

Data Security on cloud using Hybrid Cryptography a PGP based encryption methodology.

MSc Research Project
Cloud Computing

Ali Saif

Student ID: x22155996

School of Computing
National College of Ireland

Supervisor: Sean Heeney

National College of Ireland
Project Submission Sheet
School of Computing



Student Name:	Ali Saif
Student ID:	22155996
Programme:	Cloud Computing
Year:	2023
Module:	MSc Research Project
Supervisor:	Sean Heeney
Submission Due Date:	14 December 2023
Project Title:	Data Security on cloud using Hybrid Cryptography a PGP based encryption methodology
Word Count:	5680
Page Count:	20

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:	Ali Saif
Date:	14th December 2023

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST:

Attach a completed copy of this sheet to each project (including multiple copies).	<input type="checkbox"/>
Attach a Moodle submission receipt of the online project submission , to each project (including multiple copies).	<input type="checkbox"/>
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.	<input type="checkbox"/>

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):	

Data Security on cloud using Hybrid Cryptography a PGP based encryption methodology

Ali Saif
x22155996

Abstract

This report outlines a web application that uses Elliptic Curve Cryptography (ECC) and Advanced Encryption Standard (AES) to improve data security in digital communications. The application uses C#.NET for programming and Microsoft SQL Server for database administration, leveraging the .NET Framework and ASP.NET. The cloud-based implementation, hosted on Microsoft Azure, makes use of Azure App Service and SQL Database Service to provide a safe platform for data transfers. The programme prioritises data security by utilising a hybrid technique that combines AES and ECC for PGP encryption. A comparative investigation reveals that ECC is the best cryptographic method. ECC's efficiency in producing lower key sizes without sacrificing security, along with quicker cryptographic operations, demonstrates its benefit over RSA, which is especially noticeable when dealing with bigger file sizes. This abstract covers the technical stack, cloud deployment, the emphasis on ECC and AES in PGP, and the comparative study demonstrating ECC's superiority over RSA for data security in a nutshell.

0.1 IndexTerms

Elliptic Curve Cryptography (ECC), AES (Advanced Encryption Standard), Microsoft SQL Server, Microsoft Azure, Cloud Deployment

1 Introduction

1.1 Background

Technology, along with security, is a big concern all over the world. Users are adopting all technologies, from basic computing to cloud computing. No one is willing to accept technologies that cannot safeguard information. In today's digital world, providing robust data security is a top need, particularly for web applications hosted on cloud platforms. James and Rabbi (2023)(James and Rabbi, 2023). Cloud computing allows users to access storage, software, data, and servers from anywhere in the world via internet-connected devices such as computers, smartphones, tablets, and wearables. Data in the cloud is available to authorised users, allowing retrieval or access without the need for a direct server connection. Jian-Foo Lai (2022)Jian-Foo Lai,Swee-Huay Heng(2022). This research digs into the creation and evaluation of data security measures, with a special emphasis on Microsoft Azure cloud deployment and data encryption utilising the Pretty Good Privacy

(PGP) architecture strengthened with ECC and AES algorithms. The research intends to investigate the usefulness of ECC and AES in enhancing data security and secure data transfers inside Azure cloud settings by leveraging Azure's powerful services such as Azure App Service and SQL Database Service. The study will also evaluate the PGP system's correctness and performance when compared to existing cryptographic systems, to elucidate its role in enhancing data security within online applications. This project aims to give useful insights into preserving data security and confidentiality in the digital arena by concentrating on Azure's cloud infrastructure and incorporating sophisticated cryptographic algorithms like ECC and AES inside the PGP framework.

1.2 Aim of the study

The major goal of this research is to strengthen data security within online applications, with a specific focus on Microsoft Azure cloud deployment, by integrating ECC and AES algorithms within the Pretty Good Privacy (PGP) framework. The purpose is to examine the correctness and performance of the PGP system in comparison to existing cryptographic algorithms, as well as to evaluate the usefulness of ECC and AES in safeguarding data transmissions inside Azure cloud settings, stressing their roles in enhancing data protection. The study aims to provide insights into leveraging Azure's cloud services, such as Azure App Service and SQL Database Service, to create a secure platform for data exchanges, with an emphasis on the integration of ECC and AES within the PGP framework to improve data security in Azure-deployed web applications.

1.2.1 Research Question

The research questions for this report is:

1. How can a hybrid cryptographic solution that incorporates the best cryptographic techniques (AES+ECC) can be built to improve data security within cloud platforms while maintaining robust protection against potential vulnerabilities and threats?

1.3 Research Objectives

The research objectives of this report are:

1. In terms of encryption and decryption operations, compare the performance and efficiency of Elliptic Curve Cryptography (ECC) and Rivest-Shamir-Adleman (RSA) methods.
2. To create and evaluate a web application fortified with ECC and AES algorithms to assure data security in digital transactions, using the .NET Framework, ASP.NET, C#.NET, and Microsoft SQL Server for strong database administration.
3. To examine at the security features and practicality of putting the programme on Microsoft Azure using Azure App Service and SQL Database Service for safe cloud-based data storage and application hosting.
4. To assess the effectiveness of incorporating Advanced Encryption Standard (AES) and ECC into the Pretty Good Privacy (PGP) architecture for improved data security and secure data sharing capabilities.

1.4 Document Structure

This research report is structured into different Sections. The literature review depicts the prior research which has been done on securing the cloud data is provided in Section 2 of the research paper. Moving on to the methodology section the research deeply explores the techniques used for data security using encryption which is evident from Section 3 of the report. Section 4 of the research report is the main root of the report which describes the design specification of the proposed system and configuration. The technique of implementation is thoroughly covered in Section 5 of the report. Section 6 of the research report conducts various experiments and discussion on the results of the proposed model and includes methodology used to assess each model's accuracy and performance. With section 7 the report comes to the conclusion part and the future work.

2 Literature Review

2.1 PGP-based encryption using AES

Several researchers have made major progress in enhancing data protection across multiple domains while examining the cybersecurity landscape. Kale and Darekar (2018) (Kale and Darekar, 2018) attempted to improve data security by using 3D-AES, an improved version of the Advanced Encryption Standard (AES) that shuffles the original key array numerous times, significantly enhancing data encryption. Similarly, . Jothy and Delsey (2018) (Jothy et al., 2018) advocated using TRIPLE AES and PGP/SSL protocols to strengthen cloud computing security, highlighting the need of complete encryption solutions in cloud contexts. .Khairunisa and Kabetta (2021) (Khairunisa and Kabetta, 2021) used layout obfuscation in conjunction with AES-256 encryption in PHP-based applications to prevent source code disclosure and modification, demonstrating the value of encryption augmentation for increased security. Lee et al. (2018) (Lee et al., 2018) explored the integration of AES encryption inside the Heroku platform, demonstrating its usefulness in guaranteeing data security despite issues with encryption delays for bigger data quantities. Finally, . Indriyawati et al. (2021) (Indriyawati et al., 2021) addressed inefficiencies in document certification by developing a web-based system that uses AES encryption with an improved key size, allowing secure access via PHP-based interfaces and QR codes. Their common goal was to use AES encryption, either in its standard or upgraded versions, to improve data security across cloud platforms, PHP applications, as well as academic document certification systems.

. Biswal and Pattanayak (2022) Biswal et al. (2022) conducted a groundbreaking study in which they introduced a portable interior sensor system coupled to a smartphone-based interface for measuring temperature and humidity. Their breakthrough included an ESP8266 microcontroller, a DHT11 temperature sensor, and strong encryption methods such as AES and MD5 hashing, which ensured safe data transfer and user access. Meanwhile, Joshi et al. (2018) investigated ways to improve PGP security, with an emphasis on digital signatures and message encryption. To strengthen digital signatures and communications, they recommended combining RSA 4096 and AES-256 for asymmetric and symmetric encryption, respectively, with the powerful Whirlpool hashing algorithm. Both researchers encountered difficulties in smoothly incorporating these advanced cryptographic algorithms into their systems while assuring maximum performance.

Author	Focus	Encryption Method	Challenges Faced	Key Findings
Kale and Darekar (2018)	Enhancing data security via an advanced version of AES	3D-AES	Implementation complexities, Computational overhead	Improved data security through iterative shuffling, reduced encryption time
Jothy et al. (2018)	Strengthening cloud security with AES, PGP, and SSL protocols	TRIPLE AES, PGP/SSL protocols	Interoperability issues	Enhanced cloud security through robust encryption methods, emphasis on comprehensive strategies
Khairunisa and Kabita (2021)	Enhancing PHP application security with AES and obfuscation	AES with layout obfuscation	Performance impact	Strengthened PHP application security against source code exposure and manipulation
Lee et al. (2018)	Implementing AES encryption within Heroku	AES encryption within Heroku	Encryption delay for larger data sizes	Validation of AES efficacy in ensuring data security within cloud platforms
Indravati et al. (2021)	Securing document certification system with AES	AES with upgraded key size	Optimizing encryption process, seamless integration for decryption	Improved document certification security, facilitated secure access through web and QR code interfaces
Biswal et al. (2022)	Indoor Sensor System	AES, MD5 hashing	Hardware constraints, communication reliability	Secure IoT system for temperature/humidity monitoring, AES encryption, user data access control
Joshi et al. (2018)	PGP Security (Digital Signatures & Encryption)	RSA 4096, AES-256, Whirlpool hashing	Computational efficiency, integration of complex algorithms	Enhanced PGP security, robust digital signature and message encryption, Whirlpool hashing strength

Figure 1: Comparative Table of PGP-based encryption using AES

2.2 Encryption using ECC

The rise of cloud computing, real-time media apps, and IoT devices in recent years has altered the technological environment, bringing in incredible improvements but also exposing important security vulnerabilities. (2022)(Ghadi, 2021) and colleagues investigated elliptic curve cryptography (ECC) and its integration with current systems, providing approaches to improve encryption and strengthen data security. (2020)(AlMajed and AlMogren, 2020) focused on IoT settings, attempting to improve security through authenticated encryption and focusing on the plaintext-to-elliptic-curve mapping step to resist encryption attacks. Likewise, . Yathiraju (2022)(Goyal et al., 2019)focused their efforts on cloud security, developing designs that incorporate ECC, MD5 for integrity preservation, and RBAC approaches for access control, therefore reinforcing cloud environments against infiltration attempts. . 18. Sen and Thompson (2020)(Sen et al., 2020) attempted to secure real-time voice communications by integrating ECC-based encryption into softphones and painstakingly selecting elliptic curves optimal for audio encryption to balance security without sacrificing call quality. Addressing weaknesses in WPA/WPA2 PSK networks, . Singh and Nandi (2019)(Singh et al., 2019) suggested an alternative authentication technique based on ECC to resist known attacks and minimise the number of frames necessary for authentication and re-authentication.

. Yathiraju (2022)(Yathiraju, 2022) forayed into the realm of federated learning, proposing Elliptical Curve Cryptography using Blockchain-based Federated Learning (ECC-BFL) as a method to protect user privacy in distributed machine learning. They rigorously evaluated ECC-BFL to current approaches, emphasising its ability to achieve 95% classification accuracy, lower overheads, and im-

prove transaction speed. . Chilveri and Nagmode (2022)(Chilveri and Nagmode, 2020)traversed the Multi-Server Authentication environment in networks like as MANET and WSN, applying Elliptic Curve Cryptogr in a protocol to segregate credentials and strengthen security against possible assaults, exhibiting increased authentication robustness. . Sudarsono and Al Rasvid (2018)(Sudarsono and Rasvid, 2018) addressed IoT-related email security problems, arguing for a solution that uses Certificateless Cryptography (CLC) and Elliptic Curve-based encryption to provide confidentiality and integrity. For further protection, their system included multi-factor authentication.. Abdelfattah and Attia (2018)(Abdelfattah et al., 2019) changed email security by combining encryption and authentication into a single step and providing flexible email transmission choices. Finally,. 25. Duka (2020) (Duka, 2020) investigated the effectiveness of ECC and Argon2 hashing in PHP, investigating the effect of initialization settings on cryptographic operations within the Sodium library

Author	Focus	Security Technique	Challenges	Key Results
Ghadir (2021)	Ciphertext security	Integration of ECC with ElGamal ECC	Complexity integration, efficiency	Enhanced security, efficiency in encryption
AlMajed & Almgren (2020)	IoT Security	Authenticated encryption using ECC	Integration, encryption attacks	Strengthened IoT security, enhanced encryption
Goyal et al. (2019)	Cloud Security	ECC, MD5, RBAC techniques in architectures	Integration, intrusion prevention	Improved cloud security, robust intrusion prevention
Sen et al. (2020)	Real-time Voice Calls Security	ECC-based encryption in softphones	Selection of optimal elliptic curves	Secured voice calls, minimized end-to-end delays
Singh et al. (2019)	WPA/WPA2 PSK Network Security	ECC-based authentication mechanisms	Authentication redesign, frame reduction	Mitigated network vulnerabilities, streamlined auth.
Yathiraju (2022)	Privacy in Federated Learning	ECC-BFL: Elliptic Curve Cryptography with Blockchain in FL	Integrating ECC with blockchain; Comparison with established methods; Maintaining accuracy while preserving privacy	95% classification accuracy; Reduced overheads; Enhanced transaction speed
Chilver & Nag mode (2020)	Multi-Server Authentication	ECC in protocol for robust authentication in MANET/WSN	Integration challenges; Security against potential attacks; Efficient credential handling	Enhanced authentication robustness; Secure server-based authentication
Sudarsono & Rasyid (2018)	IoT Email Security	CLC-EC-based system for email security and integrity	Implementing multi-factor authentication; Ensuring confidentiality and integrity in email transmission	Improved confidentiality, integrity, and multi-factor authentication in IoT email security
Abdelfattah et al. (2019)	Secure Email Communication	CLC-EC-based system integrating	Integrating CLC-EC for efficiency;	Enhanced security, streamlined

Figure 2: Comparative Table of Encryption using ECC

3 Methodology

3.1 Pretty Good Privacy Approach (PGP)

As per Sec.2,1 where the PGP-based encryption using AES has been found a very efficient and accurate way of providing data security in cloud where PGP offers strong security and authentication in applications such as email and data storage. It uses symmetric key encryption to generate session keys, which are then encrypted for safe transmission. Encrypting this symmetric key with public key

cryptography ensures its secrecy throughout exchange. Asymmetric encryption is important because only the recipient's secret key can unlock the session key, making it inaccessible to possible attackers. Due to the temporal complexity required, this technique effectively thwarts decoding attempts. PGP guarantees that the session key stays secure and only available to the intended recipient by combining symmetric and asymmetric encryption, ensuring communication and data integrity in these applications.

3.2 Advanced Encryption Standard (AES)

In terms of cloud data security, combining Hybrid Cryptography with PGP-based encryption appears to be a formidable method. The Advanced Encryption Standard (AES) algorithm is the cornerstone of block iterative encryption. This approach supports many 128-bit of plaintext chunks that evaluate the total data. The secret key length is classified as AES-256, AES-192, AES-128 or with 14, 12, or 10 calculation cycles required to function.

The manipulation of a 128-bit plaintext frame within the State byte matrix is at the heart of AES. This matrix serves as the foundation for all AES procedures. The procedure begins with key extension, in which round keys are created and used for both encryption and decryption. The XOR operations used in the 'Insert Round Key' step fuse the State matrix also with original 128-bit private keys, following a new State matrix.

The last encryption round eliminates the 'Mix Columns' procedure observed in the first nine rounds, bringing the encryption process to a close. The use of Hybrid Cryptography in conjunction with PGP-based encryption in cloud data security demonstrates the resilience of this method. PGP's hybrid encryption, which mixes symmetric and asymmetric encryption, enables safe key exchange and strong data security. This strategy efficiently mitigates the security vulnerabilities that exist in cloud systems, ensuring data confidentiality and integrity.

3.3 Elliptic Curve Cryptography (ECC)

Implementing the Elliptic Curve Cryptography (ECC) algorithm becomes critical for ensuring robust security measures within this infrastructure, particularly with App Service for website deployment and SQL Database Service for database management. ECC, known for its efficiency and strong encryption capabilities, is particularly suited to cloud environments due to its ability to provide high-level security with smaller key sizes than other encryption methods. This is critical inside Azure's framework, particularly when sensitive data is handled via the SQL Database Service. Smaller key sizes in ECC lower computing needs dramatically, which corresponds nicely with the cloud's resource optimization goals, allowing for speedier encryption and decryption procedures while retaining rigorous security standards. The functionality of the technique focuses around the mathematical principles of elliptic curves, allowing for safe key generation and encryption operations. ECC employs a public-private key pair to provide safe communication and data security. It may be used in this context to protect data communications between the App Service for website deployment and the SQL Database Service, providing a secure route for sensitive information sharing.

Using ECC in the Azure cloud infrastructure strengthens data integrity, secrecy, and authentication processes. Its efficient cryptographic operations are in line with the scalability and performance requirements of cloud-based services such as Mi-

Microsoft Azure, offering excellent security without sacrificing system speed. Because Azure services handle website deployment and database management, ECC's strong encryption capabilities serve a crucial role in protecting important data and communications, strengthening the overall security posture inside the Azure cloud environment.

3.4 Microsoft Azure Cloud

This research is employing on Microsoft Azure Cloud which may effectively incorporate on the cloud-based public services into existing Information Technology infrastructures, independent of programming language. Windows Azure provides a wide range of options that enable customers to efficiently manage access to their data and implementations: Businesses may simplify user authentication and access control for their cloud-based services by connecting data from their central offices with Windows Azure's Domain Controller.

The use of privacy logs is a vital element that allows for real-time tracking of information flows. These logs are useful tools for risk mitigation methods, as well as for assuring openness and accountability in data exchanges. Windows Azure enables various validation processes while also improving security measures to prevent unwanted access. These approaches not only prevent unauthorised logins, but also introduce multi-factor authentication, which adds an additional layer of verification beyond typical passcodes. Clients also benefit from strong authoriz-

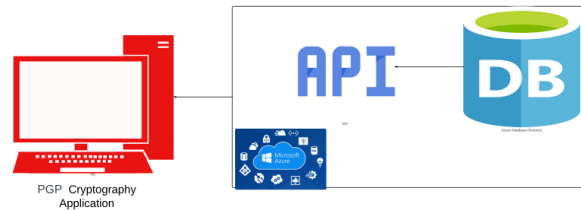


Figure 3: Cryptographic Implementation on cloud

ation mechanisms, which allow them to fine-tune resource access for users. This involves granting access based on work titles, hierarchical authority levels, and permitted rights. Granular access control improves data security by restricting user access privileges to appropriate resources based on their roles and responsibilities. Windows Azure's broad features in access management, user authentication, and permission restrictions strengthen data security inside cloud-based infrastructures. These features not only improve privacy and confidentiality, but they also provide an effective way to manage risks connected with illegal access or data breaches

2.

4 Design Specification

The system operates through the following functionalities:.

1. Registration and Sign-In Process: Users must either sign in with their current credentials or register by giving basic information such as their Full name, email

address, username, address, and contact information..

2. **Registration Confirmation:** After registering successfully, an automatically created password is delivered to the confirmed email address supplied during registration, ensuring safe access to the programme..

3. **Accessing Local Storage:** Users have access to their local storage after logging into the system, allowing them to safely upload data files..

4. **Data Encryption:** Users can encrypt data before transferring it. For increased security, users can utilise a mix of ECC and AES encryption technologies.

5. **File Management:** Users may still access and evaluate the files they've uploaded, allowing for simple administration and monitoring of their saved data..

6. **Decryption Key Retrieval:** The decryption key is securely provided to the registered or logged-in email address that is a secret key which is linked with the file transfer when a receiver chooses to download a file..

7. **File Download and Decryption:** Users may safely download and decrypt the original file using the obtained decryption key, maintaining secrecy and integrity throughout the retrieval process. This Original random key will be used to decrypt the File using AES Algorithm.

4.1 Environment Configuration

The system is built on the .NET Framework, with ASP.NET for website creation and C#.NET as the major programming language. Microsoft SQL Server powers the database architecture, delivering comprehensive data management and security. Microsoft Azure plays an important role in cloud deployment, leveraging the App Service to assist smooth website deployment and SQL Database Service for efficient database administration within the cloud environment. Furthermore, the solution stresses data security with Pretty Good Privacy (PGP), which employs a combination of Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC).

4.2 Architecture

This architectural diagram depicts the step-by-step workflow of a secure data processing system. It starts with user authentication, either by logging in with current credentials or by registering new users. To guarantee safe access, an automatically created password is emailed to the specified email address upon registration. Once logged in, users may choose which files to encrypt, which generates a secret key and sends it to the user's email for further protection. The encryption procedure is carried out, guaranteeing that the file is converted to an encrypted format. Following that, the encrypted file is safely stored in a cloud storage system. To decrypt the file, the user enters the secret key obtained via email, which starts the decryption process and results in the original file being available for download. This process emphasises the importance of a secure end-to-end data handling system, which ensures data integrity and confidentiality throughout the encryption, storage, and decryption phases.

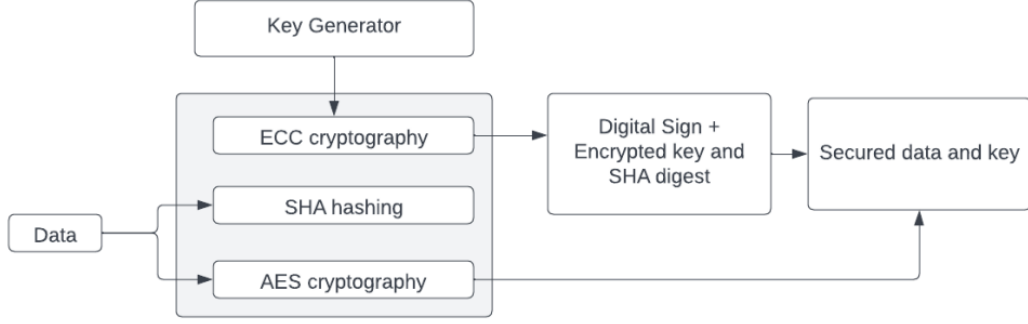


Figure 4: Architecture of the proposed system

4.3 Encryption Phase

The encryption step, as seen in the diagram, begins with encrypting the downloaded file via the file system module. Each segment is encrypted using two different cryptographic techniques: Elliptic Curve Cryptography (ECC) and Advanced Encryption Standard (AES). Following encryption, the sections are combined, resulting in a single file that is then transmitted back to the cloud. This strong encryption strategy coincides with this report’s focus on data security in cloud environments, adopting a mix of ECC and AES for increased file confidentiality and integrity

4.4 Decryption Phase

The decryption phase also follows the same techniques as the encryption phase but in reverse order. The encrypted file is first downloaded using a secret key which has been sent to the user’s email. This decryption method, which aligns with the focus of research on cloud data security, allows the secure recovery and reconstruction of the original file by reversing the encryption stages of AES and ECC encryption used during the encryption phase

5 Implementation

During the implementation phase, the system makes use of the .NET Framework’s powerful features, leveraging ASP.NET for website development and C#.NET as the major programming language, providing efficient and secure application design. The database architecture is built around Microsoft SQL Server, which provides a strong basis for data management. Microsoft Azure is the primary cloud platform, featuring App Service for website hosting and SQL Database Service for faster database administration in the cloud. PGP (Pretty Good Privacy) encryption is used in the implementation, as well as a combination of RSA + AES (an established project feature) and a revolutionary technique of ECC + AES encryption methods. ECC produces an asymmetric key pair upon user registration, which is critical for safe encryption and decryption operations. File transmission entails generating a random key for AES-based symmetric encryption, protecting data for transmission to the receiver, and encrypting this key using ECC, assuring safe key exchange. At the receiver’s end, the decryption procedure entails decrypting the received secret key with their private ECC key to get the original random key, allowing the file to be decrypted using the AES method. This thorough implementation maintains

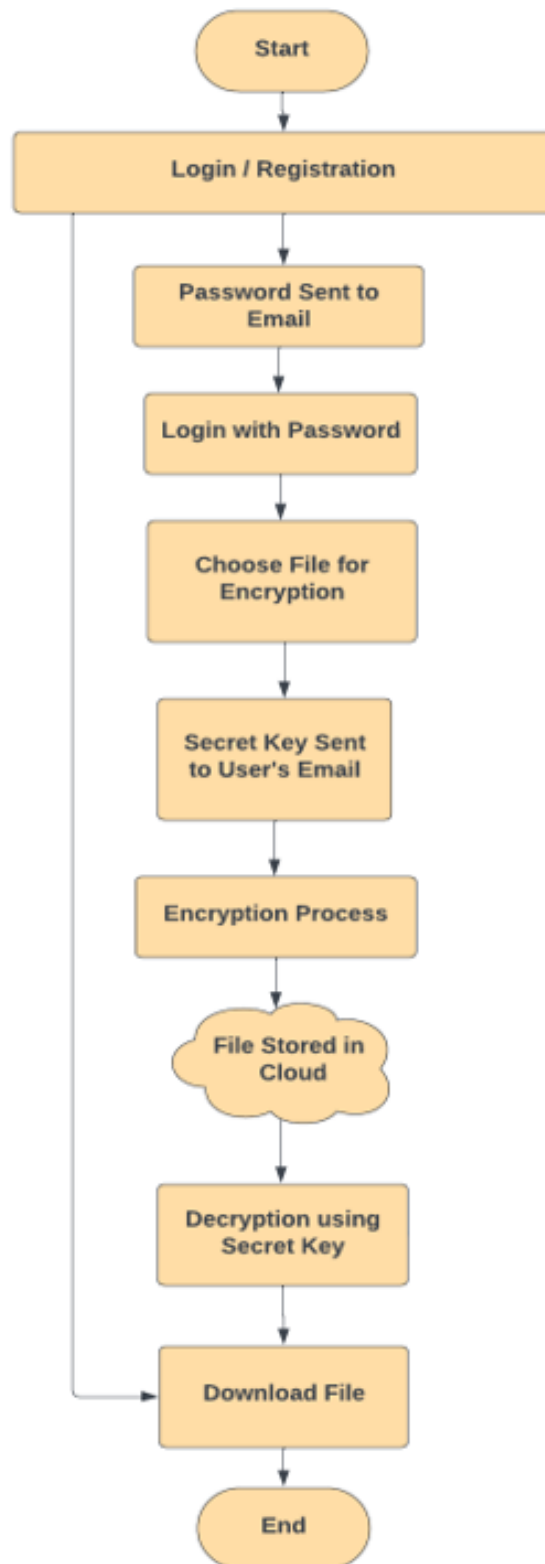


Figure 5: Workflow of the proposed system

data security and integrity during file transmission and retrieval within the Azure cloud environment, which aligns with the project's focus on safe cloud-based file sharing using PGP encryption.

5.1 System Specification

The system is designed to work within a set of settings and technical standards, which are listed below

5.1.1 Hardware Specifications

Component	Specification
Processor	Intel Core i7-10700K
RAM	16 GB DDR4
Storage	512 GB SSD
Network Interface	Gigabit Ethernet
GPU	NVIDIA GeForce RTX 3070

5.2 Software Specifications

Component	Version
Operating System	Windows 10 Pro
.NET Framework	4.8
Web Framework	ASP.NET
Programming Language	C#.NET
Database Management	Microsoft SQL Server 2019
Cloud Platform	Microsoft Azure


6 Evaluation

Cryptography is the study of using mathematical principles to encrypt and decode data, assuring the security of sensitive information or its transfer over insecure networks to just the intended receiver. This technology is commonly used to safeguard

data while it travels via open and insecure networks. A wide range of cryptographic algorithms have been investigated by academic organisations worldwide. This study proposes a framework for assessing the performance of such algorithms, with an emphasis on AES and ECC. The efficacy of AES, ECC, and Hybrid Cryptographic Algorithms is determined by two factors: time and file size. The encryption time, which varies according to file size, specifies the time required by the algorithm to transform plaintext to encrypted ciphertext. Decryption time, on the other hand, measures the algorithm's effectiveness in recovering original plaintext from ciphertext. The goal of efficiency in cryptography is to provide maximum security while yet operating quickly. The combination of these algorithms not only improves security but also speeds up processing, outperforming separate high-security solutions in terms of both security and operational efficiency.

6.1 User Registration

User can register by entering his or her details including full name, contact number, email, address as showing in figure 4



The screenshot shows a web application interface for PGP Encryption. On the left is a blue sidebar with the text "PGP ENCRYPTION". The main content area has a dark blue header with "Home" and a "Log out" button. Below the header, there is a registration form with the following fields: "Full Name:" with the value "Shafaq naz", "Contact Number:" with the value "9718371074", "Email Id:" with the value "shafaq.2017.naz@gmail.com", and "Address:" with the value "Delhi". A green "Save" button is located at the bottom of the form.

Figure 6: User Registration Screen

6.2 User Login

Users can Login by entering his or her details including User Name and Password which will come in respective email address as showing in figure 7.

6.3 Data Encryption

Here File is uploaded, and a secret key is generated which will be achieved on the respective mail address then encrypt file or data as shown in Figure 7

PGP Cryptography using ECC

User Name:

Password:

[Login](#) [Forget Password?](#) [Registration](#)

Figure 7: User Login Screen

PGP ENCRYPTION

Home

Home

Share Data / File

View Files

Forget Password

Encryption time: 0ms

Select User: shafaq.2017.naz@gmail.com

User key: RURLN3RAAAAATr1t3bWQzbH4KCEuLgBt4tqVwVuczdtdnU4PZ0ymq1tp33x8ntgph0dW4B@2qpt1N8Vvnt78rMAADKcdBdMACgB@egphVGX7yueC73bW

secret key: 20645932

Encrypt Key

Select File: Choose File No file chosen

Encryption time: 19ms

Encryption Size: 133760bytes

Encrypt Data Share

Figure 8: Upload Share Data / File on Cloud

6.4 Data Decryption

Enter that secret key and decrypt file also user can download file.

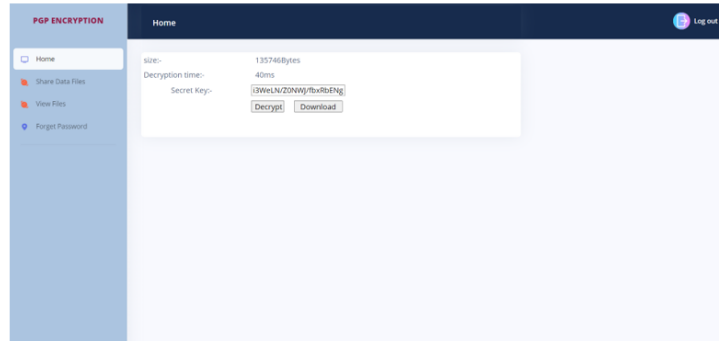


Figure 9: Decrypt file

6.5 ECC Algorithms Results

Tables 10 and 11 illustrate the encryption and decryption timings for various file sizes when assessing ECC techniques. Table 10. shows the encryption times for 33KB, 97KB, and 132KB files, with encryption times of 18ms, 21ms, and 19ms, respectively. Table 11, on the other hand, depicts decryption timings for the equivalent file sizes, indicating decryption times of 35ms, 39ms, and 40ms successively. The data shows that when file size rises, both encryption and decryption durations vary somewhat, highlighting the link between processing duration and file size inside ECC encryption and decryption procedures

Figure 10: Encryption Time of ECC (Image)

File Size (KB)	Encryption Time (m/s)
33	18
97	21
132	19

Figure 11: Decryption Time of ECC (Image)

File Size (KB)	Decryption Time (m/s)
33	35
97	39
132	40

Figure 12: Encryption Time of ECC (Pdf)

File Size (MB)	Encryption Time (m/s)
2	39
4	43

Tables 12 and 13 give encryption and decryption timings for ECC techniques especially applied to PDF files, with a focus on bigger file sizes. Table 10 shows the encryption timings for 2MB and 4MB PDF files, with encryption times of 39ms and 43ms, respectively. Table 13, on the other hand, shows decryption timings for similar PDF file sizes, with decryption times of 193ms for the 2MB file and 213ms for the 4MB file. These findings show a significant increase in processing times as file sizes rise, illustrating the effect of bigger file dimensions on ECC encryption and decryption processes in the context of PDF files

Figure 13: Decryption Time of ECC (Pdf)

File Size (MB)	Decryption Time (m/s)
2	193
4	213

6.6 RSA Algorithms Results

Tables 11 and 12 give insights into the performance of RSA algorithms when applied to picture files, with an emphasis on encryption and decryption durations across varied file sizes. Table 13 shows the encryption timings for picture files with sizes of 33KB, 97KB, and 132KB, with encryption times of 25ms, 28ms, and 32ms, respectively. It also indicates the time taken before encryption, as well as the entire processing time, which varies depending on file size. Table 15, on the other hand, shows decryption timings for the equivalent picture file sizes, with decryption times of 45ms, 52ms, and 55ms, respectively. These studies demonstrate the computing requirements of RSA encryption and decryption procedures on picture files, revealing that processing times rise as file sizes get larger

Figure 14: Encryption Time of RSA (Image)

File Size (KB)	Encryption Time (m/s)	Encryption Time before encrypted data (m/s)
33	25	49
97	28	55
132	32	44

Figure 15: Decryption Time of RSA (Image)

File Size (KB)	Decryption Time (m/s)
33	45
97	52
132	55

6.7 Comparative Analysis: ECC vs. RSA Performance

The evaluation of ECC (Elliptic Curve Cryptography) and RSA (Rivest-Shamir-Adleman) algorithms in the comparative analysis highlights ECC's superiority over RSA, primarily due to its efficiency and robustness in handling encryption and decryption operations, particularly in scenarios involving larger file sizes and diverse data formats. The innovative aspect of ECC is its ability to produce smaller key sizes while maintaining security, resulting in faster processing times and lower computational cost as compared to RSA. This efficiency is especially noticeable in higher file sizes and different data formats, where ECC consistently shows quicker encryption and decryption speeds. ECC's use of elliptic curves helps to its efficiency by requiring shorter key lengths, resulting in faster computations and reduced resource use, as opposed to RSA's use of bigger key sizes and slower processing. This research emphasises ECC's speed and computational efficiency advantage over RSA, establishing it as a better solution, particularly in scenarios requiring quick cryptographic operations across different data types and bigger file sizes.

7 Conclusion and Future Work

This study's creation and evaluation of a web application highlight its potential for improving data security by using Elliptic Curve Cryptography (ECC). The programme demonstrates promising potential in providing safe data transmissions and interactions by utilising ECC techniques. The study emphasises the effectiveness and superiority of ECC (Elliptic Curve Cryptography) over RSA (Rivest-Shamir-Adleman) in cryptographic operations, particularly in quicker encryption and decryption times over a wide range of file sizes and data types. The ability of ECC to create reduced key sizes while preserving solid security provides a significant benefit, establishing it as a favoured alternative for quick and fast cryptographic procedures in a variety of circumstances. The decision to use Pretty Good Privacy (PGP) with ECC is consistent with the goal of improving data security. Notably, this study departs from previous efforts that used PGP with RSA+AES, but in this research a unique technique of ECC+AES implemented for novelty, demonstrating the possibility for creative and safe cryptographic procedures inside the application.

7.1 Limitations

Despite the benefits of ECC, this study recognises several limitations. One restriction is the complexity of developing ECC algorithms, which necessitates a deep grasp of elliptic curve mathematics, which may be difficult for certain practitioners. Furthermore, while ECC outperforms in terms of speed and efficiency, its wider use may be hampered by the requirement to convert cryptographic systems and the existing dependence on RSA.

7.2 Future Works

Future upgrades might include the development of ECC-supported modules or libraries inside the web app, as well as the simplification of cryptographic processes for users with less cryptographic understanding. Furthermore, performing user-centric research to evaluate the app's usability, incorporating comments, and improving user experience will increase its efficacy in maintaining safe conversations.

References

- , D. M. G. (2022). A novel encryption system based on pgp using elliptic curve cryptosystem and bézier curve for secure information exchange, (1): 01–5.
URL: https://www.researchgate.net/publication/354748230_A_Novel_Encryption_System_Based_on_PGP_System
- , Hisham Almajed, A. S. A. (2020). A secure and efficient ecc-based scheme for edge computing and internet of things, *Tensorgate Journal of Sustainable Technology and Infrastructure for Developing Countries* .
URL: <https://pubmed.ncbi.nlm.nih.gov/33138018/>
- . 18. Sen, N., D.-R. and Thompson, M. (2020). Performance analysis of secure real-time transport protocol using elliptic curves, *2020 IEEE International Conference on Intelligence and Security Informatics (ISI)* **1**(1): 1–18.
URL: <https://dl.acm.org/doi/abs/10.1109/ISI49825.2020.9280526>
- . 25. Duka, M. (2020). *.Informatyka, Automatyka, Pomiar w Gospodarce i Ochronie Środowiska*, **10**(3), **1**(1): 91–94.
- . Abdelfattah, R.I., T. L. and Attia, M. (2018). An efficient secure electronic mail system based on elliptic curve certificateless signcryption., *. International Journal of Computer Applications*, **975**, p.8887 **1**(1): 26.
- . Biswal, U., P. R.-P. S. and Pattanayak, B. (2022). Aes based end-to-end encryption scheme for secure communication on internet of things (iot), (1): 01–5.
URL: <http://sumc.lt/index.php/se/article/view/708>
- . Chilveri, P. and Nagmode, M. (2022). A novel node authentication protocol connected with ecc for heterogeneous network. *wireless networks*, **1**(1): 26.
URL: <https://www.ijcna.org/Manuscripts/IJCNA-2022-O-63.pd>
- . James, E. and Rabbi, F. (2023). Fortifying the iot landscape: Strategies to counter security risks in connected systems. *tensorgate journal of sustainable technology and infrastructure for developing countries*, **6**(1), pp.32-46., *Tensorgate Journal of Sustainable Technology and Infrastructure for Developing Countries* p. 15.
URL: <https://research.tensorgate.org/index.php/tjstidc/article/view/42>
- . Jian-Foo Lai, S.-H. H. (2022). Secure file storage on cloud using hybrid cryptography, *ournal of Informatics and Web Engineering* **1**(1): 1–18.
URL: <https://journals.mmupress.com/index.php/jiwe/article/view/388>
- . Jothy, K.A., S. K. and Delsey, M. (2018). International journal of engineering sciences research technology enhancing the security of the cloud computing with triple aes, pgp over ssl algorithms, *Softw., Pract. Exper.* (1): 01–82.
URL: <https://zenodo.org/records/1165634>

- . ndriyawati, H., Winarti, T. and Vydia, V. (2021). Web-based document certification system with advanced encryption standard digital signature, *ndonesian Journal of Electrical Engineering and Computer Science* (1): 01–82.
URL: https://www.researchgate.net/publication/350813426Web-based_document_certification_system_with_advanced_encryption_standard_digital_signature
- . Singh, P.K., V. P.-V. A. N. S. and Nandi, S. (2019). Elliptic curve cryptography based mechanism for secure wi-fi connectivity, *In Distributed Computing and Internet Technology: 15th International Conference, ICDCIT 2019, Bhubaneswar, India, January 10–13, 2019* **1**(1): 1–18.
URL: <https://www.jicit.org/paper/154/ED25519-A-NEW-SECURE-COMPATIBLE-ELLIPTIC-CURVE-FOR-MOBILE-WIRELESS-NETWORK-SECURITY>
- . Sudarsono, A. and Al Rasvid, M. (2018). An implementation of data exchange in environmental monitoring using authenticated attribute-based encryption with revocation., *. In 2018 International Electronics Symposium on Knowledge Creation and Intelligent Computing (IES-KCIC)* **1**(1): 26.
URL: <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0258062>
- . Yathiraju, N. (2022). Blockchain based 5g heterogeneous networks using privacy federated learning with internet of things, *Research Journal of Computer Systems and Engineering*, *3*(1) **1**(1): 20.
URL: <https://technicaljournals.org/RJCSE/index.php/journal/article/view/37>
- Kale, N. A. and Darekar, S. A. (2018). Sms for android application by using 3d-aes, pgp and steganography., *JournalNX* pp. 99–104.
URL: <https://www.neliti.com/publications/342506/sms-for-android-application-by-using-3d-aes-pgp-and-steganographycite>
- .Khairunisa, I. and Kabetta, H. (2021). . php source code protection using layout obfuscation and aes-256 encryption algorithm, *In 2021 6th International Workshop on Big Data and Information Security (IWBIS)* (1): 133–138.
URL: <https://api.semanticscholar.org/CorpusID:245540957>
- .Lee, B.-H., Dewi, E. and Wajdi, M. (2018). Data security in cloud computing using aes under heroku cloud, (1): 01–5.
URL: https://www.researchgate.net/publication/350813426Web-based_document_certification_system_with_advanced_encryption_standard_digital_signature