National College of Ireland

Research Project Questions

MSc Research Project
Research And Computing

Neethu Devassy
Student ID: x21106312

School of Computing
National College of Ireland

Supervisor: Aqeel Kazmi

National College of Ireland
Project Submission Sheet
School of Computing

Student Name:	Neethu Devassy
Student ID:	x21106312
Programme:	Research And Computing
Year:	2022
Module:	MSc Research Project
Supervisor:	Aqeel Kazmi
Submission Due Date:	01/02/2023
Project Title:	Research Project Questions
Word Count:	5526
Page Count:	21

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:	
Date:	1st February 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):	

Research Project Questions

Neethu Devassy
x21106312

Abstract

The management of each patient's personal health records is a prominent usage of cloud-based health information security (HIS). Real-time healthcare data sharing is now possible because to cloud computing. Health data are typically outsourced and kept on third-party cloud platforms, which frees up owners from having to manage patient data while improving data accessibility. Outsourcing personal health information, however, raises substantial privacy issues due to a higher chance of divulging private health data to unwanted parties. The main obstacles of the widespread utilization of healthcare information security systems are data security and privacy of preserving personal health records. Due to the confidentiality of patient data, it must be kept in a properly secured way.In current research, an unique hybrid cryptosystem based on the Pretty Good Privacy Approach (PGP) is proposed for keeping health records based on system challenges and various security measures. By encrypting the health data before saving it on cloud servers, the developed approach enables users to save and access the information safely on cloud storage. which allow granular user access, support multimedia data files, guarantee data secrecy, greatly simplify key administration. It can meet the necessary security criteria while performing computation and storage at a minimal cost.

1 Introduction

1.1 Background

We are all interested in how medical systems are developed and run since we will all inevitably use them. The primary concern is without a doubt the anonymity of patients and their hospital information, which reveal exceedingly private information such as a people's health history and current stage of medication. User privacy is the privilege of a user to maintain data secret if they give other party authorization to see it. As a result, user confidentiality includes user privacy. This study focuses on enhancing cloud environment's information security for healthcare (HIS). Clients of HIS include medical staff, patients, nursing staff, lab workers, and others. The privacy of their users is jeopardized by cloud computing, notwithstanding its convenience. The ability of an entity to limit the information about itself that is disclosed to the cloud is how we define privacy in cloud computing. Cloud services are delivered via the Internet by public clouds. A private network is used to deliver cloud services through private clouds, which are built by organizations for their own usage. This makes it easier to control security, data access, and service quality. Both public and private clouds can be found in hybrid clouds.

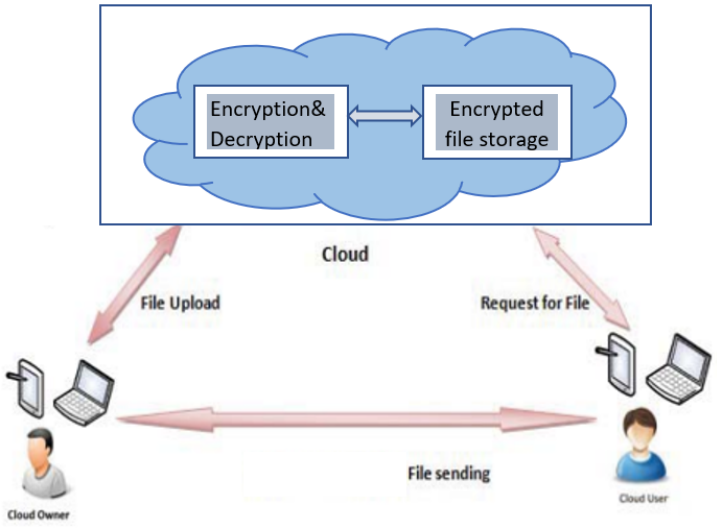

Figure 1: Information Transfer in Cloud

1.2 Motivation

Ensuring the security of data in HIS cloud computing (particularly in public clouds) is one of the major difficulties because:

- users cannot be certain that the cloud does not share their confidential information with unwanted access.
- Because they are unaware of the actual locations of their data on the cloud and the owners or managers of those locations, cloud users are unaware of who or what physically controls these data.

The fact that health information (HI) is stored on an untrustworthy third-party cloud service could severely impact the user's security. Customers' data may be used by a cloud service provider for unfair commercial gain. Even if it were technically possible, we think that users of HIS won't trust a public cloud to give them higher degrees of secrecy (or even privacy) and integrity because the lack of trust can only be partially resolved by improved technologyFarzana and Islam (2019). We require a method that allows an HIS user to rely on the cloud despite completely believing in its security measures. We anticipate that a user will be more inclined to put their trust in a privacy protection that is primarily developed at their own place. To protect the privacy of customers when working with an unreliable vendors, clinics must encrypt patient data prior to transmitting it to the remote server, that makes significantly more challenging data representation. The novel contribution of this research will achieving health information security in cloud using "PGP-based" technique called the hybrid cryptographic approach.

1.3 Justification

Users who lack the necessary authorisation may nevertheless be able to access health information in this situation. It is crucial to present a workable and compelling plan in order to increase HI security. Moreover, the vendor has complete control over on who has

act to the HI. Hence, only permitted users will have access to the HI. The combination of symmetric encryption and asymmetric encryption, is termed as hybrid cryptography techniquePariselvam and Swarnamukhi (2019). We can combine the speed and strength of the two methods if we can employ a variety of alternative techniques to strengthen the encryption. This technique is employed to guarantee secure cloud storage systems. The approach uses the AES and RSA algorithms, with AES being used for information or text encryption and RSA being used for key encryptionDomadiya and Rao (2022). This strategy uses these two methods to double-encrypt data and keys, enhancing security. For huge datasets, processing speed improvements for both encryption and decryption .Data from users, including text documents, graphics, voice recordings, and streaming video, among others, will be highly protected by the system.

1.4 Research Question

The following are the research question and goal that were used in this study:

Q1. Design a hybrid method combining the two top cryptographic techniques to increase the security of health care data in cloud platforms.?

Q2. Evaluate the PGP system's accuracy, compare its performance to that of the existing cryptographic techniques?

2 Related Work

An overview of the defenses employed to safeguard the confidentiality of health information in a public cloud is provided as an overview in this discussion.Cloud computing dangers and serious security and confidentiality risks have become important aspects.Finding answers to all of these problems is necessary since it's critical to transport data securely from the consumer end to the server.The improvement of healthcare data security from the consumer end to the server is the main goal of this research, which has employed a variety of approaches to address data protection concerns.

Farzana and Islam (2019)proposed a symmetric key-based design method to create an EHR management protocol. It is a patient-centric protocol since it delegates control of allowing data access to the patient. Achieving attribute-based access control, which uses a health professional's attributes (such as specialization, location, linked hospitals, etc.) to delegate access to a patient's EHR. The developed protocol is subsequently verified using AVISPA, a powerful evaluation utility for security measures. The protocol has been verified to be independent of identified hazards and to have the requisite security features by AVISPA. The only purpose of the AVISPA model we created is to validate protective attributes. Therefore, it's really worthless for researching efficiency or calculating the extra workload that security systems might impose. or estimating the additional burden that security mechanisms may cause. A quite long time passed before the solutions to a problem of symmetric data encryption like DES were started to be addressed. In fact, asymmetric cryptography encryption schemes employ a combination of two keys: a public key and a personal key. These keys are associated to each other logically.The encryption is performed using the recipient's unique code before being transmitted over the server. Although the data is sent to all users in the system, only the individual whose digital certificate matches the one utilized for encoding can decode it using their private keys.

Pariselvam and Swarnamukhi (2019).

Utilizing worldwide information from various E-health sources can improve the efficacy of association rule mining.All Healthcare systems are required to upload health files to a central computer. Several privacy restrictions may be broken if healthcare information is accessible on an illegal network. Due to this, the issue of distributed healthcare data mining while preserving privacy has emerged as widely known research topic within the medical sector Domadiya and Rao (2022). This study employs an efficient El Gamal homomorphic encryption strategy to protect privacy throughout a distributed association rule mining process. The benefits of the suggested strategy using data compiled from all EHR systems. The fact that security demands a secure integer value makes it extremely difficult to generate large enough keys is seen as a drawback. Lin and Jiang (2020) offered an enhanced CP-ABE solution with a specific search search feature for all users, enabling information customers to look for a certain secure messaging in the virtualized environment by utilizing a specific word. This was done in order to enable the search feature in the ciphertext. They also included the separate virtual machine idea inside the developed model design to facilitate interaction between customers and the cloud-based service , prevent significant attacks, and reduce the computational load on cloud storage. It enables a shorter ciphertext and a faster running time. However, maintaining consistent ciphertext and attribute revocation both have some major issues.

An innovative patient health information exchange protocol that safeguards patient privacy and makes it possible for HSPs to safely and swiftly access and search PHI files been proposed Xu et al. (2019). They used the searchable encryption technique together with multiple keyword and keyword scope searches. They use a modified bloom monitor and a cryptographic key to categorize health data files, incorrect data detector, and guarantee the the reliability of search queries. Experiments using actual and artificial information's are used to reveal the system's optimal utilization, while security analysis is used to show how well the state prevents privacy. It shows how well shared data is protected while upholding privacy. However, it can be difficult to manage several keys for numerous data owners. Data users must establish multiple trapdoors for data owners' data, even when employing the same request criteria. By encoding the information prior to uploading it to remote environment, Nadaf and Patil (2016) implemented a strategy that provides users with a platform for securely storing and retrieving health information on cloud services. The AES encryption scheme, which employs the unique key for both encode and decode data, was used to create the developed methodology. It solved the key management issue by mailing the secret key to the user's email address. But it uses a very simple algebraic model. Every block is always encrypted in the same manner, which is considered to be a disadvantage.

PHR's issues with data manipulation, data sharing, and information leakage were all addressed by Lu et al. (2021). They proposed a tried-and-true dynamic searchable symmetric encryption (DSSE) method using advanced discretion for electronic medical services, enabling many medical professionals can explore and obtain patient information securely and successfully. The accuracy of the searched healthcare data is checked using the homomorphic MAC (HomMAC) method. The proposed strategy offers a potentially efficient means of ensuring that virtualized medical care solutions can fulfill their stringent scalability and reliability criteria. The computational complexity and com-

munication complexity of the data owner and server are not reduced. For precise user management and file searching, it does not integrate access control. To manage enormous amounts of information, a versatile and precise access control system has been utilized Mythri and Jayram (2017). A useful tactic has evolved that is depends on functionality encryption, it offers adaptable and granular access management. It is possible to lessen the overhead of key generation by segmenting clients into distinct fields. High degrees of information safety are offered through the use of the Advanced Encryption Standard. The suggested system also examines scenarios in which shared, secure data is used by many users, owners, and authorities. The performance evaluation's findings indicate that the novel method falls short in reference to computational cost and temporal complexity.

Obiri et al. (2022) have conducted a study with the aim of enabling fine-grained network control and guaranteeing the validity of the database request and the anonymity of patient data files. In order to guarantee data privacy, query output correctness, information integrity, blind keyword search, an attribute-oriented cryptography system, and precise access control, they presented a novel personal medical records exchange mechanism. The search method that enables blind inquiry without disclosing the details of the unique key and request on the B+ tree. The scheduled key maintenance, however, was not adequately justified by them. Performance analysis of DES, AES, and Blowfish was completed in 2011 by Thakur and Kumar (2011). They used Java to carry out their investigation, and the results of their modelling showed that Blowfish outperformed alternative encryption techniques. Since there have been no successful security attacks on Blowfish, it is thought to be a better encryption method. However, the fact that AES requires more processing power than other algorithms does not help it perform as well.

Furthermore, John et al. (2015) concur with other experts that the ElGamal algorithm is quite effective in their investigation when they conduct a comparison between the Discrete Logarithm and the RSA technique. The outcome of the simulation demonstrates that the El-Gamal method performs slowly both during encryption and decryption. In order to prevent security flaws and breaches, Shabbir et al. (2021) presented the Modular Encryption Standard (MES) based on the collection of modules. Symmetric cryptography is used in MES. In this method, the user implements the first module, which uses entropy-based key creation. Health data are enlarged and decreased using the second module before being transferred to the cloud. The various cloud-service based storage is finished after the extra crypto-cloud components are finalized. The suggested remedy provides users with fine-grained network access and protects patient privacy via a requirement-based strategy. The image-based data type is not taken into account; this approach is made to encrypt and decrypt text material. Additionally, the layered architecture periodically causes system performance to drop.

Owolabi et al. (2017) analyse the performance of a few algorithms, including RSA, ECC, and AES, taking time and complexity into account. The experiment is carried out using a cryptography tool (Fidora utilizing NS2) and each algorithm is developed in C++. The outcome demonstrates that, in comparison to RSA and AES, ECC spent the most time encrypting data, making it safer due to its higher cipher complexity. The new issue of owners of Sensitive Health Information (SHI) retaining their privacy is addressed in another study by Sharma et al. (2019). The RSA key technique is used by the proposed system. In this method, the attribute authority (AA) will get the patient's and

the physician's passwords in order to create the unique key. These credentials will be encoded using a distributing mechanism. Then AA gives you the identical key. The data is subsequently encrypted using a domain-based authentication scheme before being sent to the cloud platform. The recommended approach guarantees anonymity and considerably lessens the workload associated with key handling. Due to the more sophisticated algorithm used, this solution takes longer and requires more processing power.

There is additional study on decentralized hierarchical attribute-based encryption by Liu et al. (2020). The suggested system uses a hierarchical tree structure to process multiple files in a single operation. It permits the production of anonymous keys, lowers computational complexity and storage costs. However, decentralization makes it harder for the various departments to collaborate. Oh et al. (2014) suggested a architecture for auditing broker-based encryption that restricts the records that can be found in audit logs and regulates how it can be made available for enquiries is shown along with some of the requirements. This system is based on formal audit procedures and uses Hierarchical Identity-Based Encryption (HIBE) to support the phased disclosure of data required for inspection and a control between manual and automatic checks. Using an amendment to the (ATNA) protocol, a specification for auditing HIEs, they put the techniques to the test. However, it doesn't go into detail on how HIEs use access control systems.

Zhang and Ding (2015) described a method for encrypting and decrypting digital photographs using MATLAB that is based on the Advanced Encryption Standard (AES) algorithm. In order to process the computerized pictures through the AES encryption method, they first transformed them into a binary matrix. The plain language of the algorithm was created by first dividing an array of pixel level of a computerized pictures into 4*4 matrixes for each unit of 8 bits. Second, the AES method will be used to encrypt each matrix. The encrypted matrix will be created by joining every new matrix. The findings demonstrated that this approach is vulnerable to plain document perhaps when employing a decoded key that is slightly different because it will produce an entirely incorrect image and cause decryption to fail completely. A reliable data duplication mechanism called DICE (Dual Integrity Convergent Encryption) was introduced by Agarwala et al. (2017) with the goals of preventing assaults using copy-faking and deletion and ii) providing an integrity verification at the source and destination ends. The remote machine verifies the the accepted tag's authenticity after the generated tag has been uploaded. Following user download of the code to retrieve the cipherdata, an integrity check is executed. As the output, send simply the tag rather than the lengthy ciphertext to achieve both deduplication and bandwidth reduction. The procedure of key generation and administration is not adequately explained in this work.

3 Methodology

This study focuses on creating a system that is accurate and effective in identifying security flaws in cloud storage of health information. The procedures taken to make sure high safety of health information storage in the cloud platform will be covered in this section. When used in a cloud setting, the pretty good privacy approach gives the remote server the highest level of protection. As a result, it aids cloud service providers in

Scheme	Advantage	Disadvantage	Reference
symmetric key-based design	Enhanced access control management.	Least efficient and complex computation	Farzana and Islam (2019)
asymmetric cryptography encryption	Reduces the workload of key management.	Using Complex algorithm	Pariselvam and Swarnamukhi (2019)
El Gamal homomorphic encryption	Provides security to data by better encryption technique	Poor key management	Domadiya and Rao (2022)
CP-ABE	shorter ciphertext and a faster running time	Issues with consistent ciphertext and attribute revocation	Lin and Jiang (2020)
searchable encryption technique	Provides strong security to data	Poor key management	Xu et al. (2019)
AES encryption	improved key management	followed similar encryption for every block	Nadaf and Patil (2016)
DSSE	Provide Efficiency and security	failed to reduce computational complexity and communication complexity	Lu et al. (2021)
feature-based encryption	reduced overhead of key generation	incresed complexity and computational cost	Mythri and Jayram (2017)
Attribute-oriented cryptography system	Fine grained access control and strong security	Lack of information on key maintenance	Obiri et al. (2022)
Performance analysis of DES, AES, and Blowfish	Blowfish outperformed other techniques	The processing power of AES lower than other algorithms	Thakur and Kumar (2011)
Comparison of ElGamal and RSA	Both algorithm provide strong security	The performance of ElGamal is lower than RSA	John et al. (2015)

Table 1: Summary of the literature review

winning over more customers. Thus, the major problem of data partitioning and accessing control has been solved. The process converts the actual information into a portion of an unintelligible form. The decoded data on the cloud server can only be accessed by authorized users, although all users can see the encrypted information. The suggested technique makes use of a mix of the RSA and Advanced Encryption Standard algorithms. Combining various algorithms also results in better and more precise outcomes. AES algorithm combined with RSA's key encapsulation minimizes the potential for attacks like side channel attacks and brute force assaults in the area of cloud storage by overcoming the flaws in both two algorithms.

3.1 Pretty Good Privacy Approach (PGP)

For applications such as electronic mail and data storage, PGP offers a security and authentication facility. PGP includes the symmetric key being encrypted so that it can later be used as a session key for emailing. Since the symmetric key must be supplied to the other party secretly, public key cryptography is used to encrypt it. Asymmetric encryption is appropriate in this situation because the session key can only be unlocked with the recipient's secret key, which the attacker does not know. This prevents any attacker from being able to decrypt the key in time complexity. The following algorithms were used to create the thesis:

3.2 Advanced Encryption Standard (AES)

Block iterative encryption is done using the AES algorithm. There are numerous 128-bit plaintext blocks that make up the plaintext. The length of the secret key allows it to be classified into three categories: AES-128, AES-192, and AES-256 each need 10, 12, and 14 cycles of computation. The keys for the three types have ranges of 128, 192, and 256 bits. In order to generate 11, 13, and 15 sets of sub-keys, the keys must be expanded. The round key is the key that corresponds to each round operation. It successfully integrates security, performance, efficiency, and adaptability and can fend off current hacking tools. The AES method encodes information by including a 128-bit plaintext frame to the State byte matrix. The algorithm uses State as the basis for all of its operations. The activities concerned consist of:

- Key Extension: Establishing a round-key and working with the state to both encrypt and decode.
- Insert Round Key: Using the XOR method, the State matrix and 128-bit original private keys produce the new State matrix.
- Initial Nine Sessions:

  a) Each byte in the Condition is swapped by the replacement table using Sub Bytes (S-Box). A byte can be modified by splitting it into two hexadecimal values and then searching for the S-Box. The matrixes of the substitution table are indicated by these two integers. The two hexadecimal digits at the point where the rows and columns meet are distinct entries in S-Box.

  b) Every row in the State is cycled through a unique offset when using the Shift Rows function. The initial line stays the same, the second line moves one byte to

the left hand side, the third line changes two bytes to the left side, and the fourth line travels data block to the left side.

c) The status of each column is processed individually by Mix Columns conversion. A function transformation of the first four bytes of the State column yields a new value for each byte, which is then assigned to the correct value.

d) The appropriate round key and State execute XOR component actions for every round.

- Final Round: The Mix Columns was eliminated in comparison to the initial nine rounds.

3.2.1 Improvement of AES Algorithm

The hospital information system's database holds a sizable quantity of medical records, with a wide range of record sizes. medications, doctor's orders, health records, and other data, for instance. The healthcare order information has a comparatively short data length, commonly no more than twenty bytes. The length of medical record information, such as the home page of an outpatient electronic healthcare record, the record of an outpatient medical evaluation, the landing pages of an inpatient electronic health record, the history of an admission, and so on, is in the hundreds of thousands of bytes. Data processing will take a long time if there are more data items than a given amount. The hospital staff will not tolerate a system system performance that is excessively long in the actual work setting. This research converts the serial structure to a parallel structure using the basic AES algorithm design. This research converts the serial pattern to a parallel way using the basic AES algorithm design. It aids in raising performance.

3.3 Rivest–Shamir–Adleman (RSA)

The cryptography algorithm RSA is asymmetric. Every other symmetric system operates on the same fundamental tenet. It employs a mechanism based on two keys: a public key and a private key. The private key of each person is kept secret, while their publicly access key is known to all and publicly accessible. Diffie and Hellman, who pioneered the method for the astonishing key transfer, provided the knowledge on the RSA public-key crypto algorithm. RSA uses a variable-size key and an encryption block that may be changed in size. One party uses a p key and the other employs a private key while performing an RSA computation. In the suggested work, the information will be secured by scrambling it using the RSA calculation such that only the concerned client can access it. WINDOWS AZURE

3.4 Windows Azure Cloud

- Projects that use Windows Azure can be created in practically any language and can incorporate cloud-based public services into an already-existing IT infrastructure.The key capabilities of Windows Azure enable customers to control who has access to their records and implementations:

- To make user entry to their cloud-based services easier, businesses can integrate data the researchers at their head offices with Domain Controller from Windows Azure.

- Privacy logs can be received at any moment to track information exchange and help with risk mitigation.
- Multiple types of validation are available, helping in stopping illegal login and offering a mechanism for verification in contrast to a passcode.
- Clients can set up permission protocols to limit users' resource access based on their performance in a specific position, their grade of authority, and the privileges they have been provided.

3.5 Performance Evaluation

Checking the accuracy metrics of the algorithms employed in hybrid cryptography allows for the calculation of the system's performance. Additionally, since multimedia files are compressed before being encrypted and the keys used for both techniques are analysed, it is anticipated that the space complexity for keeping encrypted files and source files would decrease.

4 Design Specification

The system is designed to function in the following ways:

- Step 1: Users must first sign in if they have previously registered or register by supplying information such as their mail id, user name, password, contact number, etc.
- Step 2: Once a user has registered for the application, an automatically generated password will be sent to the verified email address provided during registration.
- Step 3: The user can access local storage for data files to upload after logging onto the system.
- Step 4: Before transmitting the chosen data to the recipient end, the user might then encrypt it. Users of the described approach can choose to combine RSA and AES.
- Step 5: In addition, the user has the ability to access and examine the files they have submitted.
- Step 6: The decryption key is transferred to the email details provided during registration or login when a recipient selects a file to download.
- Step 7: This key can then be used by the user to download the decode or original file.

4.1 Environment Configuration

The Windows Operating System serves as the infrastructure needed to construct the model. The model was created in Visual Studio Code using C sharp .NET. Here, a hybrid crypto system is designed to be as efficient as possible while utilizing a less complicated architecture.

4.2 Architecture

In order to safeguard files, a hybrid cryptosystem is utilized. It consists of two stages. The information is originally divided into two stages, encryption and decryption components, as indicated in the architecture below fig[2].

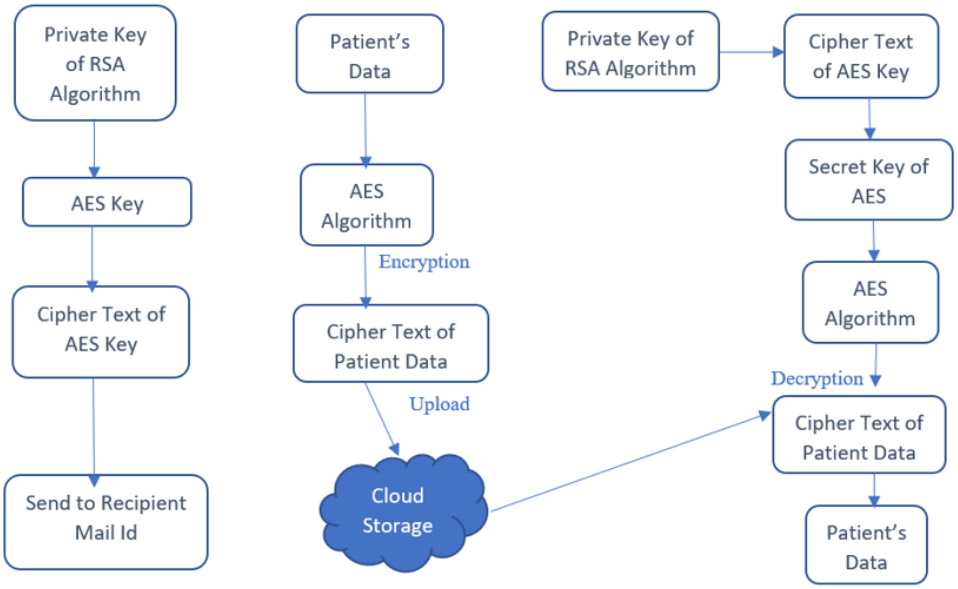

Figure 2: Hybrid Crypto System

4.3 Encryption Phase

As depicted in Figure, the encryption procedure was carried out in a number of steps. First, use the file system module to encode the downloaded file, and then divide it into two halves. Two distinct cryptographic methods, such as RSA and Advanced Encryption Standard algorithms (AES), are used to encrypt each component. After merging the sections, a single file is created and sent to the cloud once more fig[3].

4.4 Decryption Phase

The processes used in the decryption process are the exact reverse of those in the encryption process. First, the encrypted file must be downloaded, after which it is split into two halves and disseminated for decoding using the encrypted technique (AES and RSA) fig[4].

5 Implementation

Here, an effective PGP cryptographic system is created by designing it so that the optimal outcomes are attained utilizing a less sophisticated architecture. The following provides an explanation of the hardware and software requirements for development process.

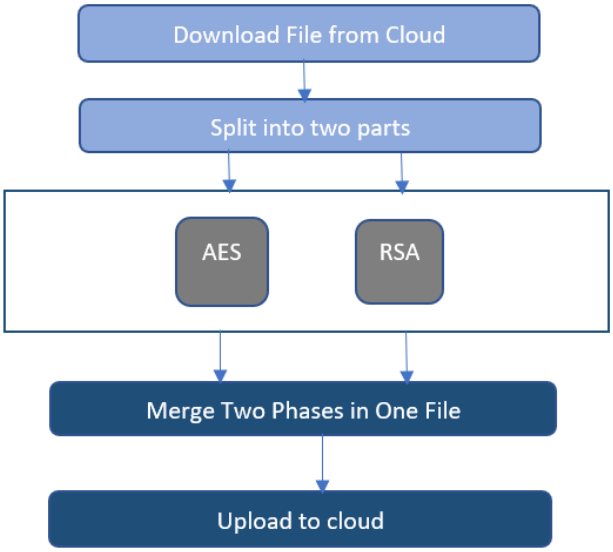

Figure 3: Proposed Encryption Process

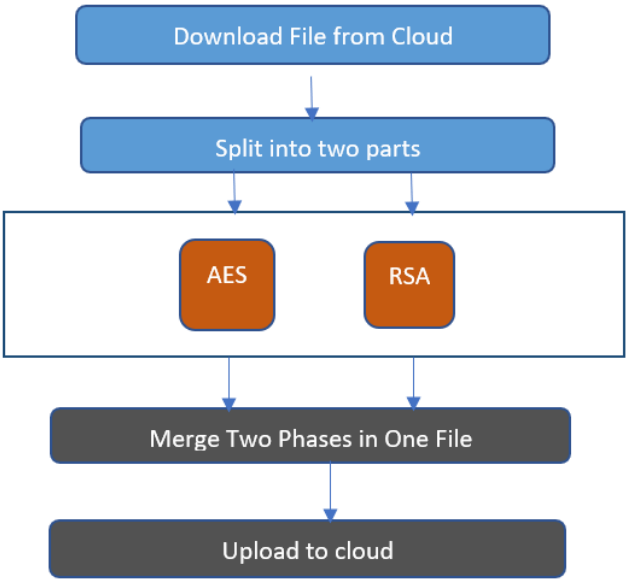

Figure 4: Proposed Decryption Process

5.1 System Specification

The system is created on a machine running Windows 10 with an Intel Core i5 processor, 8GB of RAM, and a 10GB hard drive. The foundational language is C sharp .Net. The text editor of choice is the version 15.0 of Visual Studio 2022 fig[5] and fig[6].

Operating System	Windows 10
Language used	C#
Code editor (IDE)	Visual Studio 2022

Figure 5: Software Specifications

RAM Used	8GB
HDD	10 GB
Processor	Intel core i5

Figure 6: Hardware Specification

5.2 Language used

All of the project's web pages were created using Asp.net. Due to its distinct advantages, C sharp .NET was selected as the programming language for this project's development. The majority of cryptographic libraries or packages are supported by C, making them very accessible and user-friendly. C is a language that was created specifically to facilitate web technology operations.

5.3 Flow Diagram

The proposed approach is responsible for fulfilling the cloud storage facility's current security criteria. Files are encrypted using RSA and AES, which take the least amount of time to cipher and decrypt when compared to other symmetric and asymmetric methods. When used in a cloud setting, the hybrid approach gives the remote server the highest level of protection. As a result, it aids cloud service providers in winning over more customers. The technique transforms the original data into a portion of unreadable format. Only the authorized individual gets access to the decrypted data from the cloud server, although all users can see the cipher data because it is symmetrically encrypted. The key is created immediately following the encryption of the data. Then, the recipient requests the encrypted data and the key from the sender. The recipient will use it to decode using each key after the owner accepts it from his mail ID. The data will be concurrently decrypted by the algorithm and the recipient's key entry fig[7].

6 Evaluation

The study of utilizing mathematics to encrypt and decrypt data is known as cryptography. It offers a technique to keep private information safe or send it through unsecure networks

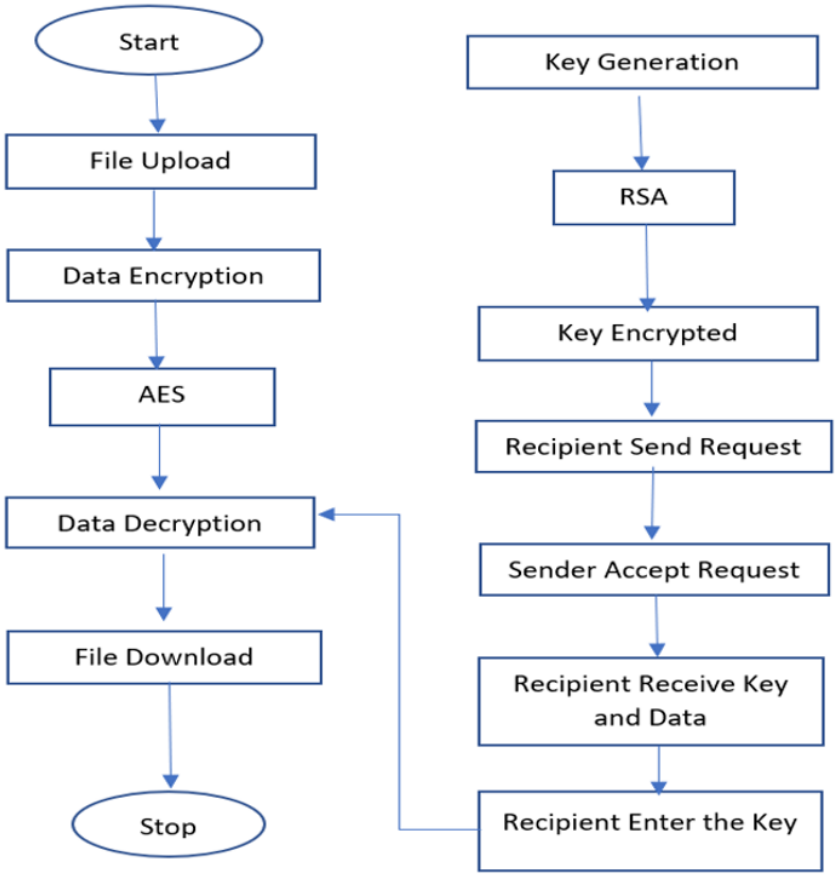

Figure 7: Hybrid crypto system flowchart

File Size (MB)	AES (Time in Sec)	Hybrid (Time in Sec)
1	5.093	4.493
2	12.28	10.240
4	23.289	18.59
8	46.295	37.263

Table 2: Encryption Time between AES Hybrid Algorithm

where only the intended recipient may access it.This method is frequently used to secure data traveling over unprotected and open networks. Worldwide research institutions have used a large number of cryptographic algorithms.The paradigm for performance analysis of cryptographic algorithms is presented in this paper. The performance analysis in this study is also demonstrated using the AES and RSA algorithms.The two factors chosen for assessing the effectiveness of AES, RAS, and Hybrid Cryptographic Algorithms are time and file size.Based on various file sizes, the encryption time can be determined as the amount of time needed by the algorithm to convert plain text into an encrypted text (cipher text). Additionally, the amount of time it takes for an algorithm to create the original plain text from a cipher text can be used to compute the decryption time.Maximum security should be offered via an efficient method, and operations should be completed faster. The hybrid of the aforementioned algorithms offers greater security and faster completion than when combined with high security.

6.1 Proposed Evaluation

Information transmission capabilities may be diminished because of the utilization of methods that promote information privacy in the cloud since encoding and decoding data requires time, which is a significant factor when deploying cryptographic techniques. There is no denying that consumers of cloud services have other considerations besides safety. Algorithms were selected for this investigation based on their decryption and encryption speed capabilities. With the use of .NET programming, file encoding and decoding duration's are computed. When analysing the current AES and RSA algorithms, file encrypt, and decryption speeds are computed for data files. Since hybrid combines two separate algorithms, it offers greater security than a conventional encryption method. Here, we employ the open-source symmetric key method AES. AES offers greater security than other symmetrical algorithms due to its huge key size of up to 128 bits. The AES keys have been encrypted using the RSA technique. When compared to the conventional RSA approach, the proposed RSA method is faster. Because we were able to quickly generate significant prime numbers and solve large modular arithmetic operations values using two separate strategies here. The assessment of the encoding and decoding duration's for various source data volumes is shown in the tables [2],[3],[4] and [5] given.

6.2 Results for Algorithms Used

The suggested system uses the AES and RSA algorithms to secure data. The proposed solution incorporates RSA and AES. We ran tests on files with sizes 1, 2, 4 and 8 megabytes and files with sizes 100, 200, 400 and 800 kilobytes on the algorithms to see how quickly they executed the data. The hybrid method and other algorithms were put into

File Size (KB)	RSA (Time in Sec)	Hybrid (Time in sec)
100	1.493	1.393
200	2.814	2.240
400	5.589	5.134
800	8.195	7.263

Table 3: Encryption Time between RSA Hybrid Algorithm

File Size (MB)	AES (Time in Sec)	Hybrid (Time in sec)
1	7.093	5.493
2	16.28	15.240
4	33.289	28.59
8	40.295	35.263

Table 4: Decryption Time between AES Hybrid Algorithm

practice using the .Net programming language, and testing were conducted using a system configuration with Intel core i5 processing at 2.50 GHz and the RAM size of 8Gegabyte.

The suggested technique requires the shortest amount of time to encode files, as illustrated in Fig. 8. The symmetric and asymmetric cryptography techniques are combined and run concurrently in the suggested system.In comparison to the current system, the hybrid algorithm requires 17 to 20 percentage less time for data files.Data in public cloud is not highly secure when only specific algorithm is used. Figure 9 illustrates how the current system requires 15 to 17 percentage more time to decrypt files than the hybrid technique.The AES algorithm achieves the quickest decryption time. however offers less protection for data.If the key size in AES increases, the number of cycles naturally increases, which raises the time required to encrypt and decrypt data. Progressive Encryption When compared to alternative symmetric techniques, the standard algorithm requires the minimum amount of time to encrypt files. As can be shown in Fig. 10, the suggested approach requires 12 to 15 percentage less time to encrypt files than AES.A secret key is used in the suggested hybrid technique for both data encoding and decoding. As illustrated in Figure 11, the suggested approach for file decryption requires 10 to 12 percentage less time than RSA.In a hybrid approach, file decoding takes the longest amount of time compared to encryption.However, compared to the AES technique, the RSA algorithm requires less time to decrypt data files.In comparison to encryption, the RSA technique requires the most time for file deceyption.

File Size (KB)	RSA (Time in Sec)	Hybrid (Time in sec)
100	1.493	1.393
200	2.814	2.240
400	5.589	5.134
800	8.195	7.263

Table 5: Decryption Time between RSA Hybrid Algorithm

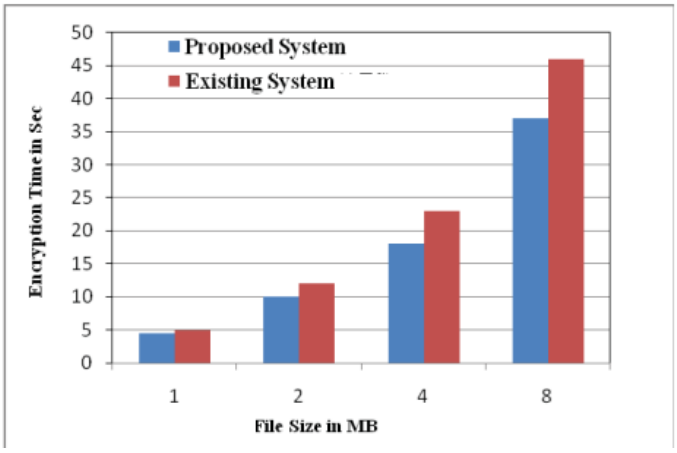

Figure 8: Comparison of Encoding Time of Hybrid Model to AES

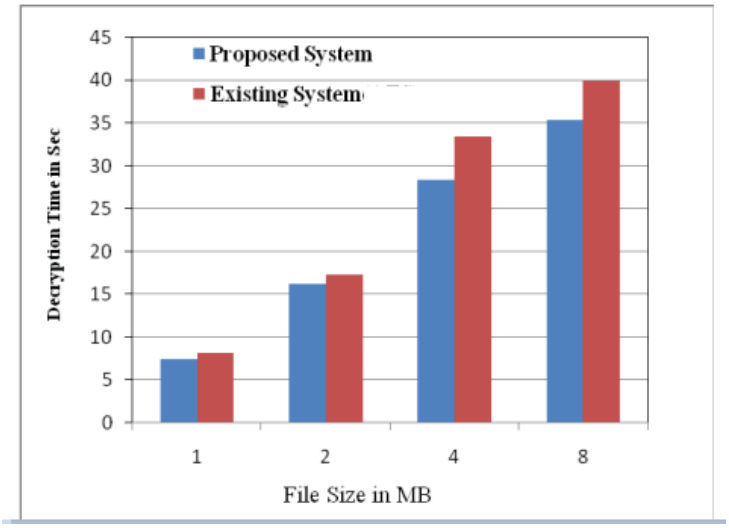

Figure 9: Comparison of Decoding Time of Hybrid Model to AES

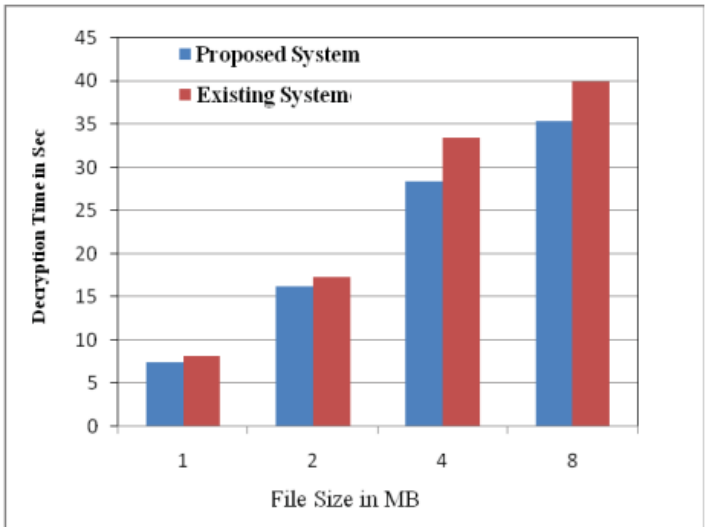

Figure 10: Comparison of Encoding Time of Hybrid Model to RSA

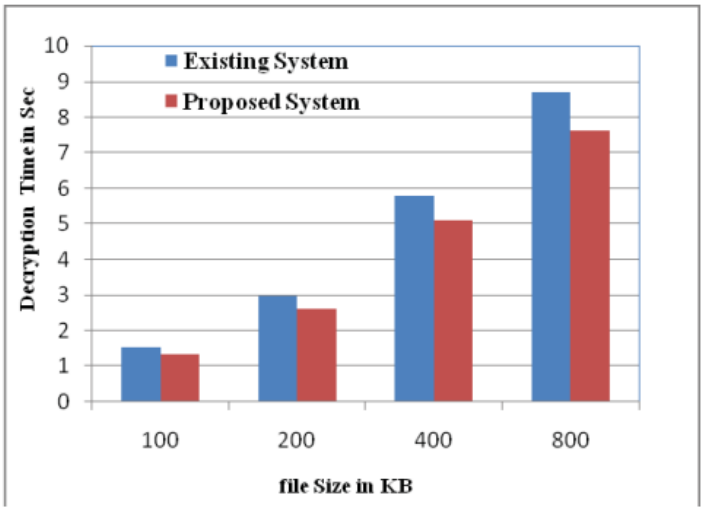

Figure 11: Comparison of Decoding Time of Hybrid Model to RSA

6.3 Security Analysis

6.3.1 Security from computational assault

For the data and key encryption procedure inside the hybrid crypto model, we used two different algorithms.This enhanced key and data protection. The attack, however, is not possible while the data is already protected.

6.3.2 Aside-Channel Attack Security

The AES algorithm's security is based on a difficult round key operation.Because each operation is based on a different set of coordinates, AES must perform numerous operations to compute the cycle.Additionally, it offers defense against differential fault assaults.

7 Conclusion and Future Work

The challenges and various security measures to safeguard the privacy of health records on current systems are described in this study. hybrid cryptographic technique based on PGP is suggested as the proposed scheme, and it satisfies the necessary security and privacy requirements. Health record owners must have complete control over any outsourced private health data in order to ensure patient data exchange. Therefore, it's crucial to store health data in an encrypted way on third-party cloud infrastructure. Improving the privacy of health information reserved in the cloud environment by combining symmetric encryption (using the AES method) and asymmetric scheme (using the RSA algorithm). The RSA algorithm encrypts the message containing any personal information or data that the sender wants to send to the receiver using the security code produced by the AES method. The suggested technique dramatically streamlines key management while preserving anonymity. It provides users with perfectly alright data access and supports big datasets that are textual, and image based. Additionally, it improves overall performance while reducing the time and money needed for encryption. Currently, this method only allows for the uploading of a single file at a time and does not yet take numerous file uploads into account while encrypting and decrypting textual data. However, this issue would be taken into account in further development.

References

Agarwala, A., Singh, P. and Atrey, P. K. (2017). Dice: A dual integrity convergent encryption protocol for client side secure data deduplication, *2017 IEEE international conference on systems, man, and cybernetics (SMC)*, IEEE, pp. 2176–2181.

Domadiya, N. and Rao, U. P. (2022). Elgamal homomorphic encryption-based privacy preserving association rule mining on horizontally partitioned healthcare data, *Journal of The Institution of Engineers (India): Series B* pp. 1–14.

Farzana, S. and Islam, S. (2019). Symmetric key-based patient controlled secured electronic health record management protocol, *Journal of High Speed Networks* **25**(3): 221–237.

John, A. O., Shola, P. and Philip, S. (2015). Comparative analysis of discrete logarithm and rsa algorithm in data cryptography, *International Journal of Computer Science and Information Security* **13**(2): 24.

Lin, H.-Y. and Jiang, Y.-R. (2020). A multi-user ciphertext policy attribute-based encryption scheme with keyword search for medical cloud system, *Applied Sciences* **11**(1): 63.

Liu, X., Yang, X., Luo, Y., Wang, L. and Zhang, Q. (2020). Anonymous electronic health record sharing scheme based on decentralized hierarchical attribute-based encryption in cloud environment, *IEEE Access* **8**: 200180–200193.

Lu, H., Chen, J. and Zhang, K. (2021). Verifiable dynamic searchable symmetric encryption with forward privacy in cloud-assisted e-healthcare systems, *International Conference on Algorithms and Architectures for Parallel Processing*, Springer, pp. 645–659.

Mythri, G. and Jayram, B. G. (2017). Feature based encryption for data privacy and access control for medical application, *2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC)*, IEEE, pp. 175–179.

Nadaf, S. J. and Patil, R. (2016). Cloud based privacy preserving secure health data storage and retrieval system, *2016 International Conference on Inventive Computation Technologies (ICICT)*, Vol. 2, IEEE, pp. 1–6.

Obiri, I. A., Xia, Q., Xia, H., Affum, E., Abla, S. and Gao, J. (2022). Personal health records sharing scheme based on attribute based signcryption with data integrity verifiable, *Journal of Computer Security* (Preprint): 1–34.

Oh, S. E., Chun, J. Y., Jia, L., Garg, D., Gunter, C. A. and Datta, A. (2014). Privacy-preserving audit for broker-based health information exchange, *Proceedings of the 4th ACM conference on Data and application security and privacy*, pp. 313–320.

Owolabi, O. Y., Shols, P. and Jibrin, M. B. (2017). Improved data security system using hybrid cryptosystem, *201.7 IJSRSET* **3**(3).

Pariselvam, S. and Swarnamukhi, M. (2019). Encrypted cloud based personal health record management using des scheme, *2019 IEEE International conference on system, computation, automation and networking (ICSCAN)*, IEEE, pp. 1–6.

Shabbir, M., Shabbir, A., Iwendi, C., Javed, A. R., Rizwan, M., Herencsar, N. and Lin, J. C.-W. (2021). Enhancing security of health information using modular encryption standard in mobile cloud computing, *IEEE Access* **9**: 8820–8834.

Sharma, K., Agrawal, A., Pandey, D., Khan, R. and Dinkar, S. K. (2019). Rsa based encryption approach for preserving confidentiality of big data, *Journal of King Saud University-Computer and Information Sciences* .

Thakur, J. and Kumar, N. (2011). Des, aes and blowfish: Symmetric key cryptography algorithms simulation based performance analysis, *International journal of emerging technology and advanced engineering* **1**(2): 6–12.

Xu, C., Wang, N., Zhu, L., Sharif, K. and Zhang, C. (2019). Achieving searchable and privacy-preserving data sharing for cloud-assisted e-healthcare system, *IEEE Internet of Things Journal* **6**(5): 8345–8356.

Zhang, Q. and Ding, Q. (2015). Digital image encryption based on advanced encryption standard (aes), *2015 Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control (IMCCC)*, IEEE, pp. 1218–1221.