors discuss a variety of security and privacy mechanisms and tools that can be used to safeguard patient data and guarantee the reliability of IoT devices and sensors. These are as follows:

- **Encryption:** Encryption can be used to secure patient data from unauthorized access and guarantee its privacy.
- **Access control:** Access control mechanisms can be used to limit patient data access to only authorized personnel.
- **Authentication:** Authentication mechanisms can be used to restrict access to patient data to only authorized devices and sensors.
- **Blockchain:** Blockchain technology can be used to create a secure, transparent, and tamper-proof record of patient information.
- **Standardization:** Standardization of communication protocols can facilitate interoperability between various Internet of Things devices and sensors.

3.3 Security and Privacy Issues in Medical Internet of Things: Overview, Countermeasures, Challenges and Future Directions

The aforementioned study offers a comprehensive examination of the security and privacy concerns that arise within the realm of Medical Internet of Things (MIoT). The researchers have undertaken a comprehensive review of existing literature to ascertain the present condition of security and privacy in the realm of Medical Internet of Things (MIoT). They have also deliberated over different instances of attack scenarios, countermeasures, difficulties, and potential avenues for future development *Security and Privacy Issues in Medical Internet of Things: Overview, Countermeasures, Challenges and Future Directions* (2021).

The authors' literature survey demonstrates that the domain of Medical Internet of Things (MIoT) is experiencing significant growth and holds promise for enhancing the healthcare industry. This technology has the potential to provide seamless medical facilities and improve the services offered by medical practitioners, nurses, pharmaceutical companies, and various government and non-government organizations involved in healthcare. Nevertheless, the authors have observed that the security and privacy of Medical Internet of Things (MIoT) devices and technologies are often disregarded and compromised by pertinent stakeholders, resulting in an increasing number of security breaches that specifically target the MIoT within the healthcare sector.

The researchers have uncovered many instances of attacks that have the potential to undermine the security and privacy of devices and technology within the context of the Medical Internet of Things (MIoT). The aforementioned items encompass: *Data Breaches*

in Healthcare Security Systems. (2021)

- Unauthorized access to patient data
- Malware attacks on MIoT devices
- Denial of Service (DoS) attacks on MIoT devices
- Man-in-the-middle (MitM) attacks on MIoT devices
- Physical attacks on MIoT devices

In order to address the aforementioned attack scenarios, the writers have deliberated over a range of countermeasures and remedies. The aforementioned items encompass:

- Encryption of patient data
- Implementation of access control mechanisms
- Regular software updates and patches
- Implementation of intrusion detection and prevention systems
- Implementation of physical security measures

The authors have furthermore outlined a range of difficulties that want attention in order to enhance the security and privacy of MIoT devices and technology. The aforementioned items encompass *Challenges in Smart Health Applications Using Wearable Medical Internet-of-Things—A Review* (2022):

- Lack of standardization in MIoT devices and technologies
- Lack of awareness among medical staff and patients regarding the security and privacy risks associated with MIoT devices and technologies
- Limited resources for implementing security and privacy measures in MIoT devices and technologies
- Lack of collaboration among stakeholders in the MIoT domain

3.4 Review of security challenges in healthcare internet of things

The paper titled "Review of Security Challenges in Healthcare Internet of Things" endeavours to evaluate the security issues and proposed solutions for the Internet of Medical Things (IoMT). The following is the paper's literature review:

- Beginning with an overview of the Internet of Things (IoT) and its various applications, including healthcare, the paper then proceeds to discuss the healthcare sector. It emphasizes the exponential development of the IoT market in healthcare services and the need for security measures to safeguard patient data.

- The authors examine a variety of security issues present in IoMTs, such as device-level and communication-level security issues. They analyse the risk factors of security attacks on IoMTs and propose a risk assessment to determine which IoMTs are most susceptible to security attacks.

- The paper discusses the security vulnerabilities of hospital-used medical devices, including Implantable Medical Devices, Radio Frequency Identification badges, and wearable medical devices. It highlights the significance of protecting the privacy and confidentiality of a patient's medical records *Review of security challenges in healthcare internet of things* (2021).

- The authors categorize the existing works on IoMT security solutions into device-level security solutions and communication-level security solutions. The resolution of device-level security issues is deemed desirable, whereas communication-level security has received only moderate attention.

- The article emphasizes the significance of securing wireless insulin pumps, which are susceptible to authentication issues. The authors propose a secure authentication protocol as a solution to this issue.

- The authors discuss the security challenges in cloud-based IoMTs and propose a solution to secure data transmission between the cloud and IoMT devices.

- The conclusion of the paper summarizes the main findings of the literature review and emphasizes the need for additional research in the area of security challenges in healthcare IoT.

In conclusion, the paper provides a comprehensive literature review of the security challenges that exist in healthcare IoT and the proposed solutions. It emphasizes the need for device-level security solutions and the significance of protecting patient data in IoMTs. The paper also proposes a risk assessment to identify the IoMT security assaults with the greatest impact.

3.5 Internet of Things Security: Challenges and Key Issues

The literature review section of this paper provides an overview of previous studies that have surveyed the security of IoT technology. The authors note that while there have been many studies on IoT security, their paper aims to identify specific security challenges and key issues that are likely to arise in the IoT environment in order to guide authentication techniques to achieve a secure IoT service. The authors cite several previous studies that have examined IoT security, including studies on IoT security architecture, IoT security protocols, and IoT security threats *Internet of Things Security: Challenges and Key Issues* (2021b). They note that many of these studies have identified the need for lightweight encryption techniques in IoT security, as well as the need for authentication and access control mechanisms. The authors also discuss some of the specific security challenges and issues that are likely to arise in the IoT environment. These include:

- **Device heterogeneity:** IoT devices come in many different shapes and sizes, and may use different communication protocols and security mechanisms. This can make it difficult to develop a unified security framework for IoT.

- **Limited resources:** Many IoT devices have limited processing power, memory, and battery life, which can make it difficult to implement complex security mechanisms.

- **Data privacy:** IoT devices often collect sensitive data about users, such as health information or location data. Ensuring the privacy of this data is a key challenge in IoT security.

- **Network security:** IoT devices are often connected to the internet, which makes them vulnerable to a wide range of network-based attacks, such as denial-of-service attacks or man-in-the-middle attacks.

The authors also provide a short guidance to researchers to accomplish secure IoT services like authentication, access control, and so on. They note that IoT solutions must come with some basic security services including authorization, authentication, confidentiality, availability, integrity, and non-repudiation. Overall, the literature review section of this paper provides a useful overview of previous studies on IoT security, and highlights some of the specific security challenges and issues that are likely to arise in the IoT environment Kaur and Gandhi (2022).

4 Security Issue

The Internet of Things has shown to be very advantageous for consumers, yielding significant benefits. However, it is important to acknowledge that challenges have also emerged in this context. The primary concerns of specialists or security professionals are on the potential risks to safety and privacy. These two factors have placed several business and governmental institutions in a difficult predicament. Numerous significant instances of espionage have drawn attention to the deficiencies inherent in Internet of Things (IoT) technologies. The persistence of this risk is attributable to the interconnectedness of Internet of Things (IoT) devices, which grants access to the unprotected and unverified Internet. Consequently, there is a need to provide new reasons for enhancing security measures *The Dependency of Healthcare on Security: Issues and Challenges* (2021).

The importance of data privacy and confidentiality, data integrity and availability, authentication and authorization, network security, device security, and regulatory conformance is highlighted by the IoT security issues in the healthcare industry. The healthcare organizations should implement stringent security measures to prevent unauthorized access, disclosure, and modification of sensitive patient data. In the sphere of healthcare, an IoT healthcare architecture that represents an effective patient discovery solution.

The use of IoT in healthcare raises a number of security concerns, including data security, privacy concerns, interoperability issues, and trust concerns. The collection and transmission of sensitive patient data by IoT devices and sensors, which are susceptible to cyberattacks and data intrusions, gives rise to these issues. Various security mechanisms and tools, such as encryption, access control, authentication, blockchain, and standardization of communication protocols, are utilized to resolve these challenges Trayush et al. (2021).

The following are some of the security challenges encountered by IoT-based e-healthcare systems:

- Data loss and unauthorized modification of medical information.

- Due to security concerns, there is a lack of trust between patients and healthcare professionals.

  This ensures that data leakage and unauthorized modification cannot occur throughout the entire communication. The security analysis and results demonstrate that the proposed model is resistant to a variety of attacks Abounassar et al. (2022).

5 IoT in Healthcare

5.1 The Role of IoT in Healthcare

IoT in Healthcare has been proved a boon both for the doctors and the patients. They can communicate with each other no matter the distance and with great connectivity. This helps the patients get better and faster diagnostics. The doctor can get the data from the patient and can make an informed decision that could led to patient's wellbeing. Also it is very helpful for the patients who are not able to visit the doctor.

The Internet of Things (IoT) has two significant objectives: firstly, the provision of effective patient care training, and secondly, the improvement of disease preventive measures. The objective is to decrease healthcare expenditures and provide accessibility for a broader demographic Zaabar et al. (2021).

By integrating intelligent objects and enhancing the efficacy of healthcare systems, IoT plays a significant role in healthcare. It reduces costs and improves the performance of patients, physicians, hospitals, and health insurance companies. Some of the roles are as follows:

- Remotely monitoring and tracing patient health
- Improving medication management and adherence
- Increasing patient safety and minimizing medical errors
- Streamlining hospital operations and enhancing efficiency
- Enabling predictive equipment maintenance
- Facilitating real-time communication between healthcare providers and patients.

In healthcare, IoT devices are becoming increasingly useful. They can provide early detection of health issues and reduce medical care expenses. The healthcare monitoring system is required for a patient who must be monitored 24 hours a day, seven days a week. The IoT-based health monitoring system can continuously monitor a person's vital health parameters. It can assist patients in an emergency by providing immediate health consultation from a physician located in a remote location. In addition, IoT-based smart systems enable remote monitoring of the patient by a guardian or family member, which is regarded as one of the greatest benefits for saving a life. IoT's function in healthcare is to provide continuous monitoring of vital health parameters, facilitate remote monitoring, and provide emergency health consultation immediately.

5.2 Drawbacks of the current system

Despite the existence of security regulations, such as the Health Insurance Portability and Accountability Act (HIPAA), the healthcare system continues to see everyday occurrences of data breaches, highlighting the limitations and disadvantages of the present security measures. The consequences of these breaches have a detrimental effect on the privacy of patients. There are potential limitations associated with the present security measures used inside the healthcare sector *The Dependency of Healthcare on Security: Issues and Challenges* (2021).

- Deficiency in the effective execution of security standards
- Insufficiency in providing comprehensive training to personnel regarding security protocols
- Insufficient security measures to safeguard against both internal and external cyberattacks
- Limited allocation of resources towards cybersecurity within healthcare organizations
- Inability to effectively address the continuously evolving cybersecurity threats
- The proliferation of electronic health records has led to a growing need for the exchange and retrieval of information across diverse healthcare practitioners. This necessitates the implementation of measures to ensure the security of the information.
- The integration of the Internet of Things inside wireless body sensor networks has resulted in the use of Cloud and Fog computing in healthcare systems. This indicates the need of implementing safe protocols for accessing, storing, and processing sensitive data in healthcare systems.
- Cyber-attacks pose a significant threat to these systems, since they may lead to the unauthorized acquisition of confidential patient information, interruption of healthcare services, and potential injury to patients.
- The absence of uniformity in security standards and practices across various healthcare institutions may be a significant obstacle to the security of healthcare systems.
- Overall, the paper emphasizes the importance of information security and privacy in the healthcare sector and highlights the need for secure methods of accessing, storing, and processing sensitive data.

6 Methodology

This research basically focuses on ensuring the privacy of the patient's data. With a proper configuration and tools we can make this happen. This section would highlight the points on how to keep the data secure and how can the application be improved as and when required.

6.1 Process Overflow

The following figure explains the flow of data from patient to the doctor. The patients sends the details in a file which is then encrypted and stored in the cloud server. The doctor access the cloud server for the patients information and decrypts the same using the secret key. The system then creates the private key and the public key which is then matched with the digital signature. If the digital signature matches, the access is granted to the doctor for the patients details, if the matching fails, the access is denied.

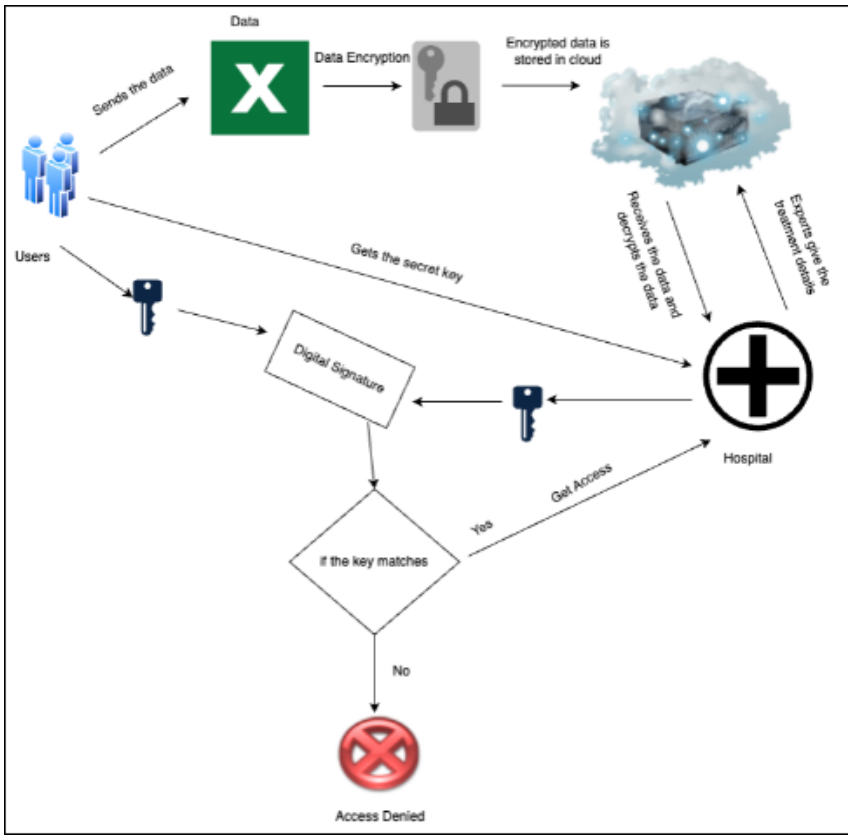

Figure 1: Most common migrations techniques mentioned in cloud system

The main objective of this project is to enhance the security and flexibility of healthcare practitioners' access to cloud-based patient-sensitive data. The results of the experiment indicate that the created secret keys provide a satisfactory level of randomness and uniqueness, hence offering appropriate security for the data held within contemporary healthcare management systems. The suggested methodology aims to optimize the efficiency of data encryption and decryption processes while enhancing privacy protocols. The investigation revealed that the proposed strategy had superior performance compared to earlier methodologies in terms of reducing execution time and cost-effectiveness (Meng et al.; 2022).

7 Design Specification

Designing a tool that would be used for encryption and decryption requires complete understanding of the attributes that are mentioned in the dataset and since we are dealing

with the dataset related to the field of medical, proper care should be taken. This section showcases how the optimization is done to get the desired results.

7.1 Flow Chart

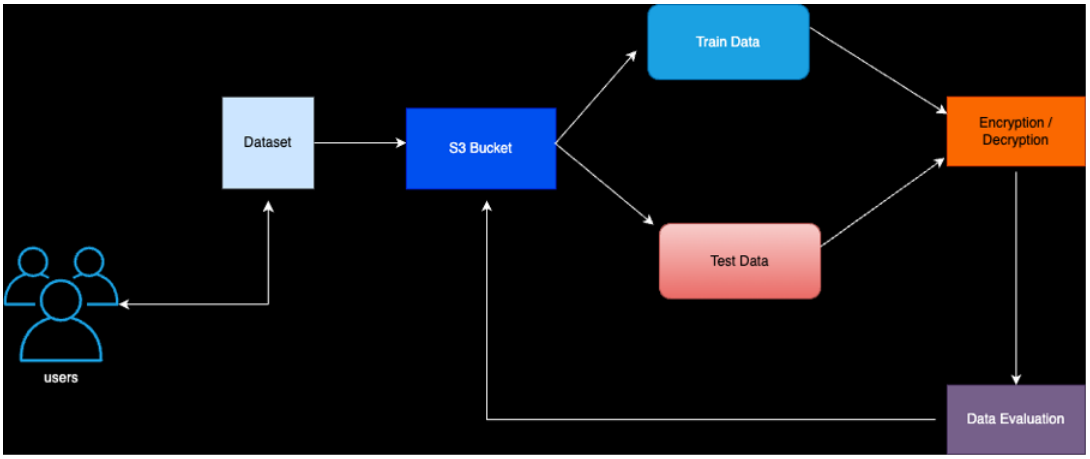

Figure 2: Flow chart

The following flowchart mentions about the basic flow of how data is being optimized and stored. The data is stored into S3 and then retrieved for encryption and decryption which is then optimized and then again stored into S3 Beltran et al. (2022).

By integrating intelligent objects and enhancing the efficacy of healthcare systems, IoT plays a significant role in healthcare. It reduces costs and improves the performance of patients, physicians, hospitals, and health insurance companies. Some of the roles are as follows:

- Remotely monitoring and tracing patient health
- Improving medication management and adherence
- Increasing patient safety and minimizing medical errors
- Streamlining hospital operations and enhancing efficiency
- Enabling predictive equipment maintenance
- Facilitating real-time communication between healthcare providers and patients.

In healthcare, IoT devices are becoming increasingly useful. They can provide early detection of health issues and reduce medical care expenses. The healthcare monitoring system is required for a patient who must be monitored 24 hours a day, seven days a week. The IoT-based health monitoring system can continuously monitor a person's vital health parameters. It can assist patients in an emergency by providing immediate health consultation from a physician located in a remote location. In addition, IoT-based smart systems enable remote monitoring of the patient by a guardian or family member, which is regarded as one of the greatest benefits for saving a life. IoT's function in healthcare is to provide continuous monitoring of vital health parameters, facilitate remote monitoring, and provide emergency health consultation immediately.

8 Implementation

This section explains the encryption and how the process would be implemented. This part also explains about the dataflow and the architecture of the application. Here the source code is mentioned.

8.1 Dataset

This paper uses a public dataset available on Kaggle. The following figure mentions all the columns that would be used for this research.

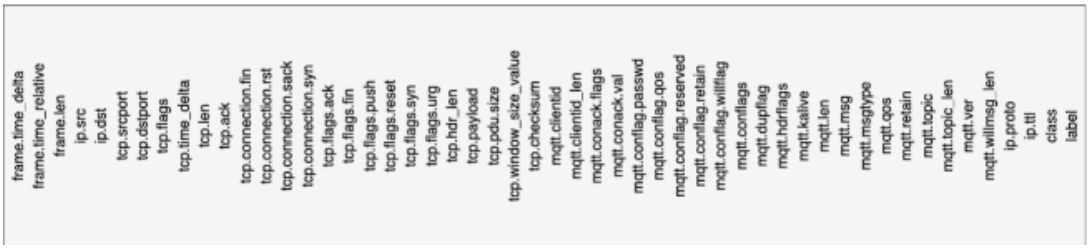

Figure 3: Most common migrations techniques mentioned in cloud system

8.2 Architecture Diagram

The following figure represents the architecture diagram of how the process works. The user adds the data into the system which is stored in the S3 bucket and then encrypted and decrypted to get the optimized data which is again stored in the bucket.

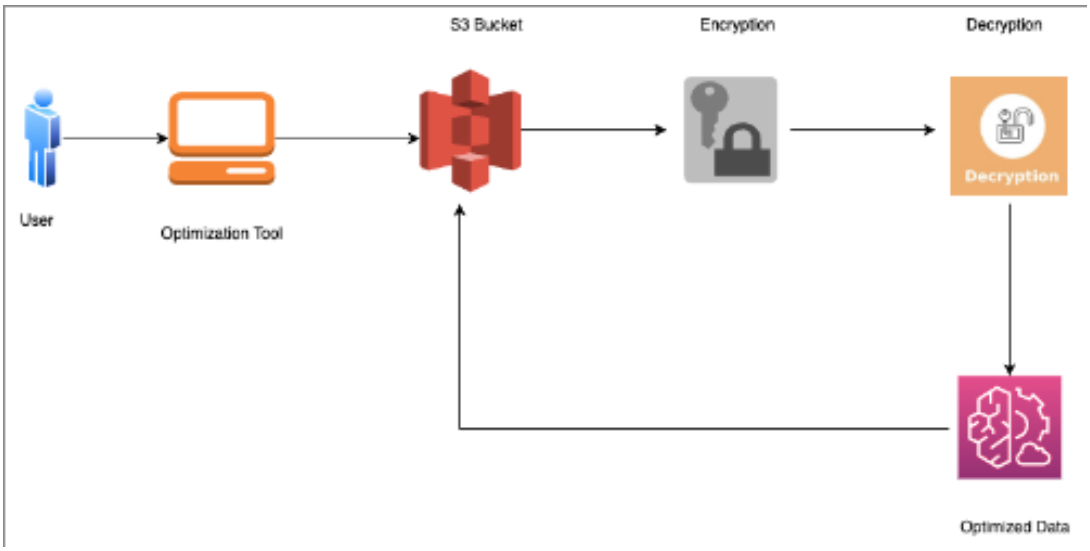

Figure 4: Most common migrations techniques mentioned in cloud system

- Here is the code to help us understand the encryption and decryption process:

```
import time
import matplotlib.pyplot as plt
from cryptography.fernet import Fernet
import pandas as pd

# Generate a random encryption key
key = Fernet.generate_key()
cipher_suite = Fernet(key)

# Load your dataset into a DataFrame
# Replace 'your_dataset.csv' with the actual path to your dataset
your_dataset_filename = 'Attack.csv'
df = pd.read_csv(your_dataset_filename)

# List of columns to encrypt
columns_to_encrypt = ['mqtt.msg', 'tcp.srcport']  # Replace with your columns

encryption_times = {}
decryption_times = {}

for column in columns_to_encrypt:
    data_sizes = [len(str(data)) for data in df[column]]

    encryption_column_times = []
    decryption_column_times = []

    for size in data_sizes:
        data = str(size).encode()  # Creating sample data

        # Encryption
        start_time = time.time()
        encrypted_data = cipher_suite.encrypt(data)
        encryption_column_times.append(time.time() - start_time)

        # Decryption
        start_time = time.time()
        decrypted_data = cipher_suite.decrypt(encrypted_data)
        decryption_column_times.append(time.time() - start_time)

    encryption_times[column] = encryption_column_times
    decryption_times[column] = decryption_column_times
```

9 Evaluation

Here, the screenshots represent creating a bucket in S3 and storing the test data and the train data in their respective folders. There is an output folder created that maintains the versioning, and when we run our code, the different timestamps are recorded. We would be plotting our data in histograms and graphs using various algorithms.

In Figure 4, we are checking the AWS region and creating a new bucket called "iot-sec1".

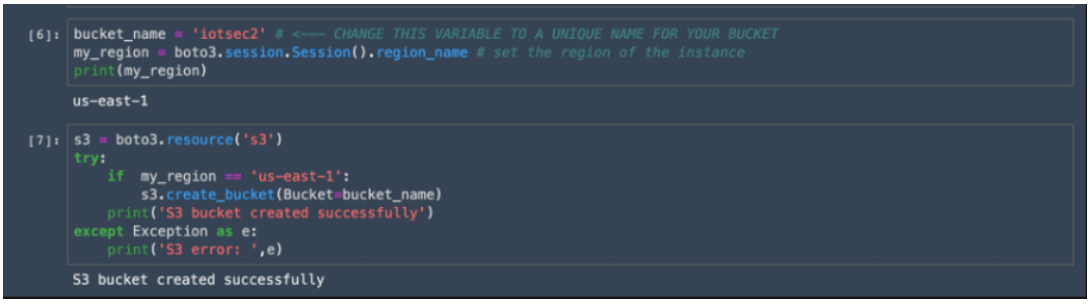

Figure 5: Checking the AWS region and are creating a new bucket.

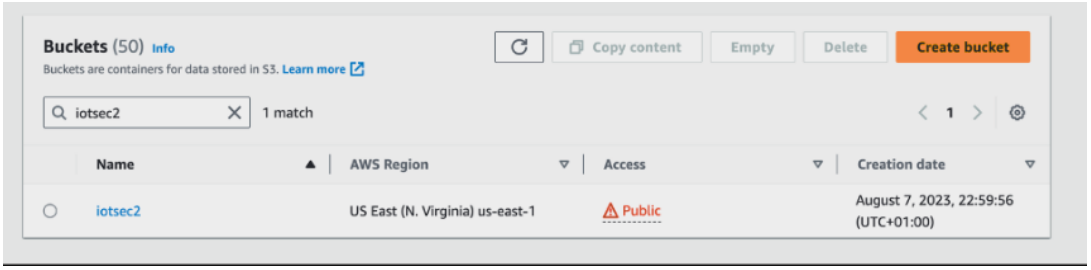

Figure 6: We can see that the S3 bucket has been successfully created.

Figure 7: will create two folders, train and test, which is depicted in Figure 5.

Here, the histogram shows the amount of time it takes to completely encrypt and decrypt the data. Most of the data is encrypted within the time stamp of 0.000 to 0.001, and the same is the result for the decryption.

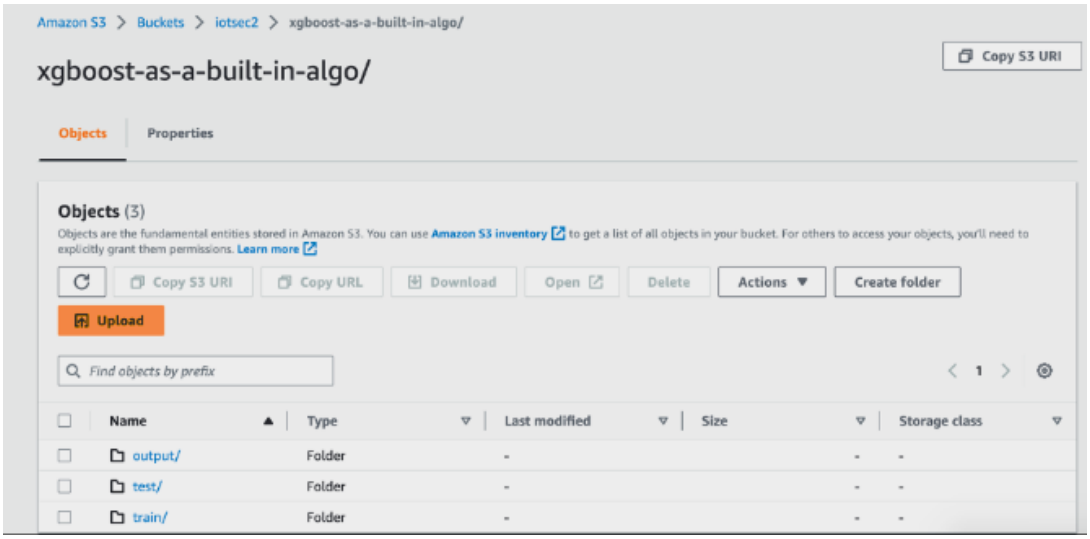

Figure 8: Most common migration techniques mentioned in cloud systems

```
# Plotting
plt.figure(figsize=(12, 6))
for column in columns_to_encrypt:
    plt.plot(data_sizes, encryption_times[column], label=f'Encrypt {column}')
    plt.plot(data_sizes, decryption_times[column], label=f'Decrypt {column}')

plt.xlabel('Data Size')
plt.ylabel('Time (seconds)')
plt.title('AES Encryption and Decryption Time')
plt.legend()
plt.grid()
plt.show()
```

10 Conclusion and Future Work

The primary focus of this research was to use cost-effective security system in an intelligent healthcare system. The patients data was encrypted and decrypted, which ensured that the data was secure. The project aimed to increase the security of the patient's information using the cloud platform. The proposed methodology exhibited a reduction in the duration required for encryption and decryption processes, as well as an improvement in the rates of maintaining confidentiality. The healthcare framework under consideration exhibited reduced energy use, financial expenditure, and processing duration compared to the methodologies investigated. Future research would try to predict and protect the data from various threats that would evolve.

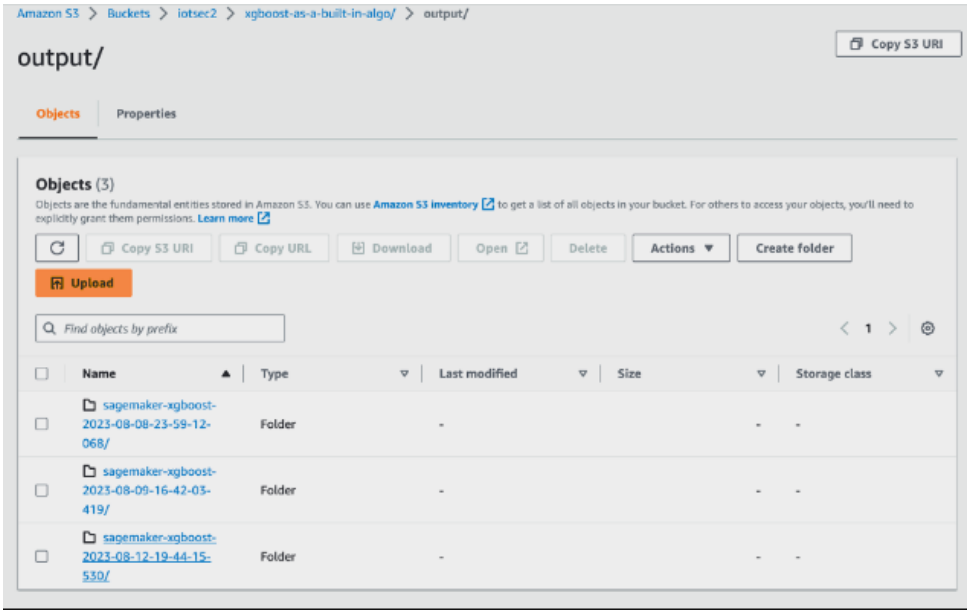

Figure 9: We can see that the output folder created, as seen in Figure 5, has different versions of our code with the timestamp of when it was created.

References

A, P. V., Dayana, R. and Vadivukkarasi, K. (2023). Healthcare data security using blockchain technology, *2023 International Conference on Intelligent Systems for Communication, IoT and Security (ICISCoIS)*, pp. 298–303.

Abounassar, E., Elkafrawy, P. and Abd El-Latif, A. (2022). *Security and Interoperability Issues with Internet of Things (IoT) in Healthcare Industry: A Survey*, pp. 159–189.

Beltran, J. A., Mudholkar, P., Mudholkar, M., Tripathi, V., Valderrama-Zapata, C. and Lourense, M. (2022). Security issues and challenges in internet of things (iot) system, *2022 5th International Conference on Contemporary Computing and Informatics (IC3I)*, pp. 57–60.

Chakraborty, S., Aich, S. and Kim, H.-C. (2019). A secure healthcare system design framework using blockchain technology, *2019 21st International Conference on Advanced Communication Technology (ICACT)*, pp. 260–264.

Challenges in Smart Health Applications Using Wearable Medical Internet-of-Things—A Review (2022). Springer, Singapore.

Data Breaches in Healthcare Security Systems. (2021). *arXiv: Cryptography and Security* .

Elkahlout, M., Abu-Saqer, M. M., Aldaour, A. F., Issa, A. and Debeljak, M. (2020). Iot-based healthcare and monitoring systems for the elderly: A literature survey study, *2020 International Conference on Assistive and Rehabilitation Technologies (iCareTech)*, pp. 92–96.

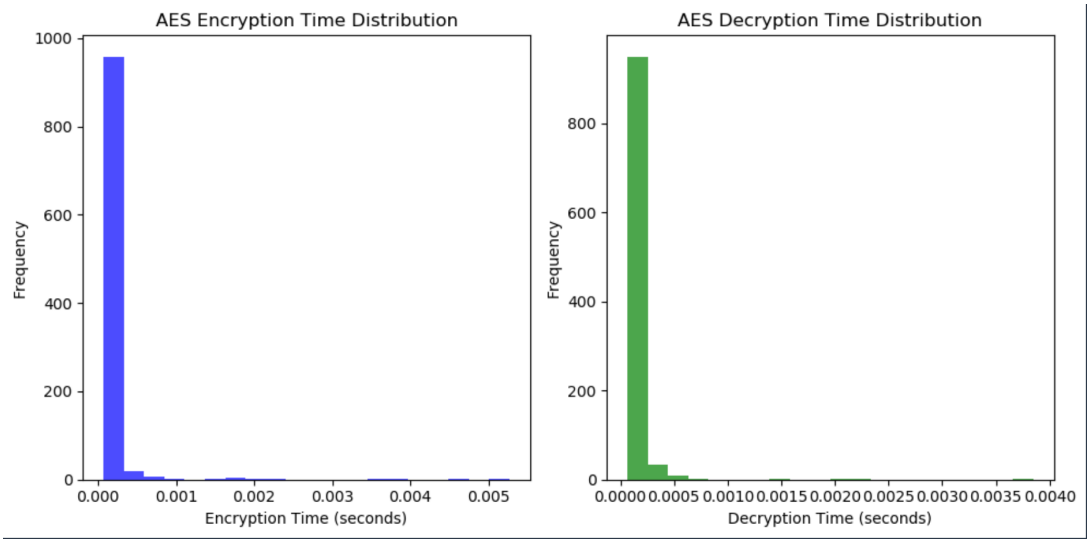

Figure 10: Histogram of Encryption and Decryption Time

Internet of Things Security: Challenges and Key Issues (2021a). *Security and Communication Networks* **2021**: 1–11.

Internet of Things Security: Challenges and Key Issues (2021b). *Security and Communication Networks* **2021**: 1–11.

Karunarathne, S. M., Saxena, N. and Khan, M. K. (2021). Security and privacy in iot smart healthcare, *IEEE Internet Computing* **25**(4): 37–48.

Kaur, K. and Gandhi, V. (2022). Internet of things: A study on protocols, security challenges and healthcare applications, *2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, pp. 1206–1210.

Kumar, A. and Sharma, I. (2023). Enhancing data privacy of iot healthcare with keylogger attack mitigation, *2023 4th International Conference for Emerging Technology (INCET)*, pp. 1–6.

Review of security challenges in healthcare internet of things (2021). *Wireless Networks* **27**(8): 5503–5509.

Security and Privacy Issues in Medical Internet of Things: Overview, Countermeasures, Challenges and Future Directions (2021). *Sustainability* **13**(21): 11645–11645.

Security Issues of IoT in Healthcare Sector: A Systematic Review (2022). Springer, Singapore.

Sowjanya, K. and Dasgupta, M. (2020). Survey of symmetric and asymmetric key management schemes in the context of iot based healthcare system, *2020 First International Conference on Power, Control and Computing Technologies (ICPC2T)*, pp. 283–288.

The Dependency of Healthcare on Security: Issues and Challenges (2021). Springer, Singapore.

Trayush, T., Bathla, R., Saini, S. and Shukla, V. K. (2021). Iot in healthcare: Challenges, benefits, applications, and opportunities, *2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, pp. 107–111.

Zaabar, B., Cheikhrouhou, O., Ammi, M., Awad, A. I. and Abid, M. (2021). Secure and privacy-aware blockchain-based remote patient monitoring system for internet of healthcare things, *2021 17th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pp. 200–205.