A Secure Cloud Based Model of Patient Management System

by

Md. Mehedi Hassan Ridoy
Md. Mumin Ul Bari
Md. Sajjad Hossain Sawran
Mahdee Abdullah Jeem

BACHELOR OF SCIENCE IN INFORMATION AND COMMUNICATION ENGINEERING

Department of Information and Communication Technology
Faculty of Science and Technology
BANGLADESH UNIVERSITY OF PROFESSIONALS
January 2022

APPROVAL

The thesis "A Secure Cloud Based Model of Patient Management System" submitted by Md. Mehedi Hassan Ridoy, Roll No: 18511022; Md. Mumin Ul Bari, Roll No: 18511023; Md. Sajjad Hossain Sawran, Roll No: 18511026 and Mahdee Abdullah Jeem, Roll No: 18511015 Session: 2017-18 has been acknowledged as satisfactory in partial fulfillment of the criteria for the degree of Bachelor of Science in Information and Communication Engineering.

Dr. Rashed Mazumder
Assistant Professor
Institute of Information Technology
Jahangirnagar University

DECLARATION

We hereby declare that This thesis is our unique work, and it was written entirely by us. All of the sources of information used in the thesis have been properly credited. The thesis has never been submitted (in whole or in part) for any degree or diploma at any institution or institute before.

Md. Mehedi Hassan Ridoy
ID: 18511022
Department of Information and Communication Technology
Faculty of Science and Technology
Bangladesh University of Professionals
09 January,2022

Md. Mumin Ul Bari
ID: 18511023
Department of Information and Communication Technology
Faculty of Science and Technology
Bangladesh University of Professionals
09 January,2022

Md. Sajjad Hossain Sawran
ID: 18511026
Department of Information and Communication Technology
Faculty of Science and Technology
Bangladesh University of Professionals
09 January,2022

Mahdee Abdullah Jeem
ID: 18511015
Department of Information and Communication Technology
Faculty of Science and Technology
Bangladesh University of Professionals
09 January,2022

ACKNOWLEDGEMENTS

By the grace of Almighty Allah, we have put in our bravery, patience, and strength to complete the thesis. We would like to express our sincere gratitude to our supervisor Dr. Rashed Mazumder, Assistant Professor, Bangladesh University of Professionals for his valuable and constructive suggestions, continuous support, great encouragement, patience, and immense knowledge. We were immensely inspired by his creativity, foresight, honesty, and encouragement. He taught us the methods to conduct the research and to make the thesis as effective as possible. It was a wonderful opportunity and honor to do the research under his guidance. We would like to thank all the faculty members of Department of Information and Communication Engineering, Bangladesh University of Professionals for dissemination of knowledge during our study, which made it possible for us to focus on the thesis. We are most grateful to our parents for their prayers, their devotion, their support, and their love. Finally, our thanks go to all our classmates who have helped us directly or indirectly to complete the research work.

ABSTRACT

Finding hospital bed in crucial moment is a challenge to normal people. If people could see which hospitals have available beds in one platform, it would ease people's difficulties to get treatment faster. We have designed a model of E-bed system which keeps count of vacant beds in the hospitals and user can find the nearest available beds in hospitals by using bi-linear maps. The system keeps track of information of hospital beds and patients. Medical data of a patient is valuable asset to one which needs to be secured. We have shown a secure way of keeping the data in cloud. User's data will be kept in cloud, that's why securing patient information is the main concern of the system. To secure user data, we have used Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC) as a hybrid algorithm. User's data will be protected by a combination of a symmetric and an asymmetric algorithm.

Keywords: GNSS, E-Bed, AES, ECC, Cloud, RFID, Hybrid Cryptography

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

AES Advanced Encryption Standard

DES Data Encryption Standard

RSA Rivest – Shamir – Adleman

ECC Elliptic Curve Cryptography

PNT Positioning, Navigation, and Timing

SCDS Support Centre for Data Sharing

RFID Radio Frequency Identification

NID National Identity Card

IDE Integrated Development Environment

UML Unified Modeling Language

NumPy Numerical Python

GPU Graphics Processing Unit

CRP C-reactive protein

OHCA Out-of-hospital Cardiac Arrest

CHAPTER 1

INTRODUCTION

1.1 Overview

This chapter provides an overview of the proposed work's background as well as its inspiration. The problem description is then presented so that the research gap may be correctly understood. To demonstrate the success of the suggested model, the work's aims are stated, and the contribution is detailed. Finally, the outline of the thesis book is presented in this chapter.

1.2 Background

The proper movement of patients through a healthcare institution depends on effective bed management. The system helps to find nearest available beds in one interface. Our vision is to secure the interface so that the user information is safe. It encompasses the medical treatment, physical resources, and internal mechanisms required to move patients from admission through discharge while ensuring a secure system. Cybersecurity breaches are becoming an increasingly serious danger to the health care business as a whole, and hospitals in particular. The health care business has fallen behind other industries in terms of protecting its primary stakeholder and hospitals must now invest significant resources and effort in safeguarding their

systems. This is easier said than done, however, because hospitals are extremely technology-driven, complicated organizations with a high degree of end point complexity, internal politics, and regulatory demands. Cybersecurity breaches are becoming an increasingly serious danger to the health care business as a whole, and hospitals in particular. The health care business has fallen behind other industries in terms of protecting its primary stakeholder (ie, people), and hospitals must now invest significant resources and effort in safeguarding their systems.

1.3 Motivation of the Study

In general, early professional treatment in crises is helpful, and its efficacy has been demonstrated in several trials, notably in the case of out-of available hospital beds. Organizations that provide emergency medical services (EMS) and health policy makers explore a variety of ways to improve response times, but time remains a critical concern. Although there is no globally agreed **EMS!** (**EMS!**) response time standard, the most commonly utilized aim is to react to 90% of calls within 9 minutes in urban areas and 15 minutes in rural regions. Elapsed time has a big influence. For every minute that cardiopulmonary resuscitation is delayed in situations of Out-of-hospital Cardiac Arrest (OHCA), for example, the survival rate drops by 10%. **CPR!** (**CPR!**). People in trouble frequently have to rely on the kindness of strangers until an ambulance arrives. In this emergency situations, the system provides information for getting proper treatment immediately.

1.4 Problem Statement

In Bangladesh, the issue of healthcare access is extremely urgent. It is estimated that barely 30 percent of the population has access to primary health services, and the general quality of healthcare in the country remains unacceptable by all conventional

standards.' However, a recent research (Sen and Acharya 1997) suggests that 'the low quality of health care remain ongoing issues' There is a lack of crucial workers, needed supplies, inadequate facilities, and poor quality staffing to blame for the poor performance of the health care system.The problems of emergency medical needs is a increasing day by day. People can not find where there is vacant seats for patients. If the number of occupied and unoccupied beds can be shown in online platform, it would ease a lot of difficulties in critical moment.[1].

1.5 Objective of the study

Overall, this study sought to provide a secure method of alleviating emergency hospital demands. The study was conducted to accomplish the following goals:

(a) To provide Hospital bed information to the patients- how many beds are available.

(b) To select the best hospital for the user via GNSS.

(c) To ensure the security of all information of hospitals and patients, which will be stored in cloud.

(d) To enhance the dynamics of hospital-based cybersecurity capabilities development.

(e) To build a system of hospital cybersecurity in Bangladesh via the interaction of internal organizational dynamics.

1.6 Contribution of the study

A model is proposed for making a system to keep track of occupied and unoccupied hospital beds, which also secures personal information of patients.The research's primary contribution is as follows:

(a) It deals with the smart idea of E-bed system which eases the difficulties of patients in critical moments.

(b) In order to provide security of patient's data in cloud, a secure model has been proposed which includes a hybrid method using AES and ECC algorithm for encryption and decryption.

1.7 Organization of the book

The six chapters of the thesis book are listed below. Introduction and basic overview of the thesis are given in **Chapter 1**, followed by a brief statement of the study's goals. According to the following structure, the remainder of the book is laid out. Researchers in the subject of data security in the cloud employ a variety of models and prior studies, which are discussed in **Chapter 2**. The operating premise of the model is explained in **Chapter 3** along with a full overview of the tools and technologies employed. It will be explained in **Chapter 4** how to use this approach in practice. Results and comparisons with other models are discussed in **Chapter 5**. Conclusions and future directions for this thesis work are presented in **Chapter 6** of this thesis.

CHAPTER 2

LITERATURE REVIEW

2.1 Overview

This chapter includes the previous work of the field of data security. The user's information will be encrypted with AES and ECC, which will work as a hybrid algorithm.

2.2 Encryption Algorithm

2.2.1 AES

According to a comparative review of numerous symmetric approaches, AES takes a very little amount of memory compared to other techniques, and its security is outstanding [2]. As a result of this, AES encryption is faster than RSA encryption [3]. AES is more secure than RSA and DSA,takes more less time to encrypt or decode [4]. In terms of key length, 3DES is over three times as sluggish as AES, whereas AES is nearly 100 times quicker than RSA with the same key length [5]. AES is regarded the finest encryption technology for cloud security since it has a wide range of key sizes, from 128, 192, and 256 bits [6]. As shown in [7], adding more rounds (Nr) 16 to AES requires more computing time to breach the algorithm's security, hence increasing the security of system data.

C. P. A. K. Mandal and A. Tiwari proposed that, AES with DES shows that AES is better because it consumes less memory. The same file size costs 10.2MB, but DES requires 43.3MB. In addition, DES has a faster simulation time than AES [8].

A. A. Hasib and A. A. M. M. Haque proposed that, a hybrid technique is utilized to boost security by encrypting data using AES and managing keys with RSA [9]. To protect Bluetooth communications, use a hybrid technique in which AES keys are encrypted by RSA. This approach leverages the strengths of both of them, making it very secure [10]. AES is employed in conjunction with DES for the transmission of digital motion pictures, which provides increased security due to AES's inability to resist algebraic assaults [11]. W. Tianfu and K. R. Babu proposed that, AES encryption is used first, followed by DES encryption. After AES and DES encryption, data is encrypted using a combined technique of AES and DES, which produces complicated results or cipher code that is difficult to break. AES has previously been employed with a variety of algorithms, including RSA, DSA, and Blowfish [12]. In this article, we will examine the performance of AES when combined with Elliptic curve encryption (ECC). Performance is measured after the user inserts text files utilizing time, storage, avalanche effect, and correlation.

The shield may also be used to protect against a variety of strikes, including asymmetrical attacks like recovery attacks and key attacks, as well as square attacks.

2.2.2 ECC

ECC is a type of public key cryptography that uses both public and private keys to authenticate a user's identity. In the mid-1980s, Koblitz and Victor Miller independently suggested the use of elliptic curves in cryptography [13]. It is a kind of PKC that uses the algebraic structure of an elliptic curve over finite fields to build its algebraic structure [14]. Elliptic curve discrete logarithm (ECDLP) difficulty is critical to ECC security, and this issue can be solved in exponential time [13].

Meanwhile, it should be noted that the efficiency of this method's scalar multiplication algorithm has a significant impact on the overall performance of the algorithm [15]. Regarding the scalar arithmetic level of computing, it is the Hamming weight of the private key that determines algorithm efficacy [16]. The Hamming weight is used to quantify the amount of non-zero digits in a scalar representation.As Hamming weight is reduced, the speed of scalar multiplication performance increases. As a result, scalar recording may be used to reduce the Hamming weight of a private key's scalar form.

An great amount of research has been done since 1985 on elliptic curve cryptography, which was separately suggested by Koblitz and Miller. The general form of an elliptic curve is:

$$y^2 = x^3 + ax + b \tag{2.1}$$

Here, x and y are elements of GF(p) and a and b are integer module p satisfying,

$$4a^3 + 27b^2 \neq 0(modp) \tag{2.2}$$

Point addition and point doubling are the most common ECC procedures. There was no easy way to multiply elliptic curves.

Table 2.1: NIST Recommended Key Size

Symmetric Key Size (bits)	RSA and Diffie-Hellman Key Size (bits)	Elliptic Curve Key Size (bits)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

Fig 2.1 shows the ECC Point Addition [17]:

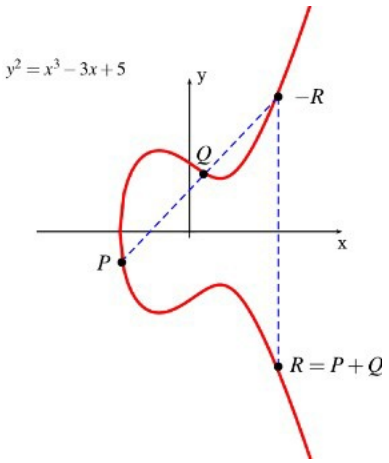

Fig. 2.1. ECC Point Adddition

Fig 2.2 shows the ECC Point Doubling [17]:

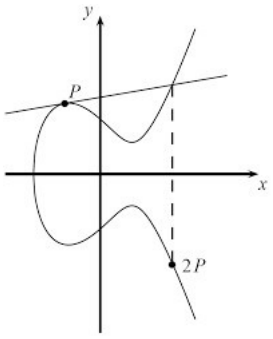

Fig. 2.2. ECC Point Doubling

Fig 2.2 and Fig 2.3 demonstrate the addition and doubling of elliptic curves. As a result of Elliptic addition, it is permitted for a straight line connecting two points to fall on the xy plane at point R. To get at the ultimate conclusion, the negative equivalent is found on the opposite side of the plane. Similar to point doubling, a tangent on P is allowed to fall on the x-y plane and its negative intercept is used to double the point P. PKC had relied on RSA for the better part of a quarter of a century.

Standardization of ECC is critical for enabling practical, efficient deployment and encourages global enterprises to use it.The National Institute of Standards and Technology (NIST) is a non-regulatory government body housed inside the Technology Administration of the United States Commerce Department. NIST specifies ECC algorithms that are considered secure for use in cryptographic applications [18]. The efficiency of scalar multiplication (kP) is critical to the performance of an ECC. In terms of security, a 160-bit ECC key offers the same degree of protection as a 1024-bit RSA/DSA key. To secure RSA keys, 1024 bits were necessary for corporate usage and 2048 for exceptionally important keys. If you want the same level of security, you can get it with a shorter key length using ECC. ECC requires a key length of at least 160 bits in order to be secure [19].

When used in the following situations, ECC is advantageous:

(a) Internet-based application, such as online banking or e-commerce, that requires a high amount of online transactions or web server requests.

(b) Devices with limited processing power and memory capacity, such as mobile devices.

(c) Portable, tiny, and lightweight smart cards and cryptographic tokens with minimal processing power, parameter storage, and memory.

2.2.3 Hybrid Algorithm

Due to simultaneous resource sharing across all users, cloud storage is growing in popularity. Owners of data prefer cloud storage versus alternative options because it is always-on and always-available. Data integrity and preservation should be checked to ensure the system's safety in this regard. AES and ECC are offered to increase the system's security. Without the trusted center, Shamir secret sharing is utilized

to distribute and manage a system. However, despite the fact that the suggested combination strategy boosts system security, it still requires a significant amount of computing resources and time [20]. ECC and AES combine to offer the most sophisticated and efficient encryption approach for cloud storage. Single AES is somewhat slower than the hybrid (ECC-AES) technique because to its higher key size, while the hybrid method provides for a smaller key size and a quicker security mechanism for safeguarding the data. Due to the fact that ECC's primary attribute is a short key size, when AES employs ECC for encryption, the key size is raised [21].

In order to keep data safe, created a hybrid cryptographic method for cloud systems. The eye-OS implementation of the hybrid algorithm is a combination of the well-known symmetric (AES-128) and asymmetric (RSA-1024) algorithms. AES-128 is used to encrypt the file before it is uploaded to the cloud storage system by the cloud user. RSA-1024 is used to encrypt the secret key, which can only be decrypted with the public key. Because only AES is used for data encryption, this approach can handle big files without sacrificing security or speed [22].

Various hybrid cryptographic models were studied in and the authors recommended using AES and FHE, which may address concerns such as data confidentiality, privacy and integrity, among others. Data Confidentiality, Integrity, Authorization, Freshness, and Non-Repudiation are some of the primary security concerns that cloud computing presents [23]. Implemented a hybrid security strategy to protect medical patient data stored in the cloud [24]. P-AES, a modified version of the AES algorithm, is used in combination with RSA to protect medical data stored in the cloud and keep it private and secure. Using their hybrid methodology, they can only protect text, not pictures or videos.

A. R. R.Kiruthika and S.Keerthana propesed that, we looked at the security concerns that cloud services face, as well as some of the most important cloud security issues. With the use of AES encryption, their strategy is able to address these critical

difficulties [25]. It has been determined that 3DES, DES and RC2 are the best algorithms for symmetric encryption in terms of speed and throughput. It's only a matter of using AES encryption to protect data stored in the cloud. Uploading data to the cloud will need the usage of a different program or piece of software that encrypts the information before it leaves the user's computer. Data uploads and downloads need the use of specialized software for key management. It was built in utilizing several techniques like as AES, ECDSA and SHA256 to ensure the security of data contained therein. Using these methods, you may safely send, receive, upload, and retrieve data from the cloud. ECDSA and SHA256 offer authentication and integrity checks, while the AES Algorithm ensures secrecy [26].

2.3 Related Problems

At the moment, data security is a key concern, since it may be hacked in a variety of ways, both external and internal. Different encryption algorithms are used to safeguard data transmission over the Internet. The disadvantage of these systems is that they need a high key size, a huge amount of memory, and a significant amount of computer power to safeguard the data. As with AES encryption, a key is generated immediately after the input file is uploaded, and as previously stated, AES employs the symmetric key encryption technique, which utilizes a single key for both encryption and decryption. Thus, if a third party obtains knowledge of the single key, the input file may simply be decrypted and re-encrypted, masking the fact that the input file has been read by someone else. While AES is a safe algorithm, its security may be undermined if the single key is known. On the other hand, ECC employs asymmetric key encryption, in which two keys, a public and a private key, are used for encryption and decryption, respectively. This is why its security level is better, since it is difficult for hackers to break both keys simultaneously. Additionally, ECC is well-known for its reduced key size. ECC can give the same degree of security as

other methods while using a lower key size. There is a need to design a system that secures data in the cloud at a low computational cost and with little time spent on the encryption/decryption process. In our suggested model, we incorporate the features of both techniques [27].

2.4 Related Works

Numerous scholars have written substantial amounts of literature on cloud security and privacy. This section of the article discusses many of these evaluations on data security in the cloud.

In 2015, Abbas and Maryoosha published a paper outlining a dependable, efficient, and scalable technique for enhancing the security of Cloud Competing data storage. Their method focused on three primary facets of private key generation: the Private Key Generator (PKG), the Trusted Cloud (TC), and the User [28].

This study described a novel architecture for enhancing data security in cloud computing. This was accomplished via the use of two encryption techniques: modified identity-based cryptography (MIBC) and the Elliptic Curve Integrated Encryption Scheme (ECIES). Their study purpose was to develop reliable, practical, and scalable approaches for enhancing data security in the cloud [28].

High-performance AES will be developed in an effort to increase its widespread use. The user's data is encrypted using the AES technique before it is delivered to the cloud. As a result, the user must decrypt the data before they can access it. Cloud storage does not include the original text. The keys are stored on a key management server. According to the study, this method of encryption secures both the encrypted data as well as the encryption keys. There were no flaws or restrictions detected in the AES encryption algorithm's storage capacity or efficiency [29].

Kumari et al. developed an ECC-based mutual authentication architecture for secure communication in this publication. This model consisted of three stages. There

are three phases: setup, extraction, and mutual authentication and session. Users authenticate one another and establish a session key. Participants may connect securely over a public communication network by using the session key. Additionally, the protocol prohibits the measurement of bilinear pairing, emphasizing how efficient it is in the communication domain [30].

According to, a proposed encryption method incorporates the chaos encryption algorithm and the Elliptic Curve Cryptography (ECC), which processes the data using one-dimensional logistical sequencing before it is encrypted, and then the second step encrypts it with an ECC encryption algorithm to provide the second level of security [31].

2.5 Cloud Based Bed Sharing Model for Hospital

Allen et al. describe a client-server system for generating a request for a bed for a particular patient, receiving a list of available beds, and identifying a bed for the patient [32].

The Iranian Ministry of Health and Medical Education (MOHME) created a nationwide bed management system in 2012 to handle cross-hospital patient referrals in hospitals. This approach was also designed to accommodate victims of mass-casualty events [33].

Create a model for shifting bed status in hospitals . The model is represented by the Web Services Description Language standard, which may be used as an interface for data gathering from the Hospital Information System. Simple Object Access protocol may be used to convey hospital bed data. All hospital bed status logs are stored in the data warehouse. In addition, provide a web application to analyze bed status logs and report available beds in hospitals [33].

To achieve a more perfect bed management system, how to preserve patient quality under the premise of quality care, and how to reduce the average hospital stay in

patients with a more suitable arrangement, enhanced communication between hospital management and patients is still required [34].

Allen et al. describe a client-server system that creates a request for a bed for a specific patient, gets a list of available beds as a selection, and finds a bed for the patient [35].

2.6 RFID related Hospital Bed System Overview

R. Want and A. Hopper proposed that, find users in intelligent office settings, an Active Badge locating system is utilized,It communicates via a network of beacons via pulse-width modulated infrared signals. Other ways that employ radio frequency or Ultra-Wide-Band technology to determine the user's position have also been proposed [36]. To determine the tag's and antenna's range, we replicated hospital bedside and nursing station conditions. The report offered various suggestions for resolving implementation challenges in hospitals [37].

Li et al. implemented a mobile health management system that applies RFID and mobile technology to find and identify people and objects inside and outside hospitals. In particular, in, when an unknown epidemiology such as severe acute respiratory syndrome (SARS) suddenly occurred in 2003, it was possible to effectively reduce the number of infected patients and strengthen the infection control process. infected patients [38].

Janz et al. demonstrated an RFID application in use in a hospital's emergency room. They concluded that data gathered from tagged patients might be used to improve medical procedures, decision-making, and resource management [39].

Fisher Monahan indicates that many hospitals are beginning to implement RFID tracking applications. Inventory, patient identification and personnel management [40].

In Table 2.2, There is a comparison of several cloud-based systems displayed.

Table 2.2: Cloud Based E-Bed Systems

Authors	**Proposed Model**	**Method**	**Aspects**
P.P *et al.* [2]	Evaluation of cryptographic algorithms.	AES,DES ,RSA,blowfish	Integrity is maintained
Mahajan *et al.* [4]	Study of encryption algorithm	AES,DSA,RSA	Integrity is maintained
Wang *et al.* [5]	Timing evaluation of cryptographic algo- rithms	AES,DES,RSA	Integrity and confidentiality
Pancholi *et al.* [6]	To secure data storage	AES	AES Encryption Decryption
Kumar *et al.* [7]	To modify AES algorithm for data security	AES	Increasing the security
Koblitz *et al.* [13]	Description of ECC	ECC	Integrity and confidentiality
Nimbhorkar *et al.* [14]	Survey on ECC	ECC	confidentiality is maintained
Ansari *et al.* [15]	High-performance architecture of EC scalar multiplication	Scalar multiplica-tion algorithm	Integrity and confidentiality
Hankerson *et al.* [18]	Software implementation	ECC	Integrity and confidentiality
Mendonca *et al.* [21]	Data security in cloud	ECC,AES	Integrity and confidentiality
Badal *et al.* [23]	Hybrid encryption	AES,FHE	confidentiality is maintained
Zhang *et al.* [24]	Medical data storage security	AES,RSA	Confidentiality, Integrity and Authorization
Rehman *et al.* [27]	Hybrid AES-ECC model	AES,ECC	confidentiality is maintained

Authors	**Proposed Model**	**Method**	**Aspects**
Dickson *et al.* [28]	Two-level cryptographic technique	AES,ECC	confidentiality is maintained
Kumari *et al.* [30]	User authen-tication protocol	ECC	Integrity and confidentiality
Boaden *et al.* [32]	Bed management system	Client server system	confidentiality is maintained
Lia *et al.* [31]	Encryption algorithm	ECC	Integrity is maintained
Abedian *et al.* [33]	Cross hospita bed management	Web Based	Integrity
Allen *et al.* [35]	Innovative hospital bed	Client server systemt	confidentiality is maintained
Baliga *et al.* [41]	Green cloud computing:	Client server system	Integrity is maintained
Hopper *et al.* [36]	Location system	Active Badge locating system	Integrity and confidentiality
Huang *et al.* [38]	service system	RFID	Integrity and confidentiality
Janz *et al.* [39]	the future with RFID	RFID	Integrity is maintained
Monahan *et al.* [40]	Tracking the social dimensions	RFID	Integrity and confidentiality

CHAPTER 3

TECHNOLOGIES AND TOOLS

3.1 Overview

This chapter explains the technology and techniques that were utilized in the study and offers a full explanation of each one. The tools and technologies presented above will give a foundation for comprehending our suggested paradigm.

3.2 Technologies

This section discusses the technology used for the project.

3.2.1 Tracking(GNSS)

At first, the system will find the nearest hospitals which have available beds and which hospital should be the best one for the patient. GNSS is used for this feature. Global Navigation Satellite Systems (GNSS) are made up of constellations of Earth-orbiting satellites that broadcast their coordinates, networks of ground control stations, and receivers that use trilateration to figure out where the ground is. GNS systems are used in all types of transportation, from space stations to planes to boats to trains to public transportation. Telecommunications, land surveying, law enforcement, emergency response and precision agriculture are all examples of where PNT

is important. PNT is also used in finance, mining, law, and scientific research. They are used to regulate computer networks, air traffic, and electricity grids, among other things.

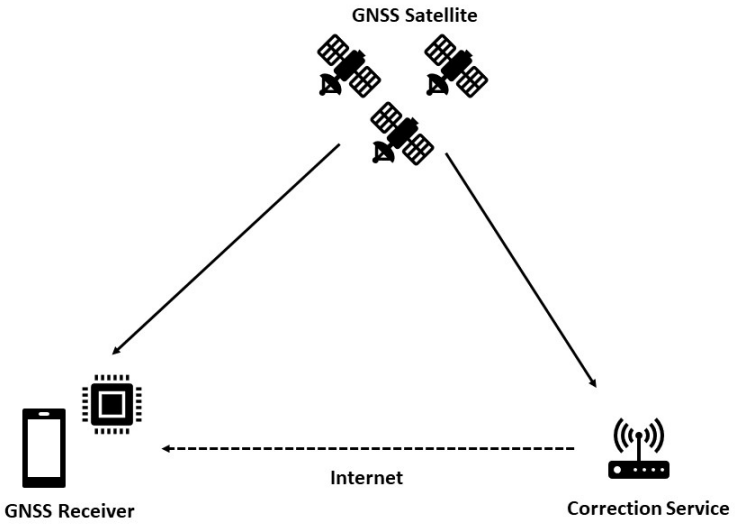

Fig. 3.1. GNSS Data Transmission.

Four criteria are used to evaluate GNSS performance:

(a) **Accuracy:** The discrepancy between the position, speed, or time of a receiver measured and its true value;

(b) **Integrity:** A system's ability to establish a level of trust and, in the case of a data anomaly, to generate an alert;

(c) **Continuity:** A system's capacity to operate continuously;

(d) **Availability:** The proportion of time that a signal meets the above-mentioned standards for accuracy, integrity, and continuity.

When the International Committee on Global Navigation Systems (ICG) completes its work, especially in ensuring interoperability across the global systems, a

GNSS user will be able to use a single device to receive signals from different satellite systems. This will result in more data collection, especially in urban and hilly areas, as well as increased precision in time and location measurements. To take advantage of these advancements, GNSS users must keep current on GNSS-related advances and have the capability to exploit multi-GNSS signals.

Thus, the particular aims of the United Nations Programme on Space Applications' GNSS priority area are to demonstrate and explain GNSS signals, codes, biases, and practical applications, as well as the consequences of projected modernization.

3.2.2 Data Accumulation

Data will be collected from the user of our system. If one user entered in our system, he or she should give his basic information like his location, and mobile number for the registration.

3.2.3 RFID

RFID is used to generate tags which will be attached to user NID and hospital bed.

3.2.3.1 What is RFID?

As the name suggests, RFID stands for "radio-frequency identification," and it refers to a system that uses radio waves to read digital data recorded in RFID tags or smart labels (described below). An RFID tag or label is scanned by a device, and the resulting data is entered into a database. Barcode asset tracking software, on the other hand, has a number of disadvantages. RFID tag data can be read beyond the line of sight, while barcodes need to be aligned with an optical scanner to be read.

3.2.3.2 How does RFID work?

Automated Identification and Data Capture (AIDC) refers to a collection of technologies that include RFID (AIDC). Computer systems may be programmed to recognize and gather data about items using AIDC technologies without the need for human participation. Radio waves are used in RFID systems to achieve this. At the most basic level, RFID systems are made up of a tag, a reader, and an antenna. Radio-frequency identification (RFID) tags have integrated circuits and antennas that communicate data to RFID readers (also called an interrogator). Data from the radio waves is subsequently processed by the reader. It is possible to save and subsequently analyze data obtained from the tags through a communications interface, and then send that data to a host computer system for analysis. Fig 3.2 shows the RFID Architecture [42]:

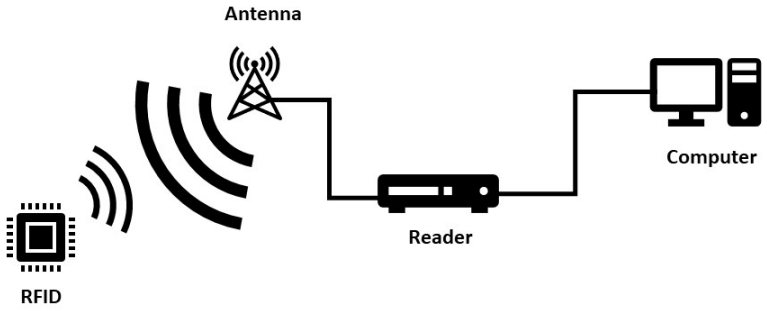

Fig. 3.2. RFID Architecture

3.2.3.3 RFID tags and smart labels

An RFID tag is made up of an integrated circuit and an antenna, as indicated above. As an added precaution, the tag is covered in a layer of protective material to keep the parts together and safe from the elements. The application dictates the kind of protective material. In the case of employee ID badges with RFID tags, the tags are usually inserted between layers of tough plastic. It is possible to use RFID tags that are either passive or active in a number of ways. Passive tags, which are smaller and less costly to deploy, are the most common kind of tag. Before they can send data, passive tags need to be "charged up" by the RFID reader. An active RFID tag has an integrated power source, allowing it to transmit data at all times, unlike passive RFID tags.

Unlike RFID tags, smart labels use both RFID and barcode technologies in the same label. A barcode and other written information may also be on the label, which is constructed of an adhesive label integrated with an RFID tag inlay. While programming RFID tags needs specialized equipment, smart labels may be encoded and produced on demand using desktop label printers.

3.2.4 Cloud

Cloud architecture refers to the technological components that create a cloud, where resources are pooled and shared via a network utilizing virtualization technologies. The following are the components of a cloud architecture:

(a) A platform for the front end (the client or device used to access the cloud)

(b) A single or more back-end platforms (servers and storage)

(c) A way for delivering services through the cloud

(d) A network for establishing connections between cloud clients, servers, and storage

When combined, these technologies offer a cloud computing architecture on which applications may operate, enabling end users to take use of cloud resources' capabilities.

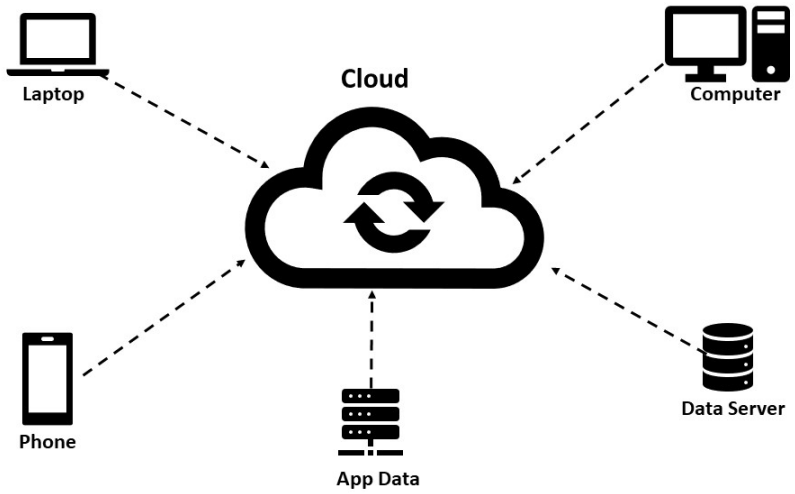

Fig. 3.3. Cloud System

As the computing industry undergoes a tremendous shift in the twenty-first century, this service provisioning model for computing utilities predicts that computing services would be easily accessible on demand, much like other current societal necessities. The promise of huge cost savings and enhanced IT agility is offered by the Cloud Computing concept. Due of cost restrictions, this technology is deemed essential for government and business adoption. Traditional methods of designing and managing data centers and corporate applications are being put to the test by the advent of cloud computing [43]. According to experts, cloud computing is already in use; nevertheless, security and compatibility remain the main obstacles to its widespread acceptance. [44] The fundamental security services for information security include

ensuring the confidentiality, integrity, and availability of data (CIA). Data security gets more challenging in cloud computing due to the inherent cloud features.

3.2.5 Security Services for Cloud

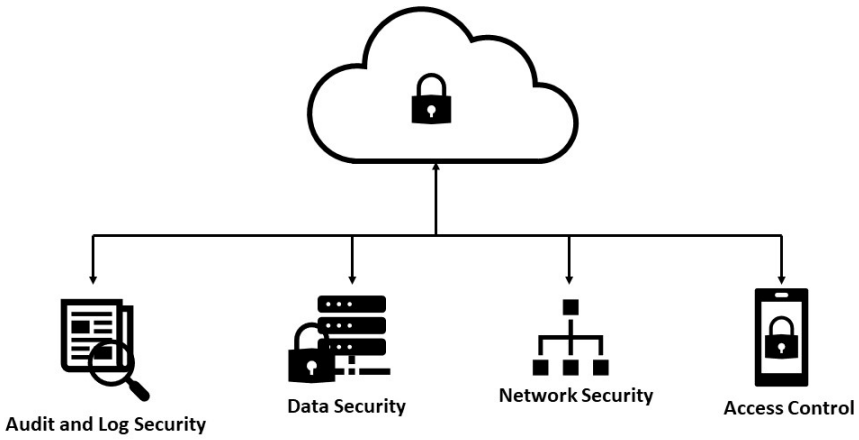

Fig. 3.4. Security Services for Cloud

Cloud computing is one of many differentiated computing models that enables the provision of multiple services regardless of location or medium, and that are readily available from any place, such as infinite database storage, networks, and communications.

Its alluring characteristics have resulted in an ever-increasing dependence on the cloud, resulting in a tremendous amount of data and generating worries about privacy and security. Significant disadvantages of cloud services, including data security and breaches, may be caused either purposefully or accidentally by cloud users. As a result, access to data should be restricted to unauthenticated and unauthorized sources. For this reason, encryption and decryption is necessary. Generally, there are two types of algorithm for encryption, which are:

(a) Symmetric key encryption

(b) Asymmetric key encryption

Public-key cryptography is another name for asymmetric key encryption. In order to decode and encrypt the communication, it comprises a public and private key combination. In addition, symmetric key encryption, where data are encrypted using a single private key and subsequently decoded, is also used to protect data. In order to keep the communication safe from hackers, the private key is used to encrypt the message. Because the key size is so enormous, it is difficult to implement symmetric cryptographic methods because of the security concerns. Table 1 contains a list of all the abbreviations used in this article [45].

Table 3.1: Acronym Table

AES	Advanced Encryption Standard
ECC	Elliptic Curve Cryptography)
RSA	Rivest–Shamir–Adleman
DES	Data Encryption Standard
PHECC	Polynomial-based hashing elliptic curve cryptography
NIST	National Institute of Standards and Technology
EAP	Extensible Authentication Protocol
CHAP	Challenge Handshake Authentication Protocol
GDLP	Generalized Discrete Logarithm Problem
API	Application Programming Interface
CSP	Cryptographic Service Provider

3.2.5.1 Encryption

Encryption may help you safeguard the data you transmit, receive, and save when you use a device to communicate. Text messages kept on your smartphone, jogging records saved on your fitness watch, and banking information received via your online account are examples of what you may save on your device. Using encryption, you may jumble plaintext such that it can only be read by the person who knows the

secret code, also known as a decryption key, to decipher it. It contributes to the protection of sensitive information via data encryption. Gigabytes of personal information are handled and saved online, either in the cloud or on servers that maintain a continuous connection to the internet. As a result, it's practically difficult to do any kind of business without your personal information being part of an organization's networked computer system, which is why it's critical to understand how to help keep such information private. It is a process of converting the original text into a non-readable version known as the cipher text. NIST (National Institutes of Standards and Technology) announced AES as a government information processing standard in 2001. High security, efficiency and ease of use make AES a popular encryption method.Symmetric block ciphers employ the same key for both encryption and decryption. As a block cipher approach, it will encrypt and decode the whole block of data at once. There are 3 block ciphers that are used in this algorithm: AES-192, AES-128, and AES-256. Each block size is represented by a different number of rounds of processing, such as 10, 12, or 14 for a 192-bit key and 256-bit keys, respectively. The acronym for elliptic curve cryptography (ECC) is ECC. When compared to other asymmetric algorithms, ECC delivers superior security with a reduced key size. ECC 160-bit encryption provides the same degree of security as RSA 1024-bit encryption. With a tiny key size, a high degree of security may be obtained. On the other hand, another benefit of this approach is that it requires less memory resources for calculation. To break ECC, we nearly double the amount of computing required to crack RSA.

3.2.5.2 Decryption

Reversing the encryption of a piece of text is known as "decryption." After encryption with the key, plain text is changed into cipher text, and the cipher is decrypted using the key to return to the original text. As part of the fundamental data protection

standards, cryptography must provide the following: authentication, confidentiality, integrity, and non-repudiation [46].

Decryption is the inverse of encryption; it is the process by which plain text or regular data is turned to a cipher. A cipher, sometimes referred to wrongly as a code, is a method in which each letter of a plain text message is substituted with another letter to disguise its meaning. To decrypt a message, you'll need a key, which is an algorithm that specifies how the message was encrypted. Julius Caesar delivered communications using one of the earliest and simplest ciphers, in which each letter was replaced with the letter three positions later in the alphabet. Then, in place of A, a D would be used. The secret to Such a cipher might be "Shift right by three," or anything along those lines. A key is a mathematical algorithm or a method for solving a mathematical problem with a finite amount of calculations, typically by repeating particular operations or stages. f(x) = y is an outstanding example of an algorithm; it is a formula that illustrates the relationship between two components in a Cartesian coordinate system. It is claimed that "y" is a function of x, which means that there is a corresponding value of y for every value of x. Assume that 2 x = y is established; then the function's key is established, and all potential values of x and y may be mapped. This is, in a nutshell, what happens during decryption. The case given is one that might be readily solved using so-called "bruteforce" techniques. Brute force decryption is a technique of decryption in which, in the absence of a key, a cryptanalyst solves a cipher by testing all potential keys. This is impractical for the majority of ciphers without the aid of a computer, and brute force is nearly impossible for the most complex current ciphers. Assume, however, that one is presented a graph with the following x and y coordinates: 1, 2; 2, 4; 3, 6, and so on. Even without the key, it would be quite straightforward to deduce from these figures that 2 x = y using brute force. This is an illustration of "insecure" encryption. In comparison, some of the encryption technologies used today for financial transactions, cellular phone

conversations, and other purposes are exceedingly "strong." Strong encryption is exemplified by a circumstance in which decryption is impossible without knowledge of the key.

3.3 Used Libraries

This section offers an overview of the libraries used in the work.

3.3.1 Libraries

Libraries have made it much easier to build alternative models than before. The suggested model may be implemented quickly and simply with the help of libraries such as Sys, Random, JSON, RE, Base64, Time, OS, and CSV .

Sys: Python's sys module has a wide range of methods and variables for working with the Python runtime environment. It offers access to the variables and functions that interact significantly with the interpreter, making it possible to operate on the interpreter.

Random: To create random numbers, Python has an in-built module called the Random module. As the term implies, these aren't genuinely random numbers. Using this module, you may generate random integers, display random values for a list or string, and more.

JSON: JavaScript Object Notation is the full form of JSON. Script (executable) files are used to store and transport data, which is written in a computer language. Python has a module named JSON that includes support for JSON. Python scripts may take advantage of this capability by importing the JSON package.

RE: Syntax of Regular Expression. A regular expression (or RE) defines a collection of strings that match it; the methods in this module let you to determine if

a given string matches a given regular expression. A regular expression (abbreviated regex or regexp; sometimes called a rational expression) is a string of characters that defines a search pattern. Typically, string-searching algorithms utilize such patterns to perform "find" or "find and replace" operations on strings, or to validate input.

Base64: The Base64 module in Python offers methods for encoding and decoding binary data to and from Base64-encoded format. It conforms to RFC 3548's Base64 encoding and decoding specifications. Base64 encoding techniques are frequently utilized when it is necessary to encode binary data that must be stored and transmitted across ASCII-compatible media. This is to ensure that the data remains unaltered throughout transfer.

Time: It is possible to express time in code using objects, integers, and texts using the Python time module. It may also be used for various purposes, such as waiting for code execution and determining the code's efficiency.

CSV: CSV (Comma Separated Values) is the most often used import/export format for spreadsheets and databases. The CSV format was widely used for many years previous to attempts to standardize it in RFC 4180. Due to the lack of a well-defined standard, small discrepancies in the data produced and consumed by various applications frequently arise. These distinctions can make processing CSV files from many sources a pain. While the delimiters and quotation characters differ, the general structure is similar enough that a single module capable of effectively manipulating such data may be written, concealing the intricacies of reading and writing the data from the programmer.

PIL: The Python Imaging Library is well-suited for picture archiving and batch processing. The pillow package in Python may be used to create thumbnails, convert photos between formats, and print images, among other things.

CHAPTER 4

SYSTEM DESIGN AND METHODOLOGY

4.1 Overview

This chapter will go through the research's methodology. The experimental setup, aim, hybrid cryptography architecture, system model, and encryption-decryption model will also be discussed in this chapter.

4.2 Experimental Setup

All of the research was done on a laptop with an Intel Core i7-8750H (2.2 GHz to 4.1 GHz), 16GB of DDR4 RAM, and an NVIDIA GeForce GTX 1050 TI 4 GB Graphics Processing Unit (GPU) . And PyCharm Integrated Development Environment (IDE) was used for running the experimental model. PyCharm is a Python-specific Integrated Development Environment (IDE) that includes a comprehensive set of important tools for Python developers. These tools are tightly integrated to produce an ideal environment for productive Python, web, and data science development.

4.3 Hybrid Cryptography Architecture

The purpose of cryptography is to allow two individuals to send a message in such a way that others will be unable to decipher it. There are several ways to accomplish this, but we'll focus on techniques for modifying the text in such a way that the receiver may reverse the change and recover the original content.

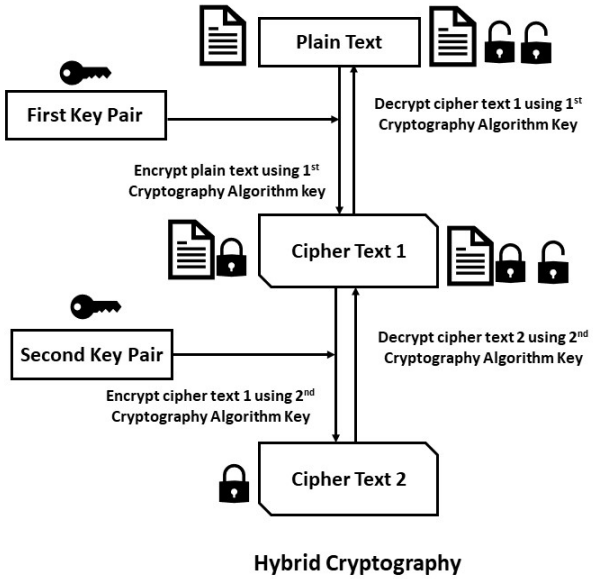

Fig. 4.1. Hybrid cryptography architecture

Modern cryptography is built on efficient encryption methods that are utilized to give greater security. Asymmetric and symmetric security systems are increasingly built with more complicated functions or key generation concepts to give greater security. However, even today, several attacks on current cryptographic algorithms have been documented. A strong cryptography algorithm is designed around the kind of method and its computational difficulty in order to prevent attackers from identifying the message that is to be sent to target nodes. Cryptography is based on mathematical concepts that yield various algorithms referred to as cryptographic Algorithms. A cryptographic algorithm, or cipher, is a mathematical function that is employed in the process of encryption and decoding [47].

4.4 System Model

In this section we will discuss about our whole system through architecture, workflow, how data is shared and accessed through cloud.

4.4.1 UML Diagram

The system model has been built in Unified Modeling Language (UML). As a general-purpose, development-oriented, modeling language, the Unified Modeling Language (UML) is aimed at helping software engineers envision the design of their systems. To build up the design, Entity-Relationship Diagram, Use Case Diagram, Class Diagram and Sequence Diagram has been proposed below.

4.4.1.1 E-R diagram:

Entity Relationship Diagrams (ER Diagrams) show the relationships between various "entities," such as people, things, and ideas, inside a system. An entity is a piece of data that is distinct from the rest. An ER diagram depicts an entity as a rectangle.

For the system, a full module of the DBMS architecture is shown by the ER Diagram. The entities are User, Hospital, Area, Vendor, Cloud, Bed, Admin and Payment. At first, an user can search for hospitals when in need. Then the system will collect the location from user device and search for nearest hospitals. The system will show which hospital has how many available beds. The user can book the beds at the right hospital without any hassle. The system will be controlled by the vendor and the admin of hospitals will monitor the overall booking process. All the information will be stored in cloud and by the permission of vendor the hospital's admin can access the data.

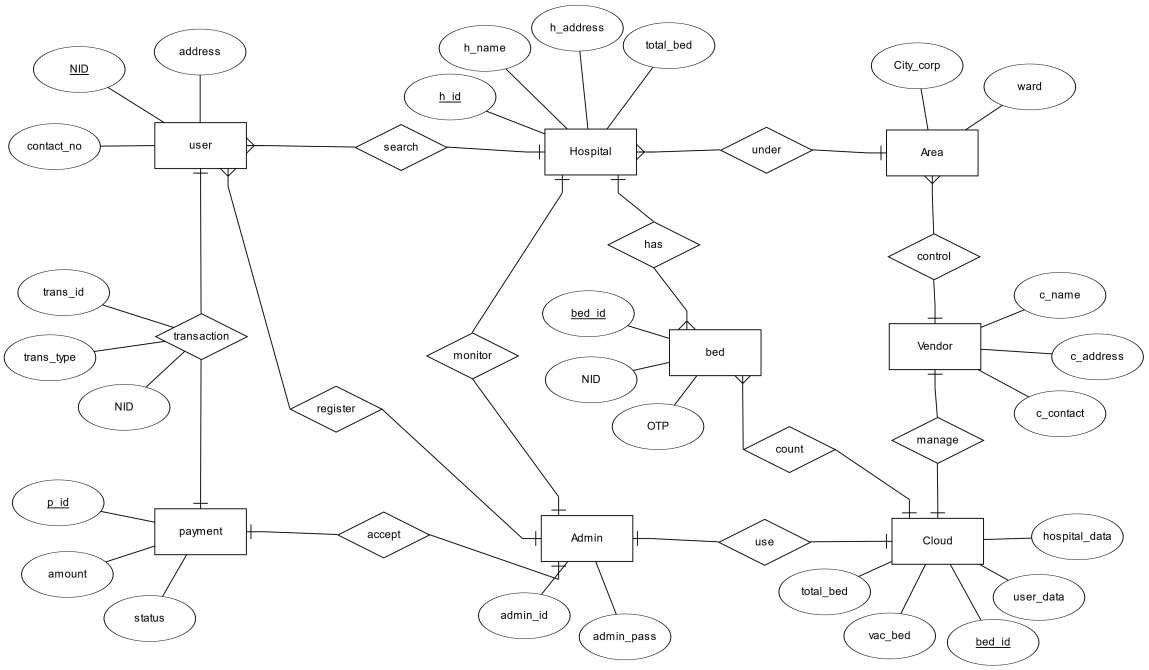

Fig. 4.2. Entity Relationship Diagram

4.4.1.2 Use case diagram:

Diagrams of use-cases show the system's high-level functionality and scope. These graphics also show how the system interacts with its participants. It's important to note that use-case diagrams do not depict the underlying workings of a system, but rather how the system is used by its users. It is important to understand how a user interacts with an engineering system via the usage of a use case diagram Finally, it should make it easier to categorize and specify needs.

For building the system, 4 actors such as hospital's admin, user, vendor and hospital have been used for creating the use case diagram. Here, the login and registration process will be proceed by the user and confirmed by the admin of the hospitals through cloud. A pin number will be sent from cloud to the user for registration. For providing total security of data the system will use Hybrid cryptography algorithm.

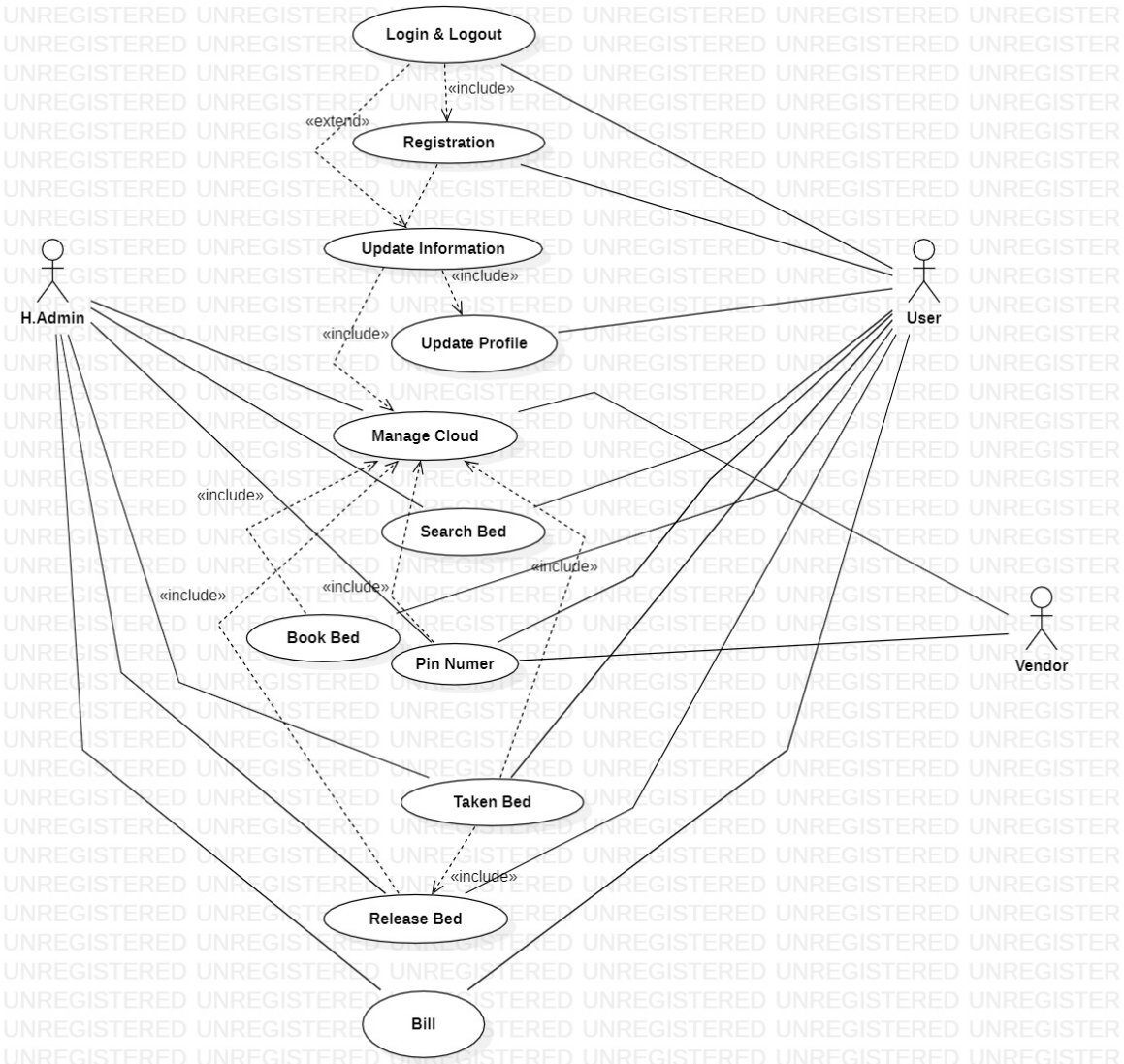

Fig. 4.3. Use case Diagram

4.4.1.3 Class diagram:

A class diagram is a visual representation of the connections and source code dependencies that exist between classes in the UML. This context refers to a class that describes the methods and variables of an object, which is a particular entity in a program or a unit of code representing a specific entity in that program. Class diagrams are the system or subsystem's blueprints. It may be used to represent the system's objects, to visualize their interactions, and to define what those objects perform and

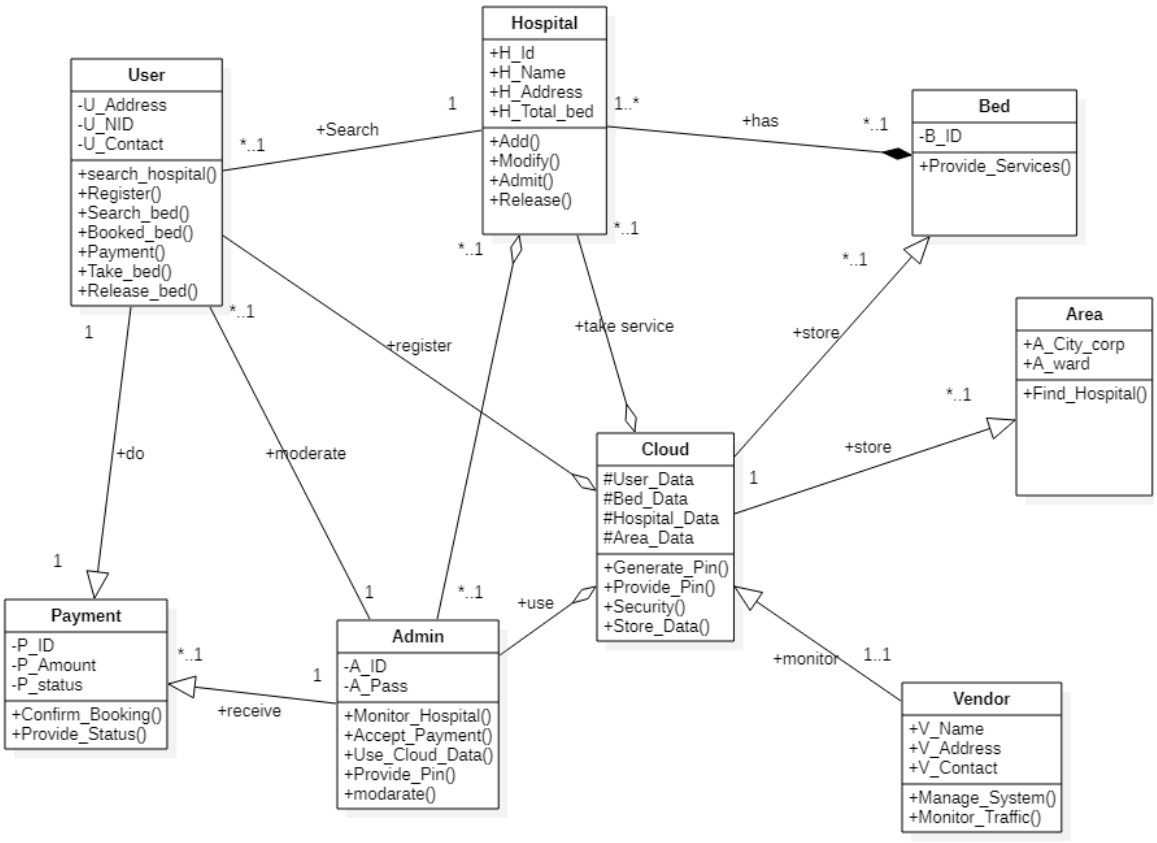

Fig. 4.4. Class Diagram

the services they offer.

4.4.1.4 Sequence diagram:

A Sequence Diagram is a kind of interaction diagram that explains how an operation is carried out. In the context of a cooperation, they record the interactions between the various items. Using the vertical axis of the diagram to represent time, Sequence Diagrams demonstrate the sequence of interaction graphically by depicting what messages are received and when. Sequence Diagram for User, Admin and Vendor are proposed below:

(a) **Admin sequence diagram:**

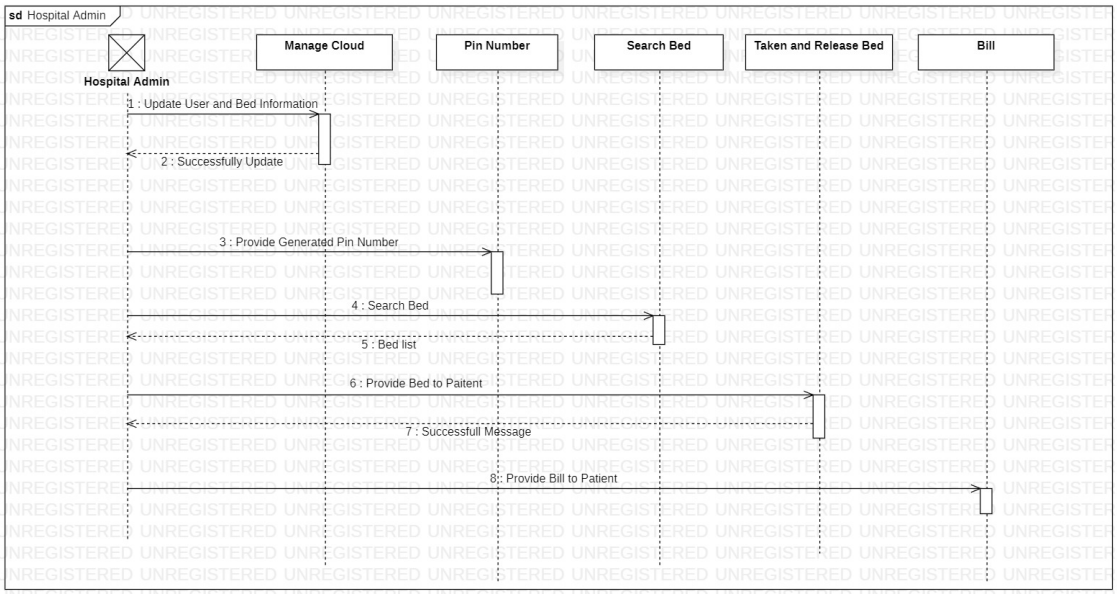

Fig. 4.5. Admin sequence diagram

The activities of hospitals admin are shown in this diagram. All the information about hospitals, hospitals facilities and beds will be provided by the admins.

This information will be stored in cloud, and through cloud, it will be accessible by users. After booking or releasing a bed, the admin will monitor the bed's availability.

(b) **User sequence diagram:** The activities of users are shown in this segment. How the users will search, register and login to the system and book vacant bed by searching process and also payment method is shown in this diagram. Some defined time will be given to the user for his booked bed. After finishing his booking, one confirmation message will be sent to his contact number. After completing all the procedure with payment, the patient will be taken to the hospital bed. Then by punching National Identity Card (NID) into the Radio Frequency Identification (RFID), which will be attached with the bed,

the information will be sent to the cloud that the bed is currently booked.

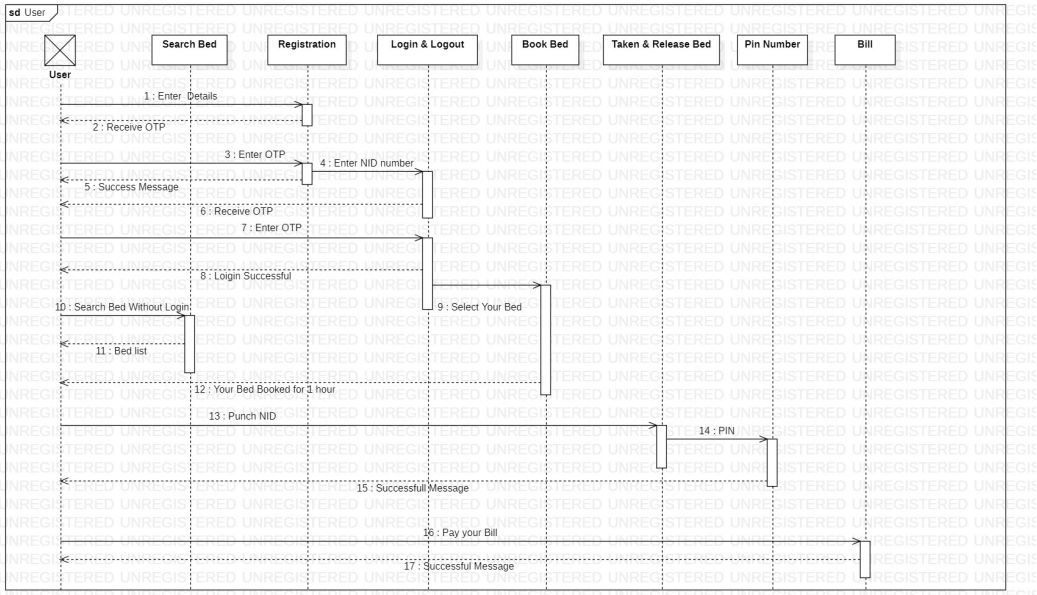

Fig. 4.6. User sequence diagram

(c) **Vendor sequence diagram:**

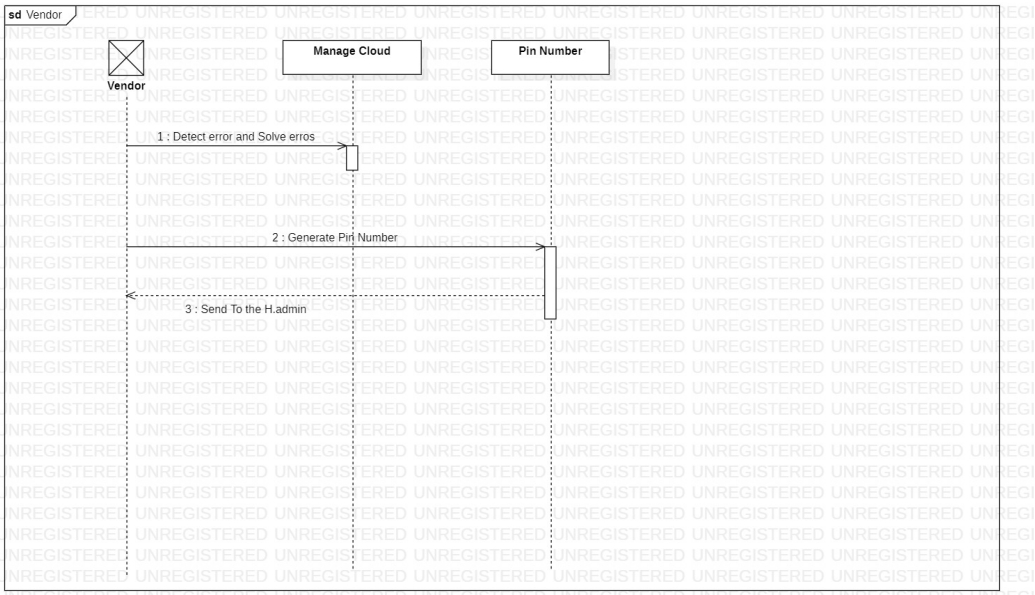

Fig. 4.7. Vendor sequence diagram

The activities of vendor are shown in this diagram. The major role of vendor will be to detect if there occurs any error. Many types of errors can occur. To

monitor the system, vendor will always keep track of the system.

4.4.2 Workflow

The workflow of the proposed system model is described bellow:

i. Through the location tracking system of the user's device, the proposed system will track the user and the system will search for the nearest available hospital.

ii. An user doesn't need to register or login to see the available hospital. When someone needs to book a bed, he needs to register or login to the system.

iii. After logging in, user needs to make payment within a defined time to ensure the confirmation of booking.

iv. While the patient is taken to the hospital, by this time, a PIN will be provided to the user's contact number. The user will punch his NID through RFID and give the PIN. RFID will collect data from the NID.

v. At this time, the data will be sent to cloud. And before going to the cloud, the data will must be encrypted.

vi. While the data is sent to cloud, the system will know that this bed is now occupied. Which will be updated at the moment. The other users will see that this bed is now unavailable.

vii. As these are user's or patient's personal information, the system will use hybrid cryptography to ensure the security of data in cloud.

viii. Again, while the patient will be released, the user will punch his NID again with another PIN provided by the admin.

ix. RFID will collect data again and it will inform the system that the bed is now available.

x. Thus the system will make this bed available to other users.

4.4.3 Sharing Data to Network

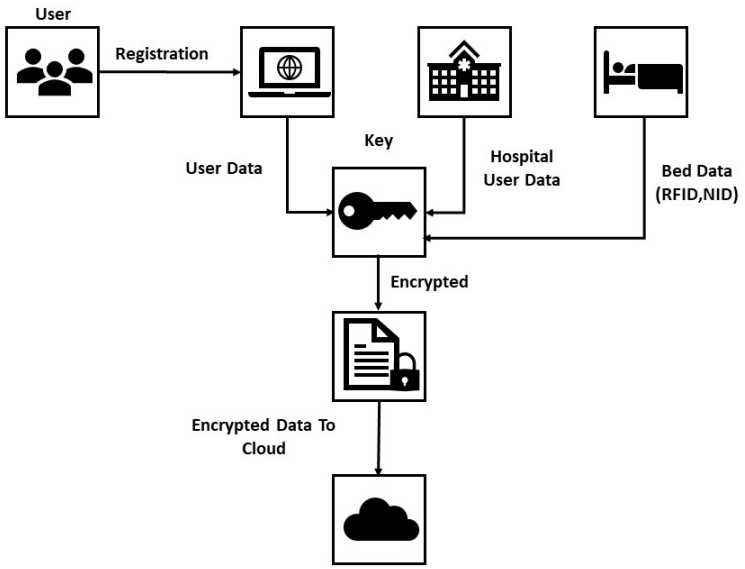

Fig. 4.8. Sharing data to network

The term "data sharing" or "shared data" currently has no commonly agreed meaning. It is not unusual for a new technology or practice to take some time before one of the numerous viable names and meanings emerges. Support Centre for Data Sharing (SCDS) refers to "data sharing" as the collection of activities, technology, cultural factors, and legal frameworks important to transactions in any sort of digital data between organizations of all sizes.

From the user, the data will be stored in the cloud. All data will be encrypted by a hybrid algorithm which is constructed by AES and ECC.

4.4.4 Accessing Data from Network

Data that are stored encrypted in cloud can be only accessed by the authorized users. As these are user's or patient's personal information, these should not be accessed by any unauthorized person.

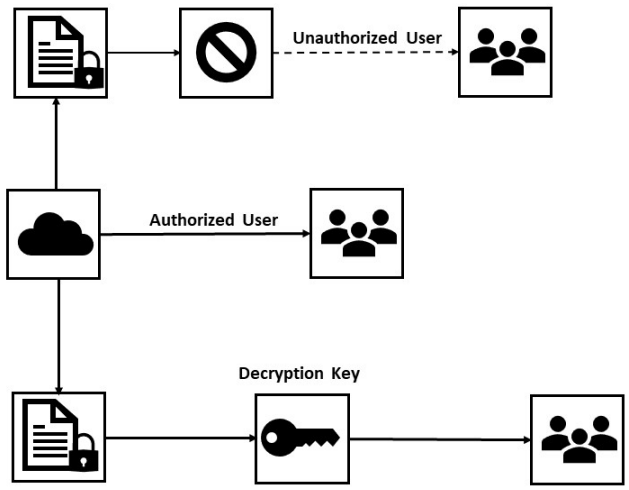

Fig. 4.9. Accessing data.

4.4.5 Security Layer

As user's personal information will be stored in cloud, the data must be secured. So that no one can invade the system. For doing that, the data should be in such a way so that unauthorized person cannot enter the system. Now how to do that? The data will be encrypted. Using an algorithm to scramble, or encrypt, data, and then using a key to decode the information, encryption protects sensitive information from being intercepted and misused. The plaintext of an encrypted communication is the message that is contained inside the encrypted message. It is referred to as ciphertext when it is in its encrypted and unreadable form.

To encrypt data in the system, a hybrid algorithm which is mixed with AES and ECC has been proposed. AES is chosen over other symmetric algorithms such as RSA, DSA, because AES is faster. AES takes less time to encode and decode. On the other hand, ECC is chosen because of the tiny key sizes, ECC is particularly well suited for use on devices with limited storage or processing capacity, which are becoming more widespread in the digital world. For more typical web server use cases, lower key sizes may provide faster SSL handshakes while still providing higher security.

4.4.6 Cloud

The cloud computing system is being used by a wide range of companies to store data on the cloud, allowing them to access it at any time. A cloud computing architecture may be divided into two categories: on-premises and cloud-based. It's a front-end and a back-end issue. The internet connects the two ends of the wire.Back end is in charge of ensuring the safety of cloud users' data. The back end is used by the service providers. It manages all of the resources necessary to provide services. Data storage, virtual machines, servers, traffic management methods, and so on are all part of the system.

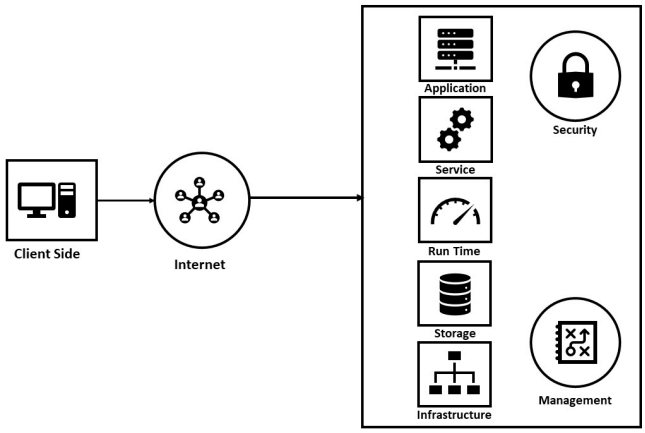

Fig. 4.10. Cloud architecture

4.5 Data Preparation

The research work focuses on encrypting any type of data. For encryption purposes, the following data set is used.The data set is based on user details. Here .jpg is the user image and .txt is the user information.

Table 4.1: Data preparation table

No	Name	File Type	File Size
1	Sample1	.jpg	38 KB
2	Sample1	.txt	1 KB
3	Sample2	.jpg	34 KB
4	Sample2	.txt	1 KB
5	Sample3	.jpg	48 KB
6	Sample3	.txt	1 KB
7	Sample4	.jpg	49 KB
8	Sample4	.txt	1 KB

4.6 Experimental Model

The operating method of the encryption is depicted in this diagram. Fig 4.11 depicts the encryption of picture data throughout the creation of the image.The encryption algorithm is based on the Python programming language, which is used to create it.

Data size appears to have been decreased following the encryption process, which is excellent for storage management.

Fig. 4.11. Data encryption process

In Fig 4.12, the first image is a sample image data. The data is encrypted through the hybrid algorithm which is the combination of AES and ECC algorithm. After encryption, the data will be as the second image.

Fig. 4.12. Encrypted data

It is shown in Fig. 4.13 how the decryption process for the encrypted sample data is carried out. Despite the fact that the encrypted data was lower in size, following decryption, the data is returned to its original size and format. Which ensures that there is no data loss.

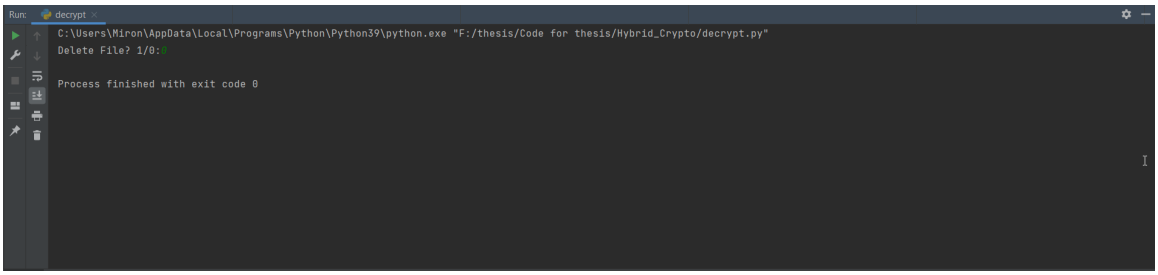

Fig. 4.13. Data decryption process

And finally in 4.14, we have found the decrypted data as the original data which was encrypted.

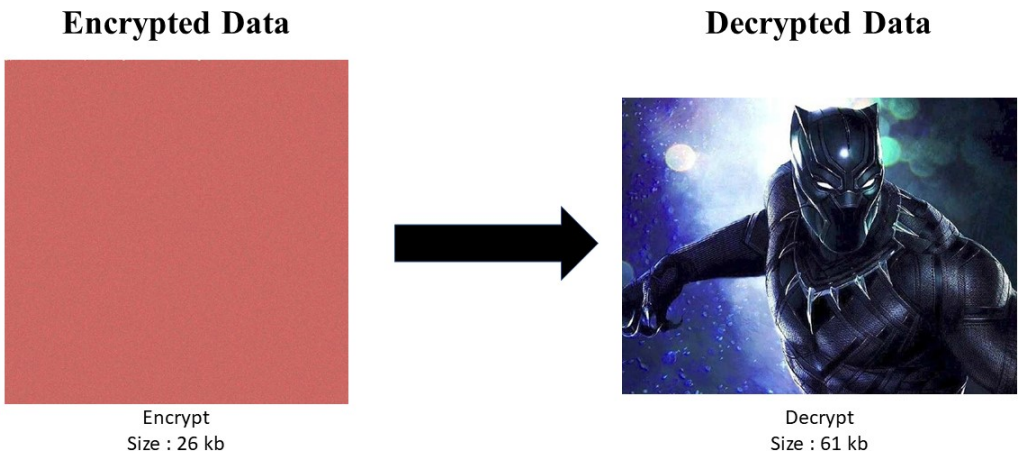

Fig. 4.14. Decrypted data

4.7 Creation of Keys and QR Code

The procedure's keys will be generated at random. The system creates a picture-based QR code representation of the keys, which is subsequently used to extract the key in text format. This provides an additional level of security for the AES keys. The second level of security is achieved by encrypting the AES keys using an ECC public key generated from the base64 encoded text file used as input.

The decryption technique is identical to the encryption procedure, except that the approach is slightly more sophisticated. A hybrid system, as defined in this paper, consists of two forms of encryption: symmetric encryption using AES (128,192,256 bits) and asymmetric encryption using ECC.

4.8 Encryption Module

This section contains information about the encryption module that has been suggested for the system. The module will accept plain text, images, or any other type of data in any format. After that, the AES key QR Code will be created automatically. The public key for AES will be obtained. Then the public key pair K_{Public}, $K_{Private}$ will be sent as input to the program. The public key of the AES algorithm will be encrypted. This data file would be encoded in Base64 format, and the resulting encoded text would be stored as plaintext P1. The plaintext will be encrypted using the previously encrypted AES key, which will be used to decrypt the plaintext. Then the AES plaintext will be encrypted with the AES public key, and the process will repeat. Finally, the Ciphertext will be returned as C1.json, which stands for Ciphertext JSON. Consequently, the encryption process will be completed.

Algorithm 1 Encryption using Hybrid Algorithm

Input: Plain Data.
Output: Ciphertext.

step 01. Input a plain data format as txt, docs, jpg etc. D1
step 02. Input AES key QR Code which is generated
step 03. Extract the AES Public Key
step 04. Input the ECC key pair K_{Public}, $K_{Private}$
step 05. Encrypt the AES public key Using K_{Public}
step 06. Encode this data file into Base64
step 07. Encoded text as plaintext P1
step 08. Encrypt the plaintext using Encrypted AES key
step 09. Encrypt the AES encrypted plaintext with K_{Public}
step 10. Return the Ciphertext as C1.json

Following fig shows how the encryption process is done [17]:

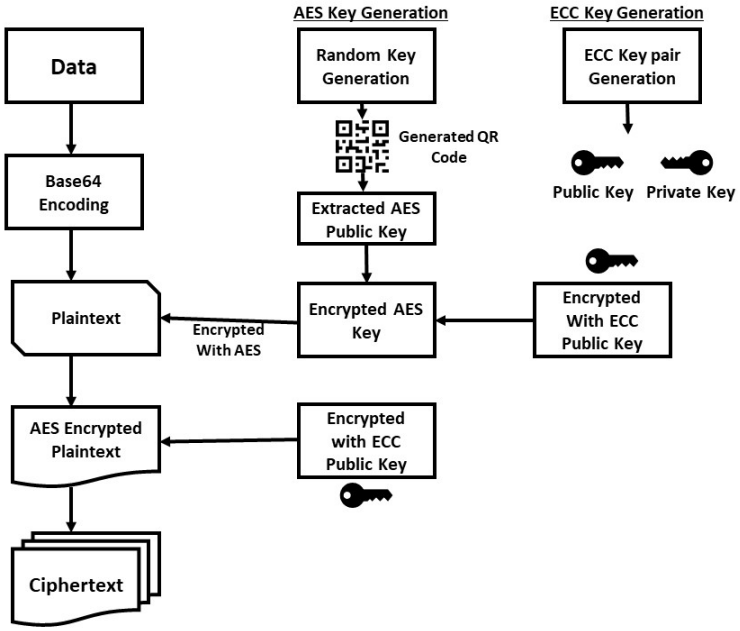

Fig. 4.15. Encryption procedure

4.9 Decryption Module

This section includes the decryption module proposed in the system. While needed decryption, the cipherext file C1.json will be enter the module as input. C1.json will be decrypted with the private key $K_{Private}$.

After that, AES key will be encrypted with $K_{Private}$. AES encrypted plaintext will be then decrypted. The AES encrypted plaintext will be decoded with Base64. And finally the plaintext will be returned as D1. Following fig shows the decryption process [17]:

Algorithm 2 Decryption using Hybrid Algorithm

Input: Ciphertext.
Output: Plain Data.

step 01. Input Ciphertext as C1.json
step 02. Decrypt C1.json with $K_{Private}$
step 03. Encrypt AES key with $K_{Private}$
step 04. Decrypt the AES encrypted plaintext
step 05. Decode the AES encrypted plaintext with Base64
step 06. Return the plaintext, D1.

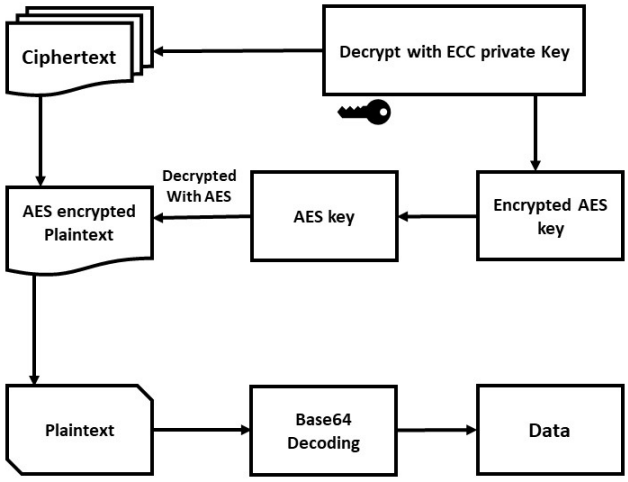

Fig. 4.16. Decryption procedure

CHAPTER 5

RESULT AND DISCUSSION

5.1 Overview

This chapter focuses on the output of the proposed model. The chapter shows the performance of the encryption algorithm. How better the encryption algorithm secures the system, is shown in this chapter.

5.2 Security Analysis of the proposed model

The security of the proposed model is discussed in the following section considering each aspect independently.

5.2.1 Integrity

In reality, the user has no control over the data that has been outsourced. In order to conserve storage space, the cloud may delete data that is seldom or often accessed, compromising the security of user data stored there. Most consumers can't tell if their cloud data is still complete since they have little auditing capabilities. If the problem persists, the user can enlist the help of a third party to conduct an audit of his or her data, which will examine the data for completeness, validity, and consistency and identify any errors. Data security can be jeopardized if a member of

a group is careless while using cloud storage with sharing services, making integrity audits critical for groups. Moreover, members of the same group can exchange data with each other and access and alter the data they have shared with each other.

5.2.2 Confidentiality

In our system model, as the users and patients have to give personal information of them, so it must be secured and cant not be accessed or modify by unlawful, unauthorised and any 3rd party. So, here we have to consider confidentiality in the protection for these data or information. Protecting data from unauthorized access, disclosure, or theft is at the heart of maintaining data confidentiality. It's all about protecting the privacy of information, including permissions to access and use it. Confidentiality If disclosed to a wider audience than the one intended, information with minor confidentiality issues may be termed "public" or otherwise not dangerous. Confidential data must be kept that way in order to avoid identity theft, system compromises, legal ramifications, reputational harm, and other grave consequences.

5.2.3 Availability

Our proposed system is a kind of peer to peer distributed with a centralized server which is cloud. so in case of unavailability, we have to suffer from data loss and also will not get the proper security of personal information of users. The term "availability" refers to the fact that the data is accessible to the user at any time. Risks arise when third-party service providers retain data in faraway places that are not under their control. Data is lost if the cloud fails to deliver service.

5.2.4 Scalability

We must ensure that our systems are able to work properly even if they are expanded or reduced in size or volume. The system of protection and keeping data safe we need to know the system. Scalability is the capacity of a system to grow or decrease in performance and cost in response to changes in application and system processing demands. Patients private information must be better protected in our system. Because of this, our suggested approach has to be more scalable. In order to get the results we desire, we need a system that can meet the model's fundamental setup requirements.

5.2.5 Cost

The system does not require heavy expense. The hybrid algorithm is based on AES and ECC algorithm, which needs lower cost than other algorithms. And for the other components, there will be expense for server and cloud space which will be not so expensive.

5.3 Performance Analysis

Table 5.1: Performance Analysis Table

Original File	**Size of File**	**Loss in Data**	**Retain Data**	**Encrypt Time**	**Decrypt Time**
Sample1.jpg	38193	0	100	2.54	6.574
Sample1.txt	176	0	100	0.308	0.125
Sample2.jpg	34608	0	100	2.191	5.411
Sample2.txt	77	0	100	0.298	0.119
Sample3.jpg	48869	0	100	3.705	10.177
Sample3.txt	85	0	100	0.293	0.119
Sample4.jpg	49415	0	100	3.798	10.415
Sample4.txt	84	0	100	0.284	0.114

5.4 Discussion

Now a days, it becomes a major problem of finding a nearest hospital for the patients who is in critical situation. To reduce this hassle of finding hospital we proposed a system model which will show all the nearest hospital and users can see easily which hospital have vacancy of beds in one platform or website. The users do not need to visit all the hospital's website individually. In our study, we demonstrated a system that helps patients and other patients locate the closest hospital in the event of an emergency. The system model collects user data and guarantees the most secure model since the data is most important. So for this criteria, we used a hybrid algorithm which is the combination of AES and ECC that is much efficient for data security and also ensures a model that is more secured than other present models. Our used hybrid algorithm will provide the data security and in future the model will establish the best way for the emergency patients who needs the better treatment and this can be happened in one platform of internet. At the beginning of our research, we saw that hospitals have their own digital platform individually but no common platform. Thus we established a way that can manage the E-Bed system which can ensure the easiest way for reducing the patient's hassle. We also tried to show a track for a researcher who want to develop hospitals e-bed system. And we also established the system model for a better implementation and hope that this work will be very helpful for the future researchers also.

CHAPTER 6

CONCLUSIONS

6.1 Overview of the chapter

This chapter will finally conclude the whole thesis work and suggest some possible paths it can progress towards in the future.

6.2 Conclusion

Finding available hospital beds at a crucial moment is a very tough task nowadays. It is very hard to find vacant seats in hospitals, especially when some pandemic comes. For that reason, a model has been proposed that can solve this problem. A person can easily trace the nearest hospital that has an available bed for him. Everything in the world is moving to a digital world. So this problem can be solved digitally too. While working digitally, there's a high chance of data leaks or unauthorized deeds. To prevent that, the proposed model has a high security layer that will keep the model safe and will protect user data. A hybrid cryptography algorithm has been used to keep the system secure. The hybrid algorithm, made with the combination of AES and ECC, ensures the security of the user data. Finally, the model will help a lot of people in critical moments.

6.3 Major Findings and Future Scopes

In this paper, we propose a secure model to reduce the complexity of finding and booking hospital beds. The model shows how it can work efficiently in an emergency situation. As it includes the user's personal information, we have proposed a hybrid encryption algorithm to secure the data. Our purpose was to ensure the security of the model. We have compared different algorithms to find the best-fitting one. Furthermore, we compared the architectures using a variety of criteria to ensure the accuracy of our findings.

Despite the impressive results, the suggested paradigm has not yet been widely applied, and additional testing may be required. A better application of our methodology is still possible because the study is scalable and improving. In the future, the design may be adapted to function more efficiently with a wider range of eHealth technologies.

REFERENCES

[1] G. Pradhan, B. Prabhakaran, and C. Li, "Hand-gesture computing for the hearing and speech impaired," *IEEE Annals of the History of Computing*, vol. 15, no. 02, pp. 20–27, 2008.

[2] P. P. et al, "A comprehensive evaluation of cryptographic algorithms: Des, 3des, aes, rsa and blowfish," pp. 617–624, 2016.

[3] P. P. et al., "Comparative analysis of des, aes, rsa encryption algorithms," *Global Journal of Computer Science and Technology 13*, no. 1, 2014.

[4] P. Mahajan and A. Sachdeva, "A study of encryption algorithms aes, des and rsa for security," *Global Journal of Computer Science and Technology 13*, no. 15, 2013.

[5] Y. Wang and M. Hu, "Timing evaluation of the known cryptographic algorithms," *Computational Intelligence and Security, 2009 International Conference on IEEE*, vol. 2.

[6] V. R. Pancholi and B. P. Patel, "Enhancement of cloud computing security with secure data storage using aes," *International Journal for Innovative Research in Science and Technology 2*, no. 9, pp. 18–21, 2016.

[7] P. Kumar and S. B. Rana., "Development of modified aes algorithm for data

security," *Optik-International Journal for Light and Electron Optics 127*, no. 4, pp. 2341–2345, 2016.

[8] C. P. A. K. Mandal and A. Tiwari, "Performance evaluation of cryptographic algorithms: Des and aes," *Electrical, Electronics and Computer Science (SCEECS), 2012 IEEE Students' Conference on. IEEE*, pp. 1–5.

[9] A. A. Hasib and A. A. M. M. Haque, "A comparative study of the performance and security issues of aes and rsa cryptography," *Convergence and Hybrid Information Technology, 2008. ICCIT'08. Third International Conference on. IEEE*, vol. 2, no. 4, pp. 505–510.

[10] K. et al, "Bluetooth communication using hybrid encryption algorithm based on aes and rsa.," *International Journal of Computer Applications 71*, no. 22, 2013.

[11] e. a. M. B. Vishnu, "Security enhancement of digital motion image transmission using hybrid aes-des algorithm," *2008 14th Asia-Pacific Conference on Communications. IEEE*, pp. 1–5.

[12] W. Tianfu and K. R. Babu, "Design of a hybrid cryptographic algorithm," *International Journal of Computer Science Communication Networks 2*, no. 2, 2012.

[13] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of computation*, no. 48, pp. 203–209, 1987.

[14] S. U. Nimbhorkar and D. L. G. Malik., "A survey on elliptic curve cryptography (ecc)," *International Journal of Advanced Studies in Computers,Science and Engineering vol.1*, pp. 1–5, 2012.

[15] M. Ansari, B.; Hasan, "High-performance architecture of elliptic curve scalar

multiplication," *Computers, IEEE Transactions*, vol. 57, no. 11, pp. 1443–1453, 2008.

[16] Z. H. W. Z. . W. Y. Wang, B., "Speeding up scalar multiplication using a new signed binary representation for integers," *LNCS.4577*, vol. 155, pp. 277–285, 2007.

[17] S. G. Sridhar C. Iyer, R.R. Sedamkar, "Multimedia encryption using hybrid cryptographic approach," *International Journal of Computer Applications (0975 8887)*, pp. 1–5, 2016.

[18] L. H. J. Hankerson, D. and A. Menezes, "Software implementation of elliptic curve cryptography over binary fields.," *Cryptographic Hardware and Embedded Systems, CHES'00. LNCS, 1965*, pp. 1–24, 2000.

[19] N. Torri and K. Yokoyama, "Elliptic curve cryptosystem," *FUJITSU Sci. Tech. J., 36(2)*, pp. 140–146, 2000.

[20] M. C. T. Dhirendra KR Shukla, Vijay K.R. Dwivedi, "Encryption algorithm in cloud computing," *Materials Today: Proceedings*, vol. 37, pp. 1869–1875, 2021.

[21] S. Mendonca, "Data security in cloud using aes," *Int. J. Eng. Res. Technol*, vol. 7, 2018.

[22] V. S. Mahalle and A. K. Shahade, "Enhancing the data security in cloud by implementing hybrid (Rsa Aes) encryption algorithm," *2014 Int. Conf. Power, Autom. Commun. INPAC 2014*, no. 1, pp. 145–149, 2014.

[23] L. Kumar and N. Badal, "A review on hybrid encryption in cloud computing," *Proc. - 2019 4th Int. Conf. Internet Things Smart Innov. Usages, IoT-SIU 2019*, pp. 1–6, 2019.

[24] W. F. Zhang, Y. Chen and Q. Wu, "Hybrid encryption algorithms for medical data storage security in cloud database," *Int. J. Database Manag. Syst.*, vol. 11, no. 01, pp. 57–73, 2019.

[25] a. R. R.Kiruthika, S.Keerthana, "Enhancing cloud computing security using aes algorithm," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 5, pp. 630–635, march 2015.

[26] V. K. Soman and V. Natarajan, "An enhanced hybrid data security algorithm for cloud," *Int.Conf. Networks Adv. Comput. Technol. NetACT 2017*, pp. 416–419, july 2017.

[27] S. Rehman, N. Bajwa, M. Shah, A. Aseeri, and A. Anjum, "Hybrid aes-ecc model for the security of data over cloud storage," *Electronics*, vol. 10, p. 2673, 10 2021.

[28] D. E. D. A. Dickson Kodzo Mawuli Hodowu, Dennis Redeemer Korda, "An enhancement of data security in cloud computing with an implementation of a two-level cryptographic technique, using aes and ecc algorithm," *INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH TECHNOLOGY (IJERT)*, vol. 9, September 2020.

[29] S. N. Mendonca, "Data security in cloud using aes," *International Journal of Engineering Research Technology (IJERT)*, vol. 5, pp. 205–208, 2018.

[30] A. Kumari, M. Y. Abbasi, V. Kumar, and A. A. Khan, "A secure user authentication protocol using elliptic curve cryptography," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 22, no. 4, pp. 521–530, 2019.

[31] N. Jia, S. Liu, Q. Ding, S. Wu, and X. Pan, "A new method of encryption algorithm based on chaos and ecc," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 7, pp. 637–644, 01 2016.

[32] R. Boaden, N. Proudlove, and M. Wilson, "An exploratory study of bed management," *Journal of management in medicine*, vol. 13, pp. 234–50, 02 1999.

[33] S. Abedian, H. Kazemi, H. Riazi, and E. Bitaraf, "Cross hospital bed management system.," *Studies in health technology and informatics*, vol. 205, pp. 126–130, 08 2014.

[34] L. Ren, X. Zhang, J. Wang, S. Tang, and N. Gong, "Design of hospital beds center management information system based on his," in *2017 IEEE International Conference on Bioinformatics and Biomedicine (BIBM)*, pp. 1093–1096, 2017.

[35] F. YoungA and A. Nicholls, "Innovative hospital bed management using spatial technology," 01 2007.

[36] R. Want, A. Hopper, V. Falcao, and J. Gibbons, "The active badge location system," *ACM Trans. Inf. Syst.*, vol. 10, pp. 91–102, 01 1992.

[37] R. Hosaka, "Feasibility study of convenient automatic identification system of medical articles using lf-band rfid in hospital.," *Systems and Computers in Japan*, vol. 35, pp. 74–82, 09 2004.

[38] C.-J. Li, L. Liu, S.-Z. Chen, C. Wu, C.-H. Huang, and X.-M. Chen, "Mobile healthcare service system using rfid," vol. 2, pp. 1014 – 1019 Vol.2, 02 2004.

[39] B. Janz, M. Pitts, and R. Otondo, "Back to the future with rfid: Lessons learned—some old, some new," *Communications of the Association for Information Systems*, vol. 15, pp. 162–148, 01 2005.

[40] J. Fisher and T. Monahan, "Tracking the social dimensions of rfid systems in hospitals," *International journal of medical informatics*, vol. 77, pp. 176–83, 04 2008.

[41] J. Baliga, R. W. A. Ayre, K. Hinton, and R. S. Tucker, "Green cloud computing: Balancing energy in processing, storage, and transport," *Proceedings of the IEEE*, vol. 99, no. 1, pp. 149–167, 2011.

[42] A. S. T. K. Mohammed, M. Elmogy, "Review of educational business intelligence using radio frequency identification technology," *International Journal of Intelligent Computing and Information Science*, pp. 33–49, 2017.

[43] W. K. M. Abdullahi Ibrahim, A.; Cheruiyot, "Data security in cloud computing with elliptic curve cryptography," *International Journal of Computer (IJC)*, pp. 1–14, 2017.

[44] P. Siani., "Privacy, security and trust in cloud computing," *Privacy and Security for Cloud Computing*, pp. 3–42, 2013.

[45] M. A. S. A. . A. Saba Rehman, Nida Talat Bajwa and A. Anjum, "Hybrid aes-ecc model for the security of data over cloud storage," pp. 1–20, 2021.

[46] V. C. Samiksha Sharma, "Analysis of aes encryption with ecc," pp. 195–196, 2016.

[47] S. D. K. R THANUJA, "A novel cryptographic architecture," *Journal of Theoretical and Applied Information Technology*, vol. 38, no. 1, pp. 74–75, 2012.