

EXPLORING THE SECURITY OF DATA IN THE CLOUD USING ENCRYPTION

A DISSERTATION

SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR
THE AWARD OF DEGREE
OF
MASTER OF TECHNOLOGY
IN
SOFTWARE ENGINEERING

Submitted by:

HARSH KAMDAR
2K20/SWE/10

Under the supervision of

DR. ABHILASHA SHARMA
(Assistant Professor)



DEPARTMENT OF SOFTWARE ENGINEERING
DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Bawana Road, Delhi-110042

MAY, 2022

DEPARTMENT OF SOFTWARE ENGINEERING

DELHI TECHNOLOGICAL UNIVERSITY

(Formerly Delhi College of Engineering)

Bawana Road, Delhi - 110042

CANDIDATE'S DECLARATION

I, Harsh Kamdar, Roll No. 2K20/SWE/10 student of M. Tech (Software Engineering) hereby declare that the project Dissertation titled "Exploring the Security of Data in the Cloud Using Encryption" which is submitted by me to the Department of Software Engineering, Delhi Technological University, Delhi in partial fulfilment of the requirement for the award of the degree of Master of Technology, is original and not copied from any source without proper citation. This work has not previously formed the basis for the award of and Degree, Diploma Associateship, Fellowship or other similar title or recognition.

Place: Delhi

Date: *May 30, 2022*



HARSH KAMDAR

DEPARTMENT OF SOFTWARE ENGINEERING

DELHI TECHNOLOGICAL UNIVERSITY

(Formerly Delhi College of Engineering)

Bawana Road, Delhi - 110042

CERTIFICATE

I hereby certify that the Project Dissertation titled “**Exploring the Security of Data in the Cloud Using Encryption**” which is submitted by Harsh Kamdar, 2K20/SWE/10 Department of Software Engineering, Delhi Technological University, Delhi in partial fulfilment of the requirement for the award of the degree of Master of Technology, is a record of the project work carried out by the student under my supervision. To the best of my knowledge, this work has not been submitted in part or full for any Degree or Diploma to this University or elsewhere.



Place: Delhi

Date: *May 30, 2022*

DR. ABHILASHA SHARMA

SUPERVISOR

Assistant Professor,

Department of Software Engineering,

Delhi Technological University

(Formerly Delhi College of Engineering)

Bawana Road, Delhi - 110042

ACKNOWLEDGMENT

The success of this project requires the assistance and input of numerous people and the organisation. I am grateful to everyone who helped in shaping the result of the project.

I express my sincere thanks to **Dr. Abhilasha Sharma**, my project guide, for providing me with the opportunity to undertake this project under her guidance. Her constant support and encouragement have made me realise that it is the process of learning which weighs more than the end result. I am highly indebted to the panel faculties during all the progress evaluations for their guidance, constant supervision and for motivating me to complete my work. They helped me throughout with new ideas, provided information necessary and pushed me to complete the work.

I also thank all my fellow students and my family for their continued support.



HARSH KAMDAR

ABSTRACT

The rise of cloud computing over the past few years has resulted in a growing interest among a variety of consumers, businesses, and institutions in taking use of the cloud's various services and applications. The cloud has captured a significant amount of attention from the academic community, the information technology sector, and government agencies due to the fact that it offers a very appealing package of services. Computing in the cloud offers the promise of scalability as well as the availability of resources on demand. As the number of users who access the internet continues to rise on a daily basis, and as the number of attackers follows a similar trajectory, it has become absolutely essential to provide an effective security mechanism for cloud computing in order to ensure the safety of the vast numbers of user requests that are processed on it. Strong security measures in cloud computing systems are, as a result, one of the most critical concerns that researchers need to give significant emphasis to. In an effort to find a solution to this issue, a variety of researchers have proposed a number of different cryptography methods.

The use of cloud computing opens up a vast number of doors while also presenting a number of obstacles. The cloud is facing an increasingly difficult problem in terms of security as its capabilities continue to expand. Can users put their full faith in the cloud? Is it safe to save their data in the cloud? Although it is challenging to provide accurate answers to these questions, encrypting the data on the client side can unquestionably serve as an additional layer of safety. In this study, the AES-GCM algorithm was utilized to accomplish the same goal.

CONTENTS

CANDIDATE’S DECLARATION	i
CERTIFICATE	ii
ACKNOWLEDGEMENT	iii
ABSTRACT	iv
CONTENTS	v
LIST OF FIGURE(S)	vii
LIST OF TABLE(S)	viii
LIST OF ABBREVIATION(S)	ix
CHAPTER 1 INTRODUCTION	1
1.1 Overview	1
1.2 Motivation	2
1.3 Objectives	2
1.4 Problem Statement	3
CHAPTER 2 BACKGROUND	4
2.1 Cloud Computing	4
2.2 Cryptography	5
2.2.1 Components of Cryptosystem	6
2.3 Encryption	7
2.3.1 Types of Encryptions	8
2.3.2 Symmetric Encryption	8
2.3.3 Asymmetric Encryption	9
2.3.4 Hashing	10
2.3.5 Need for Encryption	10
2.4 Encryption Algorithms	11
CHAPTER 3 LITERATURE REVIEW	13
CHAPTER 4 TECHNIQUES USED	24
4.1 Client-side Encryption	24

4.2	AES with Galois/Counter Mode (AES-GCM)	25
CHAPTER 5 EXPERIMENTAL SETUP		29
5.1	Programming Tools and Software Used	29
5.2	System Specification	30
5.3	Dataset Used	31
5.4	Output	31
CHAPTER 6 RESULT AND ANALYSIS		33
6.1	Time Analysis for Encryption	33
6.2	Time Analysis for Decryption	34
CHAPTER 7 CONCLUSION AND FUTURE WORK		36
7.1	Conclusion	36
7.2	Future Work	36
REFERENCES		38

LIST OF FIGURE(S)

Figure 2.1 The Computing Using Cloud	4
Figure 2.2 Various Components of Cryptosystem	6
Figure 2.3 Various Types of Cryptography	7
Figure 2.4 The Basic Process of Encryption	8
Figure 2.5 The Basic Process of Symmetric Encryption	9
Figure 2.6 The Basic Process of Asymmetric Encryption	9
Figure 2.7 The Basic Process of Hashing	10
Figure 4.1 Process of Client-side Encryption and Client-side Decryption	25
Figure 4.2 The Process of Authenticated Encryption.	27
Figure 4.3 The Operation of Authenticated Encryption.	28
Figure 5.1 The parameters of Function for AES	30
Figure 5.2 File before encryption	31
Figure 5.3 The Output after the Encryption Function Invoked	32
Figure 5.4 The Encrypted File created in the Folder	32
Figure 5.5 The Output After the Decryption Function Invoked	33
Figure 5.6 Figure 5.6 The File After the Decryption	33
Figure 6.1 Graph of File Size vs Time Taken for the Process of Encryption	35
Figure 6.2 Graph of File Size vs Time Taken for the Process of Decryption	36

LIST OF TABLE(S)

Table 2.1 A Summary of the Popular Algorithms Used for Encryption	12
Table 6.1 Summary of Time Taken to Encrypt Files of Various Sizes	34
Table 6.2 Summary of Time Taken to Decrypt Files of Various Sizes	35

LIST OF ABBREVIATION(S)

1. ISP : Internet Service Provider(s)
2. CSP : Cloud Service Provider(s)
3. IS : Internet Security
4. API : Application Programming Interface
5. AES : Advanced Encryption Standard
6. DES : Data Encryption Standard
7. RSA : Rivest-Shamir-Adleman
8. AAD : Additional Authenticated Data
9. IDLE : Integrated Development and Learning Environment
10. CSE : Client-Side Encryption

CHAPTER 1

INTRODUCTION

This chapter gives an overview of the study carried out. It also specifies the motivation and objective for undertaking this study. Also, the problem statement has been given.

1.1 OVERVIEW

Cloud computing is an emerging dominant technology in the Information and Communications Technology (ICT) era that will provide stakeholders with economical high-speed computing and data storage capabilities. It assures stakeholders that new technologies like the Internet of Everything (IoE) and powerful mobile technologies would make their daily lives smarter.

Customers are outsourcing more and more of their data to cloud storage servers as a result of the multiple benefits that come with rapid technological advancements. Therefore, the data owner transfers the data to a third-party cloud storage server that will store the data and return it to the user upon request. With an enormous amount of data being generated every second, it becomes challenging for a small business to routinely scale up its storage hardware as new data are produced. With storage maintenance becoming increasingly complex, outsourcing data to the cloud enables small businesses to decrease costs associated with maintenance, storage, and human resources. In cloud servers, additional backups are offered for the safe storage of data, hence reducing issues caused by hardware breakdowns.

Despite its numerous benefits, cloud-based data storage raises numerous security risks that must be thoroughly analyzed in order to arrive at a viable solution and avoid the issue of local data storage.

The requirement for data security in cloud computing is becoming increasingly pressing as IT organizations migrate. Daily cloud computing is thriving, but it also confronts dozens of new security challenges. Cloud computing is rapidly being utilized to store secret information

in the health care, IT field, NGOs, and the government sector. Encryption is used to safeguard confidential information from unauthorized access.

1.2 MOTIVATION

Cloud computing has several opportunities as well as drawbacks. Cybersecurity has become a big concern for the cloud as its capabilities have grown. Can people entirely trust the cloud? Is their information safe in the cloud? These are valid concerns that have yet to be addressed. Cloud computing has proven increasingly appealing to cyber criminals. Internal and external threats to cloud security include malicious insiders, software faults, harmful programs, and administrator errors.

Cloud computing's road to success is said to be hampered by security concerns. Cloud computing poses a variety of security challenges.

Cloud storage raises two significant concerns: safety and reliability. Clients are unwilling to hand up their data to a third party unless they are assured that they will be able to retrieve it whenever they want and that no one will have access to it.

Businesses migrating to the cloud from a traditional on-premises environment are concerned about cloud security. To gain the trust of cloud users, the CSP must provide greater information security measures. With the constant evolution of cloud technology, the encryption techniques linked with it should continue to improve.

1.3 OBJECTIVES

The work has been conducted while keeping the following objectives in mind:

- The vital role that encryption plays in ensuring the security of data stored in cloud environments.
- To implement client-side encryption as an additional security measure.
- To examine the time required to encrypt and decrypt files of different sizes.

1.4 PROBLEM STATEMENT

Considering cloud computing is a web-based service, a variety of concerns have been highlighted, including unauthorized access, user privacy, data theft, and data leaking. The security of the user's data is the primary responsibility of cloud service providers. Therefore, for successful data security, we require a system that provides both data encryption and secure protection against data theft. Researchers have developed a number of data security measures for cloud environments.

Encryption is frequently presented as the solution to cloud-based confidentiality issues. When a cloud service maintains data in an encrypted format, it is crucial to determine if the middleman or the CSP is accountable for overseeing the encryption-keys. It is important to note that if the CSP has access to the encryption keys or administers them, they will be able to view and decrypt data stored at the provider's location. Client-side encryption consequently plays a critical part here.

Interception of data while it is in transit is always a possibility whenever sensitive information is sent via a network. This is especially true in situations when the network is not operated or controlled by the organization, such as the case with the Internet. Organization/User must verify that all sensitive data in transit, including login credentials, is encrypted using only globally acknowledged encryption techniques and algorithms.

The risk that employees of the cloud service provider will get unauthorized access to sensitive information or commit data theft is a significant worry for businesses that want to adopt cloud services.

“Design a mechanism to enhance the security of cloud data by implementing client-side encryption using an efficient encryption technique.”

CHAPTER 2

BACKGROUND

In this chapter, the theories that need to be known in order to comprehend the approach (client-side encryption) that has been utilized in the study that is being considered are provided.

2.1 CLOUD COMPUTING

The term "cloud" refers to a type of computing technology that is based on the Internet and in which shared resources including software, platforms, storage, and information are made available to clients on demand.

The term "cloud computing" refers to a computing platform that allows for the sharing of resources, such as software, infrastructures, applications, and business processes. Cloud computing refers to an online shared database of computer resources. It does this by making the pool's computing resources available to users over the internet. The new paradigm of computing known as cloud computing promises to openly distribute data storage, processing power, and service offerings across vast numbers of users.

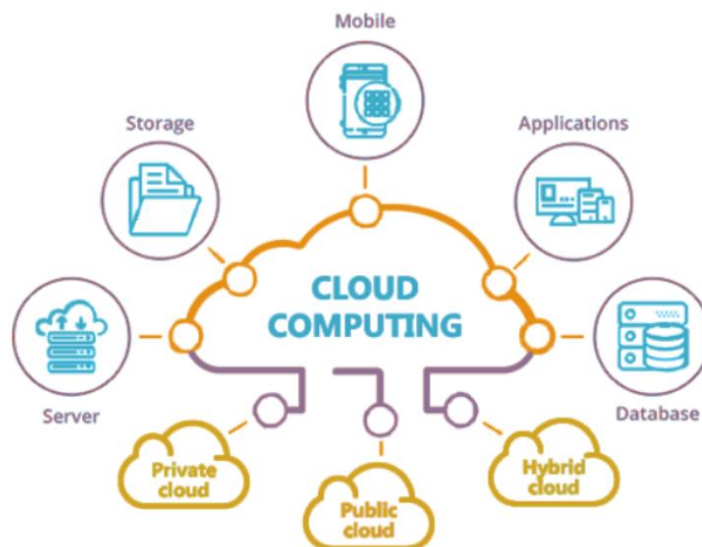


Figure 2.1 The Computing Using Cloud [1]

Some of the security issues in a cloud environment:

- Vulnerabilities in Shared Technology
- Data Breach or Loss
- Unsecure API(s)
- Malicious Insiders
- Service, Account, and Traffic Hijacking

Current cloud computing solutions have significant limitations when it comes to ensuring the privacy of user data. Since sensitive user data is supplied in an unencrypted format to remote machines owned and run by third-party service providers, the danger of unauthorized disclosure by service providers is rather significant. There are numerous methods for securing user data from external attackers. Encryption is an example.

2.2 CRYPTOGRAPHY

Based on the mathematical theory, cryptography is a computer science approach for safeguarding data. Cryptography is a combination of three terms:

Cryptography is a combination of three terms:

- Cryptography
- Cryptology
- Cryptanalysis

Frequently, the three names are used interchangeably. Cryptology is the study of communication across unsecured channels and the associated security issues. The design of an entire cryptosystem is known as cryptography. Cryptanalysis is the breaking of a cryptosystem.

2.2.1 Components of Cryptosystem

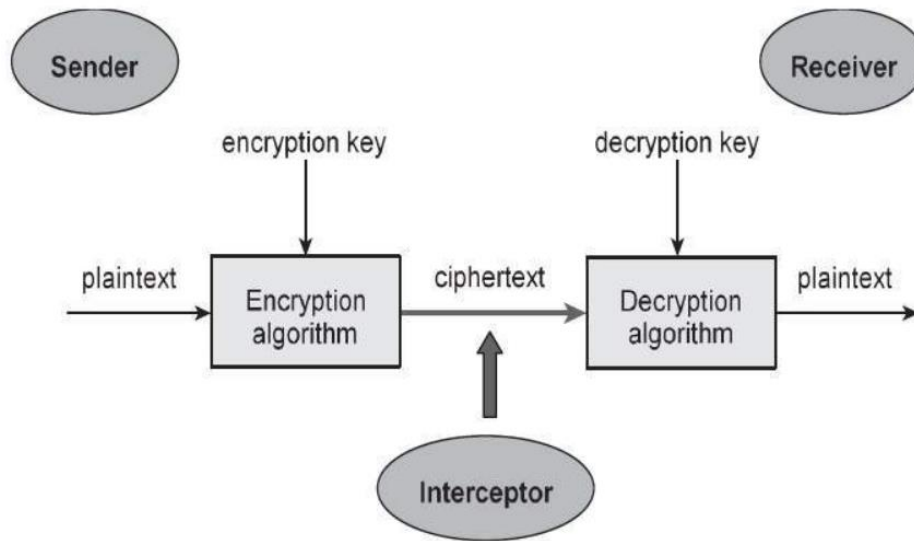


Figure 2.2 Various Components of Cryptosystem [2]

Plaintext: This represents the data that is being safeguarded during transmission.

Encryption algorithm: The mathematical procedure for generating a ciphertext from plaintext and an encryption key. To generate a ciphertext, this cryptographic procedure combines plaintext with an encryption key.

Ciphertext: Ciphertext is a scrambled form of plaintext generated by an encryption algorithm with a specified encryption key. It permits interceptions by anyone with access to the communication channel.

Decryption algorithm: The mathematical procedure that yields a distinct plaintext for any given ciphertext and decryption key. It is a cryptographic method whose inputs are ciphertext and a decryption key, and whose output is plaintext.

Encryption key: It is the value known by the sender. To compute the ciphertext, they feed the encryption key along with the plaintext into the encryption algorithm.

Decryption key: It is value known by the recipient. They compute the plaintext by feeding the decryption key and the ciphertext into the decryption algorithm.

Interceptor: An interceptor is a third party who attempts to deduce the plaintext. He or she can view the ciphertext and may even be aware of the decryption algorithm, but never the decryption key.

Cryptography is classified into three types. They are conversion methods, key-based conversion methods, and process-based conversion methods. The plaintext is turned into ciphertext in three ways in the conversion method: substitution, transposition, and concealment. The symmetric and asymmetric keys are used to encrypt and decrypt plaintext in the key-based approach. Plain text is treated using block and stream ciphers in the process-based technique.

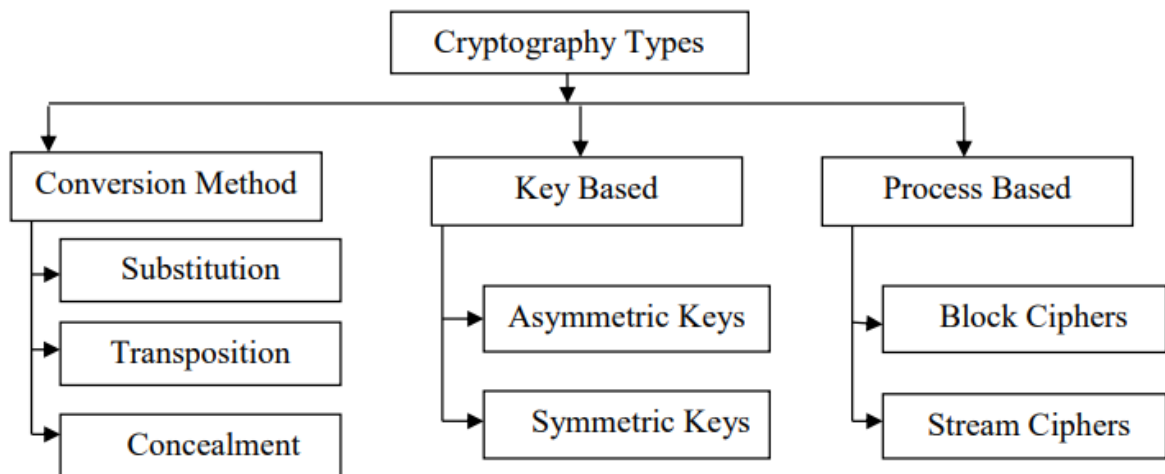


Figure 2.3 Various Types of Cryptography [3]

2.3 ENCRYPTION

Encryption scrambles data in order that only legal entities may interpret it. It takes readable records and makes it seem random. Encryption necessitates the employment of a cryptographic key, which is a set of mathematical values agreed upon by the sender and recipient of an encrypted message.



Figure 2.4 The Basic Process of Encryption [4]

Though encrypted data appears to be randomized, encryption proceeds in a systematic, predictable way, letting an entity that gets the encrypted data and has the correct key to decrypt the data, converting it back to original form. Super secure encrypting will use keys that are complicated so much that a third party will be extremely improbable to decrypt or crack the encrypted data using brute force — that is, guessing the key.

Data can be encrypted "in transit," while it is being transmitted somewhere else, "at rest," when it is stored, or "in use," when it is being processed.

A key in cryptography is a set of characters that is used in an encryption method to make data appear random. It conceals (encrypts) data in the same way that a physical key does, allowing only those with the correct key to open (decrypt) it.

2.3.1 Types of Encryptions

There are various data encryption methods to select from. Most Internet Security (IS) experts divide encryption into three types: symmetric, asymmetric, and hashing. These are further subdivided into many categories.

2.3.2 Symmetric Encryption

This method, sometimes known as private-key cryptography or a secret key algorithm, necessitates the sender and receiver sharing the same key. Therefore, the recipient must possess the key before the communication can be decrypted. This strategy is most effective for closed systems, which are less susceptible to invasion by a third party.

Positively, symmetric encryption is more fast than asymmetric encryption. Negatively, both parties must ensure that the key is safely held and accessible only to the intended entity.



Figure 2.5 The Basic Process of Symmetric Encryption [5]

2.3.3 Asymmetric Encryption

This method, which is also known as public cryptography, encrypts data using two mathematically related keys: a public and a private key. One key is used for encryption, while the other is used for decryption.

As its name suggests, the public key is accessible to anybody, whereas the private key is restricted to the intended receivers, who require it to decrypt the messages. Both keys consist of enormous numbers that are not identical but are coupled with one another, hence the term "asymmetric."



Figure 2.6 The Basic Process of Asymmetric Encryption [6]

2.3.4 Hashing

Hashing creates a unique, fixed-length signature for a data or a message. Every message has its own unique hash, making it easy to track even minute changes to the data. Hash-encrypted data cannot be reversed or decrypted. Therefore, hashing is only utilized for data verification.

Even while many people who specialize in internet security don't even believe hashing to be a true encryption method, the border between the two is fuzzy enough that we may continue to call it that. In conclusion, it is an effective strategy to demonstrate that the data has not been altered.



Figure 2.7 The Basic Process of Hashing [7]

2.3.5 Need for Encryption

- Encryption protects one's privacy by ensuring that only the intended recipient or the legitimate owner of the material may read communications or data that is at rest. This prevents data from being intercepted and read by advertising networks, attackers, ISP(s), and, in some situations, governments.
- Encryption prevents data breaches regardless of whether the data is in transit or at rest. If a business device's hard disk is correctly encrypted and it is lost or stolen, the data residing on that device will remain secure. In the similar way, encrypted communications allow the communicating parties to share sensitive information without the information being leaked.
- Encryption also helps against hostile behavior such as on-path attacks, which can compromise data integrity. Together, encryption and other safeguards for data integrity make sure that data sent across the Internet has not been changed.

- Among other things, encryption with the public key can be used to prove that the owner of a website has the private key mentioned in the website's TLS certificate. This makes sure that website visitors are redirected to the legitimate website.
- Several government standards and industry require organizations that manage user data to keep such data encrypted for all of these reasons. PCI-DSS, HIPAA, and the GDPR are instances of regulatory and compliance standards that necessitate encryption.

2.4 ENCRYPTION ALGORITHMS

Today, there are a variety of encryption methods to choose from. Below are some of the most popular.

Advanced Encryption Standard (AES): The AES is a well-known encryption technique that uses 192 and 256-bit keys for some very demanding encryption needs, despite being incredibly efficient in 128-bit version. Except for brute force, AES is widely thought to be resistant to all attacks. Regardless, many internet security experts predict that AES will become the de facto standard for encrypting data in the private sector in the near future.

Triple Data Encryption Standard (Triple DES): Triple DES is the successor of the Data Encryption Standard (DES) algorithm, which was developed in response to attackers who cracked DES. Symmetric encryption was previously the most popular symmetric technique in the industry, but it is rapidly being phased out. Triple DES applies the DES algorithm three times to each data block and is often used to encrypt UNIX passwords and ATM PINs.

Blowfish: Another algorithm meant to replace DES is Blowfish. This symmetric technique divides messages into 64-bit chunks and encrypts each block separately. Blowfish have earned a reputation for their speed, adaptability, and indestructibility. It is in the public domain; thus, it is free, which increases its appeal. Blowfish is often used to secure e-commerce platforms and password management applications.

Twofish: Twofish is the successor to Blowfish. 128-bit data blocks are deciphered using license-free, symmetric encryption. Furthermore, regardless of the size of the key, Twofish

always encrypts data in 16 rounds. Twofish is ideal for both software and hardware contexts and is among the quickest of its kind. This strategy is utilized by the majority of modern file and folder encryption software solutions.

Rivest-Shamir-Adleman (RSA): RSA is an asymmetric encryption method that operates by factoring the product of two big prime numbers. Only a person who knows these two numbers can effectively decode the message. RSA is often used for digital signatures, but when encrypting huge amounts of data, the method slows down.

Table 2.1 A Summary of the Popular Algorithms Used for Encryption

Encryption Algorithms	Year	Length of Key	Cipher Type
AES	2000	128, 192, 256	Symmetric block
Triple DES	1978	168	Symmetric block
Blowfish	1993	32-448	Symmetric block
Twofish	1998	128, 192, 256	Symmetric block
RSA	1977	1024-4096	Asymmetric

CHAPTER 3

LITERATURE REVIEW

This review of the literature is a good basis for future work on this project. It will also tell us about all the other research that has been done on this area of study.

1. Cloud computing is a dynamic technology that has received a lot of attention in recent years. Providers and customers must ensure that the cloud is protected from all internal and external hazards, as well as a shared understanding between customer and provider regarding cloud security. One of the most pressing concerns in the computer cloud is data security, which encompasses a wide range of issues such as confidentiality, integrity, surveillance, trust, availability, security, anonymity, communication power, government, and backup copy and assistance. However, the most important aspect of data security is the security and privacy of data stored in cloud storage. The importance of data security in the cloud is explored in this study by Hemalatha, N., et al. This study compares and contrasts the various encryption algorithms used in the cloud. [8]
2. Data security has risen to the top of the top computer security list. Because data and information should not be leaked to a third party user, effective security measures should be used. This paper by Saranya, R. Gowthami, and A. Kousalya provides an overview of several cloud protection algorithms that use cryptographic techniques. Different algorithms use different protections, but they are all vulnerable to certain conditions. As a result, no single security algorithm can be trusted. As a result, we argue that in cloud-based systems, the security of multiple levels is critical to data security at each level. [9]
3. Cloud computing is a flexible, inexpensive, and well-proven business platform for customer service and online services. Cloud computing allows distributed computation, multi-user-friendly properties and multiple domain infrastructure for administrative purposes. As a result, it is highly vulnerable to security threats, danger. Cloud security is currently a major problem. Its acceptance is directed at its safety, confidentiality, and security. Cloud service companies are concerned about privacy issues. They are in charge

of handling the services. Usually, the service provider needs to ensure that they provide secure infrastructure, as well as their customer data and information remains secure. By establishing safety policies and procedures, applications can be made safer. Methods reliability, ownership management, software sharing, data protection, availability, data repository, data handling and modification, multi-platform support, and intellectual property amid security concerns In this study by Sugumaran, M., B. Bala Murugan, and D. Kamalraj, some of the strategies used to protect the data are discussed, as well as the proposed data protection framework in the cloud. This structure is designed to store data in the cloud in encrypted form using block cipher cryptography technology. [10]

4. Cloud computing is a new, next-generation technology in the rapidly evolving world of knowledge technology. It offers a variety of benefits, but there are still some problems with this technology. The most difficult challenge with this technology is security. In this study by Islam, N. K. V., and M. K. V. Riyas explored a number of encryption techniques to overcome this security problem, as well as the advantages and disadvantages of these algorithms. They came to the conclusion that a homomorphic algorithm is the best way to capture important data in a cloud computing space. Because homomorphic algorithms may work on encrypted data, they are much more secure than other algorithms such as RSA, DES, and AES. Future work will focus on using hardware or software techniques that use a homomorphic approach to protect cloud users from any type of security attack. [11]

5. Despite the many benefits of cloud storage, there are still many security issues that need to be addressed. Cloud storage solutions for large and small businesses will be the future if we can eliminate or handle this security error. Kartit, Zaid, et al have developed a system for this study that allows data to be stored in the cloud. Using our algorithm ensures data security. Data can only be accessed by an authorized user. Even if a criminal (unauthorized user) receives data accidentally or intentionally, we will not be able to delete it without two keys from two different locations. They focused on the many potential alternatives in this area as well, especially in homomorphic encryption. [12]

6. It is known that since the advent of the internet, people all over the world have relied heavily on it. People also use the cloud to store large amounts of data. Researchers are faced with the daunting task of protecting user privacy and sensitive data so that unauthorized people can access and modify it. Cryptography is the process of transforming a user's useful information into a useless form for unauthorized persons, allowing only authorized people to access and understand it. There are several cryptographic algorithms for privacy verification, selected based on user requirements or organizational security specifications. This study by Semwal, Pradeep, and Mahesh Kumar Sharma. Compares various encryption algorithms based on their many key features and evaluates their operating costs according to a few key conditions. DES, 3DES, IDEA, CAST128, AES, Blowfish, RSA, ABE, and ECC are some of the algorithms used. [13]

7. Data security on cloud computing is discussed in this study by Albugmi, Ahmed, et al. It is a study of data in the clouds and the security issues that come with it. The paper will go through some details of data protection measures and procedures used worldwide to provide high data security by reducing risks and threats. Cloud data acquisition is useful for many applications, but it also raises concerns about disclosing data to operating systems that may already have security errors. Similarly, using cloud computing virtualization may place data at risk if a guest OS is used over a hypervisor without knowing the OS visitor's reliability, which may include security error. In addition, the article discusses Data-in data security issues. - Transport and Data - At rest. The research is based on all levels of SaaS (Software as a Service), PaaS (Platform as a Service), and IaaS (Infrastructure as a Service) (Infrastructure as a Service). The increase in cloud computing usage undoubtedly accelerates the process of better cloud data storage systems. If the data stored in the cloud is not properly protected, it could be compromised. Risks and threats to data security in the cloud were explored in this study, as well as a review of three categories of security concerns. Virtualization is being investigated to determine the risk posed by the hypervisor. Threats brought by the public cloud and multidisciplinary action have also been addressed. Data security, as well as its challenges and solutions to the cloud computing, was one of the main topics of paper. Data for

various regions has been tested, as well as effective cloud encryption methods. The study looked at block cyphers, stream cyphers, and hash functions, all of which are used to encrypt data in the cloud, whether resting or on the move. [14]

8. Cloud Computing is becoming increasingly popular, and sharing technology with Grid Computing, Utility Computing, and Distributed Computing. Users can build applications in the cloud and access them anywhere using cloud service providers such as Amazon IBM, Google Application, Microsoft Azure, and others. Cloud data is stored and accessible from a remote server using the services of cloud service providers. Because data is transmitted via a remote server, security is a major issue (the Internet). Security concerns need to be addressed before cloud Computing can be used commercially. In this paper Rao, R. Velumadhava, and K. Selvamani discuss data security concerns in the cloud-based environment, as well as ways to overcome them. In this paper, data security issues, as well as solutions to these challenges, are discussed, to reduce the risks associated with cloud computing. Computer security standards for concrete clouds can be defined in the future. Advanced encryption methods for storing and retrieving data from the cloud can be used to enable secure data access. Appropriate key management methods can also be used to distribute the key to cloud users, ensuring that only authorized people have access to the information. [15]
9. There are a number of critical policy issues in cloud computing technology, including privacy, security, anonymity, communication power, government surveillance, trust, and legal liability, to name a few. Most important to them is security, and how the cloud provider guarantees. In general, cloud computing has a wide range of clients, including everyday users, professionals, and businesses, all with different reasons for moving to the cloud. If cloud clients are professional, security influences computer performance, and cloud providers must develop a way to balance their security and performance. For businesses, the most pressing issue is still security, but with a different perspective. High performance may not be as important to them as it is to studies. Cipher Cloud is a platform that allows users to keep their data private while using public cloud services. To achieve this, Cipher Cloud uses a two-step encryption method that ensures that any data

transmitted from the client to the cloud server or vice versa is fully protected and secure. The strongest security controls needed to protect the most sensitive data may not occur on computer cloud computing systems, but may be possible in confidential cloud computing systems. This study by Kaur, Manpreet, and Rajbir Singh proposes selected encryption methods as the most promising cloud computing strategy, which truly ensures the confidentiality of data, such as cloud computing models. [16]

10. Due to the proliferation of mobile devices and cloud computing, data storage (such as photos, recordings, messages, and texts) in the cloud has become the norm among individual and class clients. However, cloud service providers may not be completely reliable in order to ensure the integrity and accessibility of client and reused / transferred data to the cloud. As a result, a new security model, as well as a selection of the right keys, is provided to improve the online security level of cloud data. In the proposed study, Hussaini, Sheena first used the K-Mediod integration method, which is based on the data range, to compile the confidential information we collected. Combined data is then encrypted and stored in the cloud using Blowfish Encryption (BE). Saving and securing confidential information in the cloud is a major issue for cyber data security. They have developed an effective cloud storage framework based on privacy in this study that improves processing speed while ensuring privacy and reliability through data integration. The BE algorithm is used to improve online security, with a metaheuristic algorithm that selects the best key. Compared to blowfish, RSA, and AES, the recommended blowfish encryption solution achieves the highest level of online security in cloud storage by achieving instant key break time. Compared to existing techniques, simulation results show that the proposed blowfish algorithm enhances online security accuracy on all confidential information while requiring minimal encryption, encryption, and duration. [17]

11. A new curve in the line of information technology and computer paradigm cloud computing. Cloud computing has transformed corporate and government sectors simultaneously by reaching out to all parties not only in the field of information and communication technology, but also in the field of new technologies in the very different

agricultural sector that was not affected by technological advances. An internet computer, which is predicted to grow faster than mobile computing. IoT, or Internet of Things, is a term used to describe the internet of things. As more and more measures are added to the equation, every day, hackers and intruders have a gateway into the cloud of access threats Security is fueled by cloud computing, which brings new threats, new types of problems. Data security is one of the major problem areas highlighted, and user data security is of paramount importance. The cloud service provider is responsible for ensuring the privacy of the user and the data they store. This study by Mishra, Nishit, et al. focuses on a cloud computing security model that uses cryptography to protect data security and the integrity of user data stored in the cloud. [18]

12. Cloud computing is a concept used to solve everyday computer problems. Cloud computing is a collection of visual resources that are made available to consumers online. Cloud computing is an Internet-based computer technology development. The most common problems with cloud computing include data privacy, security, anonymity, and trust, among others. Most important to them is security, and how the cloud provider guarantees. Cloud protection includes medical protection (statistics) and storage (websites hosted by the Cloud provider). In this project, Khan, Shakeeba S., and R. R. Tuteja explore various cloud security challenges and various cryptographic strategies that can be used to improve cloud security. Cloud computing is a relatively new concept, and many firms are trying to migrate to the cloud but are unable to do so in security issues. As a result, cloud security is important, as it will remove barriers to business cloud acceptance. There are many security algorithms that can be used in the cloud. Other symmetric algorithms include DES, Triple-DES, AES, and Blowfish. Symmetric algorithms are widely used by DES and AES. AES is much harder to use than DES. Asymmetric algorithms are RSA and Diffie-Hellman Key Exchange. Currently, these security measures are used in the context of cloud computing. [19]

13. Cloud computing is a concept used to solve everyday computer problems. Cloud computing is a collection of visual resources that are made available to consumers online. Cloud computing is an Internet-based computer technology development. The most

common problems with cloud computing include data privacy, security, anonymity, and trust, among others. Most important to them is security, and how the cloud provider guarantees. The work plan recommended for this study was done by Kaur, Mandeep, and Manis Mahajan. reduce concerns about data privacy by using encryption methods to improve cloud security from the perspective of various cloud clients. The three ideas connected to the cloud computing paradigm in the form of size were discarded during the book review. This size depends on how the data is used, where it is stored in relation to the data owner, and how the data is protected. Cipher Cloud encrypts data, ensuring that it remains in the hands of its owner, regardless of where the data is stored or who controls it. Even in the event of a refund or change of ownership, only the user will be able to decrypt the data. In addition, the data is protected during transmission using the HTTPS TLS 1.0 standard, making it difficult for anyone to inhale. [20]

14. Information and communication protection systems that use mathematical understanding to convert messages into complex formats. Cryptography, like cryptanalysis, is closely related to the cryptology department. Strategies include combining caption words, dots, and other ways to hide data during storage or transit. Cryptography, on the other hand, is often connected to cloud computing in the modern era. Moving data to the cloud, on the other hand, is a significant change in participation that causes customers to expire before enrolling in the desired service, which may result in unnecessary orders for sensitive information and data loss. Musa, Abu, and Ashiq Mahmood have developed and enforced symmetric key encryption in our research work, which encrypts the file locally before uploading to the cloud and removes the file encryption after downloading to the client side using a key generated during encryption. Key values are also calculated using a different algorithm in this algorithm. As a result, for large files, our system provides greater security and efficiency. In this way, we may add an extra layer of security, preventing unwanted attacks on personal data and a lack of similarity. [21]

15. The amount of sensitive data to be stored, as well as the number of risks in this data, has grown in line with the development of computer systems, making data retention more important for computer users. With devices that are always connected to the Internet,

cloud data storage services are now operational and widespread, providing quick access to such data from anywhere. Such operation poses a challenge, namely the confidentiality of data sent to other parties for maintenance. Disk encryption solutions have received a lot of attention from home users, as they are used on personal computers and also have native options in other smartphone applications. In encryption, the current study done by da Rocha, Marciano, et al. used the technological power of Intel Software Guard Extensions (Intel SGX) to seal. The real reality is file system is built where applications can store their data while maintaining the security guarantees provided by the operating system. Before sending data to a storage provider, Intel SGX technology is used. This way, even if the storage provider is unreliable, you will still be able to access your data. The data was not interrupted. Cryptomator software, which is a free cryptography program on the client side, was used to validate the proposal. The Intel SGX (enclave) data encryption system was connected to the cloud encryption tool. The results show that the system is operational and secure, and that it can be upgraded and configured to make it easier to use and connect to cloud-based synchronization services. [22]

16. Cloud computing has emerged as the latest component of computer technology, which offers a variety of benefits to many organizations with a variety of business models at low cost. When you upload sensitive data to a cloud server, however, there is always a security problem. Client on the client side is a common and effective way to assure end users that the data they upload will not be accessible to a third party. Different techniques are used by cloud service providers to protect data, but most of them, like Google Drive, do not use encryption on the client side. In this study, Islam, Md Mahidul recommends using a combination of Advanced Encryption Level and Secure Hash Algorithm with First Vector to protect data from hacking or loss when storing or uploading data to a cloud server. Cloud computing has become a popular tool in the digital age, yet there are many security concerns. Many researchers are trying to solve the security risk. Our proposed approach will be effective in the context of data security in this study. We have provided a secure encryption method for the client side, which will keep the data safe when uploaded to the cloud. [23]

17. Client-side encryption (CSE) is important in ensuring that information stored on public cloud services is accessible only to targeted users. CSE, on the other hand, makes file synchronization methods such as deduplication and delta codecs extremely difficult, which is necessary to reduce the high bandwidth capabilities associated with cloud storage services. In this study, Henziger, Eric, and Niklas Carlsson provide a comprehensive analysis that includes robust evaluations using four popular CSE resources (CSEs) and four popular non-CSEs to assess high CSE-related fees. Compared to non-CSEs, our findings suggest that existing CSEs can integrate CSE with bandwidth savings features such as compression and reduction with additional costs. Well, they do. Delta encoding uses fewer CSEs than non-CSEs, and the difference in bandwidth saving between applications that use delta codecs may be significant. [24]

18. Souza, Stefano MPC, and Ricardo S. Puttini in their paper describes that when it comes to providing sensitive data to the cloud, there are a few issues to consider. The escrow data for health and financial records, for example, is subject to strict regulatory limits. End users and authorities need reassurance to organizations that limited data will never be accessed by an outside company. For books, encryption on the client side is a common solution. Most studies, on the other hand, fail to consider the impact of safety solutions on performance and use. Such negative effects can be minimized with homomorphic encryption and configuration systems, which allow for regular searches for cloud-encrypted records while maintaining the confidentiality and privacy of the end user. Given the natural risks of cloud services and the existence of unique application cases, such as those mentioned above, where the only way to decompress computing is to encrypt all data in advance, it is possible to conclude that cloud security is likely to include related. future strategies. As a result, there is still a clear need for the development, testing, and comprehensive use of simple and effective homomorphic cryptographic primitives, as well as the development of open and free software projects that include carefully selected libraries for cryptographic works found in the archives. OpenSSL, GnuCrypto, BouncyCastle, and LibTomCrypt, to name a few, have had a significant impact on the distribution and use of cryptographic primitives on a daily computer. information taps, APIs, and frameworks such as Mylar can close the gap,

provide strong cryptographic features to regular programmers and improve the quality of the overall software. This will make a significant contribution to the development of security and privacy in the cloud computing. [25]

19. Cloud computing is now the most widely used network in the world. Cloud computing allows end users to share resources and store data online. There are many security risks with existing cloud computing platforms. As a result, security becomes an integral part of the data stored in the cloud. We have provided this paper as a solution to this problem. This work by Surv, Niteen, et al. describes the AES encryption method based on client-based encryption on the AES side and the encryption method. AES encryption and decryption are the safest and fastest way to encrypt and decrypt data encryption. Client-side encryption on the client side is an excellent way to ensure data security during transfer and storage. On a cloud computing, this study raised user authentication to protect data encryption algorithms. They introduced a data-protected method in this study to address the issue of data security and privacy on cloud computing. The client can provide higher data security with this paper than the existing system. Ensuring the privacy and security of data transmitted and stored in the cloud. Using a single secret key, define the client-side encryption method and how to remove encryption. Next, in this study, we looked at the AES encryption and decryption protocol to protect cloud customer data and ensure data privacy. [26]

20. In recent times, there has been an increasing interest in the efficient use of computer resources so that large amounts of data can be processed at a lower cost. The need for a set of shared resources in a broader network that provides flexibility, large computational capacity, and the ability to store data locally has led to the development of cloud computing. As a result, encryption of important data is necessary and highly recommended. In an unreliable environment like public cloud, server-side encryption is very dangerous. Encryption on the client side, on the other hand, may undermine the benefits of the cloud because encryption and decryption take time. Rahmani, Hossein, et al. have created a private cloud as a central point to handle this issue. In this study, they

propose Encryption As a Service based on XaaS vision to eliminate the security risks of cloud provider encryption and the ineffectiveness of client-side encryption. [27]

21. The quick growth of cloud computing as a new technology and many subtle security issues poses many challenges. These challenges are specified in the service provider's cloud servers and transfer processes. Ideally, this paper introduces a different data-based model with cloud key servers and a client-based data encryption service to increase reliability in cloud computing. In the proposed model, the key generating process is performed on a separate cloud application and public and private keys are stored on key cloud servers. In addition, encryption and decryption procedures are performed on the client side through a service called "data encryption service". In order to use this encryption comparison program was made by analyzing the strengths and weaknesses of the six popular asymmetric encryption algorithms (namely RSA Small-e, Original RSA, RSA Small-d, MREA, E-RSA, and EAMRSA) over time, key size and security parameters. These algorithms are briefly described and redesigned in the same context in order to use a simulation process to investigate the performance of a client-based data encryption service. In addition, security analysis was performed by reviewing the performance of defined algorithms against three popular attacks: Brute Force, Mathematical, and Timing Attack. According to the results E-RSA is the most suitable algorithm to use in client-based data encryption service for achieving speed, accuracy, and security on this service based on the interaction issues of the third-party client service. [28]

CHAPTER 4

TECHNIQUES USED

The system model and recommended algorithm for application in the system are presented in this chapter. The information can be uploaded to the cloud in an encrypted form using this system, and the information can only be decrypted by the recipient who has been authorized for it.

4.1 CLIENT-SIDE ENCRYPTION

Before the data is moved from the client's local storage and transmitted elsewhere, it is encrypted using the client-side encryption approach. Because the CSP does not have access to the encryption key that was used, it is difficult for the CSP to retrieve the data that was hosted on its servers in a form that is either useful or understandable. This technique of encrypting the data on the client side offers a way for achieving a significant level of confidentiality. [29]

Encryption performed on the client's device works to reduce or eliminate the risk that sensitive information could be accessed by a service provider or third parties who force (directly or indirectly) service providers to allow access to data. Client-side encryption ensures that data and files based on the cloud can only be accessed at the client's end of the transmission. Client-side encryption protects the privacy of the data all the way from its original source to its final destination server by ensuring that the data remains encrypted while passing through any interim servers. Users are provided with more peace of mind as a result of this, as it prevents the loss of data and the illicit disclosure of personal or confidential information. [29]

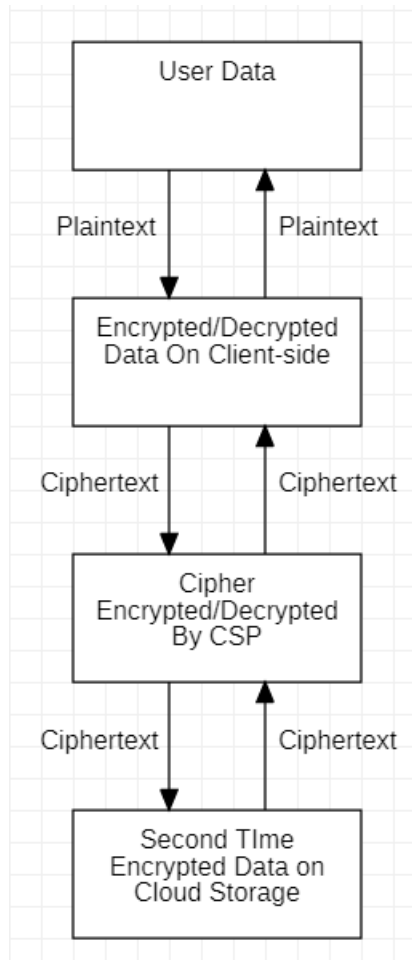


Figure 4.1 Process of Client-side Encryption and Client-side Decryption [30]

The downward arrows indicate the encryption process, and the upward arrows indicate the decryption process.

In this work, AES with Galois/Counter Mode, as detailed in the following section, has been utilized.

4.2 AES WITH GALOIS/COUNTER MODE (AES-GCM)

AES-GCM is able to provide authenticated encryption (both confidentiality and authentication), in addition to the capability to evaluate the integrity and authentication of Additional Authenticated data (AAD) that has been delivered in the plain. [31]

GCM is a cryptographic algorithm that consists of two operations: authenticated encryption and authenticated decryption. The permitted encryption procedure takes four-bit strings as its input format.:

- A sufficiently long secret key K for the associated block cipher.
- An initialization vector IV with an arbitrary bit count between 1 and 2^{64} . Each IV value for a key with a fixed value must be unique, but their lengths need not be the same. IV values of 96 bits can be processed more efficiently, hence this length is suggested for cases where efficiency is crucial.
- A plaintext P , whose number of bits might range from 0 and $2^{39}-256$.
- AAD, marked by the letter A . This data not encrypted but it is authenticated, and its bit length can range from 0 to 2^{64} .

It has two outputs:

- A ciphertext C with the same length as the plaintext P
- The authentication tag T , whose length might range between 0 and 128. The tag's length is denoted by the symbol t .

IV , K , A , C , and T are the five inputs to the authorized decryption operation. It only has one output, which is either the plaintext value P or the special symbol **FAIL**, which indicates that the inputs are not valid. For given plaintext P , initialization vector IV , the ciphertext C , additional authenticated data A , and tag T generated by the encrypt operation with inputs K , IV , A , and P are authentic for the key K . If its inputs were not produced by the encrypt operation with the same key, the approved decrypt operation will undoubtedly return **FAIL**.

[31]

Additional Authenticated Data A is used to secure information that must be authenticated, but it cannot be encrypted. The input could comprise ports, addresses, protocol version numbers, sequence numbers, and other data that indicate how plaintext should be treated, transmitted, or processed when using GCM to secure a network protocol. It is desired to verify these fields in many instances, but they must be kept clear in order for the network or system to function properly. When the information is included in the AAD, authentication is provided without putting the information into the ciphertext. [31]

The IV's main goal is to serve as a nonce, meaning that it must be unique for each invocation of the encryption procedure given a particular key. It's fine if the IV is created at random as long as the IV values are very likely to be distinct. It isn't required to add the IV in the field of AAD because it is authenticated. [31]

Plaintext receives both message confidentiality and message authentication. The length t of the authentication tag determines the authentication strength of P, IV, and A. GCM functions as a MAC on the input A when the length of P is zero. GMAC refers to the mode of operation in which GCM is used as a stand-alone message authentication code. [31]

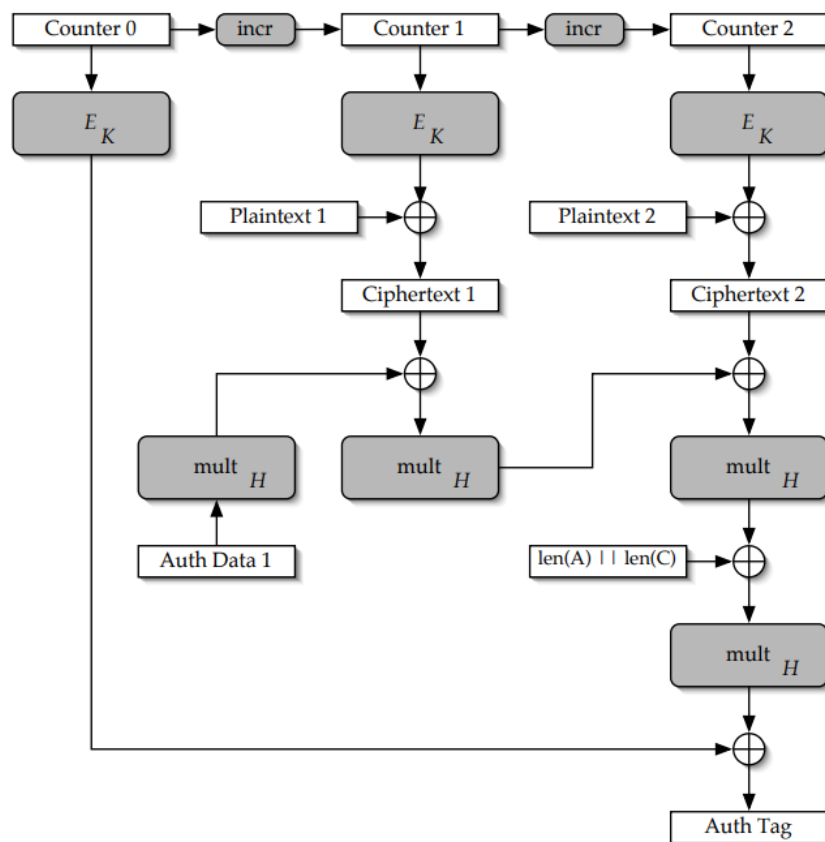


Figure 4.2 The Process of Authenticated Encryption. [31]

A situation with only one block of Additional Authenticated Data (labeled Auth Data 1) and two plaintext blocks is shown for simplicity. Here, E_K stands for block cipher encryption with the key K , $mult_H$ stands for hash key H multiplication in $GF(2^{128})$, and $incr$ stands for counter increment function.

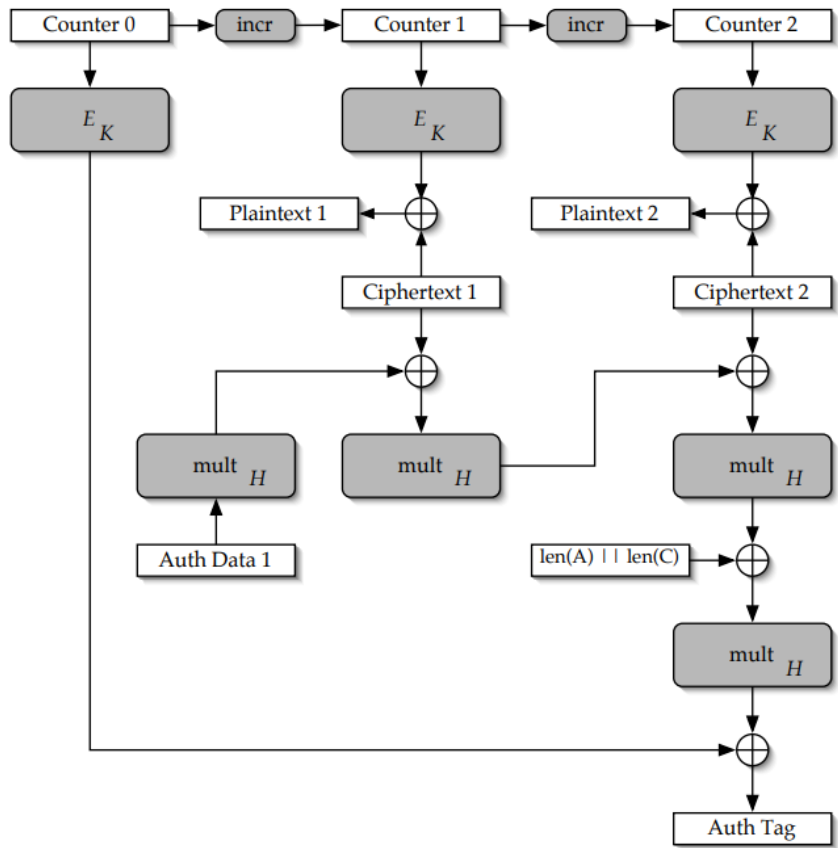


Figure 4.3 The Operation of Authenticated decryption, Depicting the Identical Scenario as in the Preceding Figure. [31]

CHAPTER 5

EXPERIMENTAL SETUP

This chapter will cover the experimental design of the conducted study. It provides a concise explanation of the programming tools, software, modules, and dataset used. In addition, the specifics of the system utilized for system development and implementation. Furthermore, several system runtime snapshots have been included.

5.1 PROGRAMMING TOOLS AND SOFTWARE USED

Python 3.10 has been utilized to achieve the intended results of this study. The data that has been encrypted has been stored using Google Drive. In order to facilitate the development process, the Python's Integrated Development and Learning Environment (IDLE) has been utilized.

The development work makes use of the following modules or functions:

`time`: The `time` module in Python offers a variety of ways to represent time in code, including numbers, strings, and objects. It also does things like wait while code is running and measure how efficient your code is in addition to showing time. [32]

`getpass`: In many programs, there is a requirement to secure the data or software, in which case we identify the users using a secret key or password. It is feasible to accept the password in a Python program using the `getpass()` function. [33]

`get_random_bytes`; It returns a random-length byte string. [34]

`PyCryptodome`: It is a Python module containing cryptographic primitives which are basically low-level. It provides the support for Python 2.7, Python 3.5 and later versions, as well as PyPy. `PyCryptodome` is a `PyCrypto` fork. [35]

Some of the upgrades over the previous official version of `PyCrypto` are as follows:

- Encryption modes with authentication (GCM, EAX, CCM, OCB, SIV).
- AES acceleration on Intel processors through AES-NI.

- API that is more compact and better.
- Top support for PyPy.

AES: Galois/Counter Mode has been defined in NIST Special Publication 800-38D. It only functions in conjunction with a cipher that is a 128-bit cipher, such as AES. [36]

At the level of the Crypto.Cipher module, there is a function called new () that is responsible for the creation of a new GCM cipher object for the appropriate base algorithm.. [36]

```
Crypto.Cipher.<algorithm>.new(key, mode, *, nonce=None, mac_len=None)
```

Create a new GCM object, using <algorithm> as the base block cipher.

- Parameters:**
- **key** (*bytes*) – the cryptographic key
 - **mode** – the constant `Crypto.Cipher.<algorithm>.MODE_GCM`
 - **nonce** (*bytes*) – the value of the fixed nonce. It must be unique for the combination message/key. If not present, the library creates a random nonce (16 bytes long for AES).
 - **mac_len** (*integer*) – the desired length of the MAC tag, from 4 to 16 bytes (default: 16).

Returns: a GCM cipher object

Figure 5.1 The parameters of Function for AES [36]

script: Colin Percival made scrypt, which is a key derivation function based on a password. It takes several parameters as input and the produced output is the derived key.

Not only is it hard to compute, but it also uses a lot of memory. This makes it safer against the threat of custom ASICs.

5.2 SYSTEM SPECIFICATION

The methodology is developed on a system with the following characteristics:

Processor that has been used: Intel Core i5, 2.3GHz

Memory (RAM) of the system used: 8GB

OS: Windows 10

5.3 DATASET USED:

The dummy files have been downloaded from [37] in order to study the process of encryption and decryption on various file sizes. All files are zip archives. The results and analysis of the experiments are presented in the following chapter.

5.4 OUTPUT:

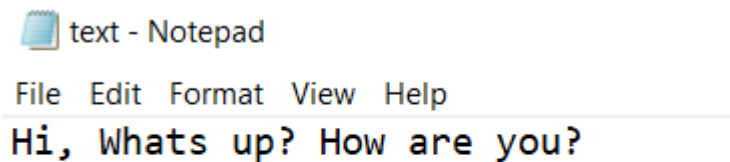


Figure 5.2 File before encryption

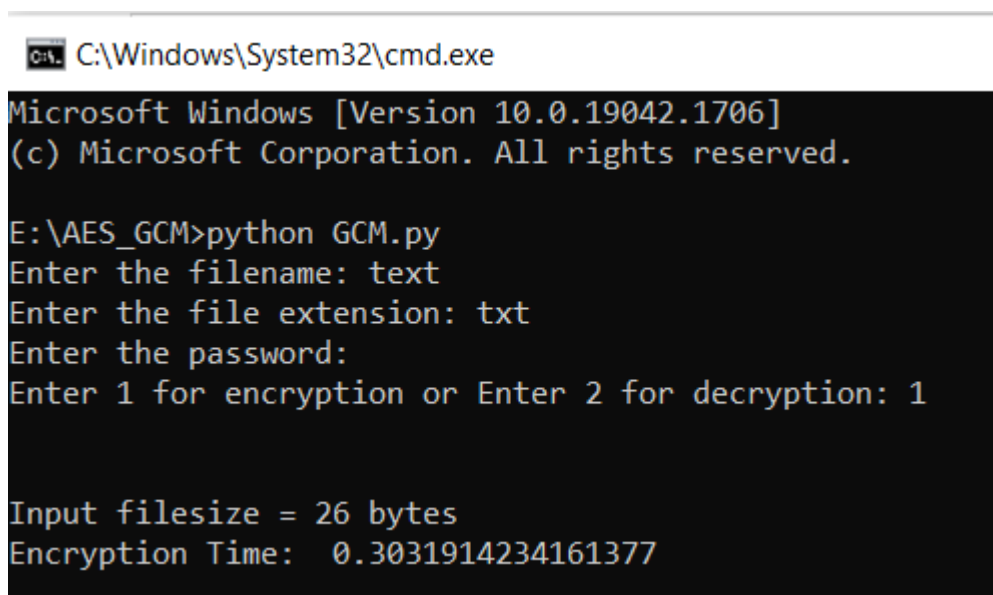


Figure 5.3 The Output after the Encryption Function Invoked

Encryption




Name	Date modified	Type	Size
 GCM	5/29/2022 10:29 AM	Python File	5 KB
 text	5/29/2022 10:37 AM	Text Document	1 KB
 text.txt.encrypted	5/29/2022 10:30 AM	ENCRYPTED File	1 KB

Figure 5.4 The Encrypted File created in the Folder

```

C:\Windows\System32\cmd.exe

Microsoft Windows [Version 10.0.19042.1706]
(c) Microsoft Corporation. All rights reserved.

E:\AES_GCM>python GCM.py
Enter the filename: text
Enter the file extension: txt
Enter the password:
Enter 1 for encryption or Enter 2 for decryption: 2

Decryption Time: 0.29465460777282715

E:\AES_GCM>_

```

Figure 5.5 The Output After the Decryption Function Invoked

```

decrypted - Notepad
File Edit Format View Help
Hi, Whats up? How are you?

```

Figure 5.6 The File After the Decryption, Which Gives Back the Original Content

CHAPTER 6

RESULT AND ANALYSIS

This chapter discusses the outcomes of the experiment that was conducted using the methodology described in the prior chapter. Also included are the analyses that were performed. For the sake of clarity in reporting, graphs have been plotted to highlight how the amount of time required to encrypt and decrypt the files considerably increases as the file size increases.

6.1 TIME ANALYSIS FOR ENCRYPTION

Table 6.1 Summary of Time Taken to Encrypt Files of Various Sizes

File Size (MB)	Encryption Time (milliseconds)
10MB	322.2 (0.3222)
50MB	395.1 (0.3951)
100MB	481.3 (0.4813)
200MB	870.4 (0.8704)
512MB	5415.1 (5.4151)

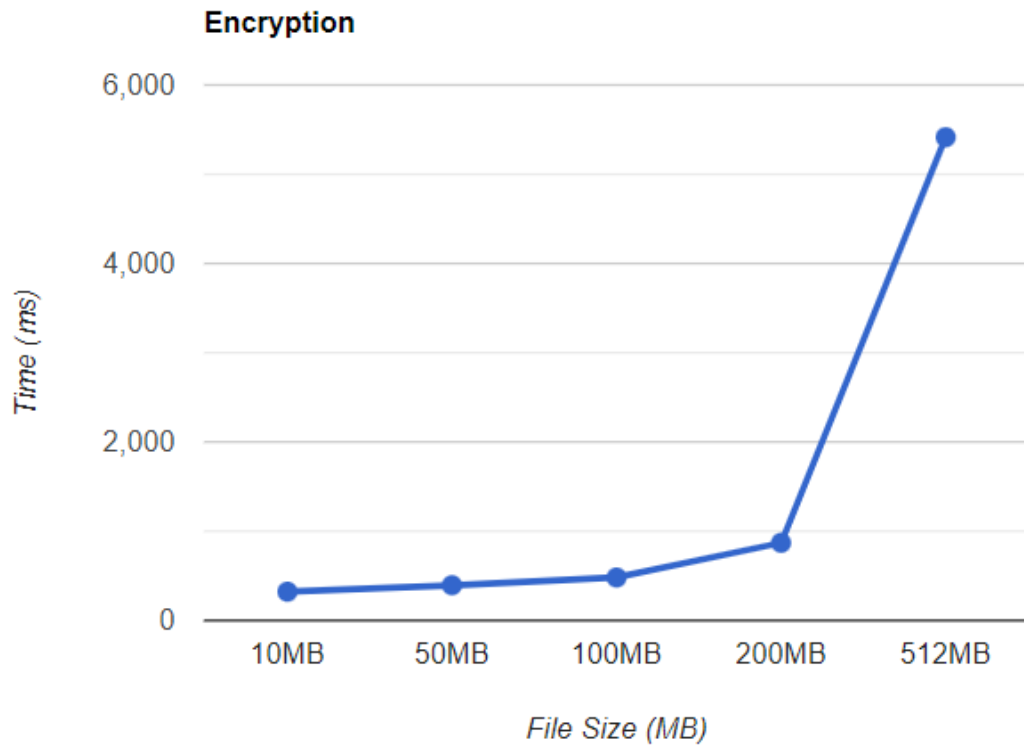


Figure 6.1 Graph of File Size vs Time Taken for the Process of Encryption [38]

6.2 TIME ANALYSIS FOR DECRYPTION

Table 6.2 Summary of Time Taken to Decrypt Files of Various Sizes

File Size	Decryption Time (milliseconds)
10MB	326.1
50MB	442.2
100MB	569.4
200MB	905.8
512MB	5701.1

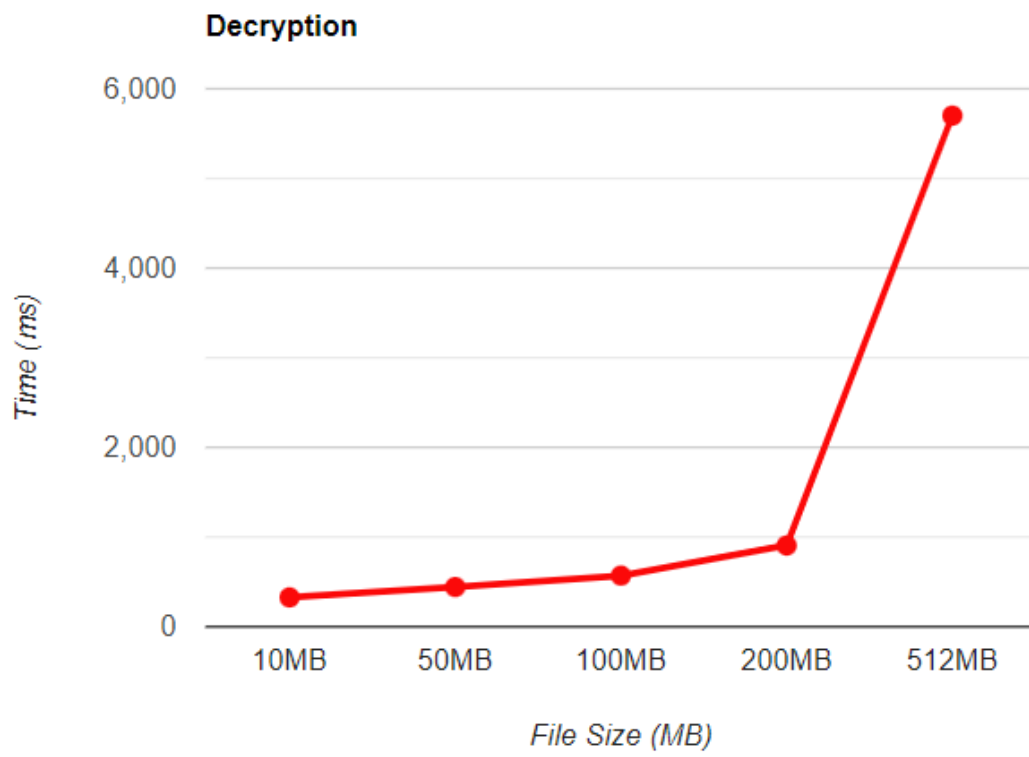


Figure 6.2 Graph of File Size vs Time Taken for the Process of Decryption [38]

CHAPTER 7

CONCLUSION AND FUTURE WORK

Following summarizing results and discussing the recommended methodology, this section gives the summary, final conclusion, and likely future studies in this area.

7.1 CONCLUSION

As information technology has progressed, there has been a corresponding rise in the demand for more secure methods of data protection in the cloud. Within the realm of cloud computing security, data security has emerged as the most pressing concern. Because the data and information shouldn't be given to a user from a third party, the right steps need to be taken.

The primary goal that we hope to accomplish with this study is to add an extra layer of protection by establishing encryption based on local storage before moving information to cloud storage, which reduces the risk of data theft or loss during transit, reduces data intervention, and snooping is prevented while data is being transferred within the service providers themselves, or once it is stored on the cloud. It also alleviates the problem of a lack of appropriate encryption standards on the service providers' side. To accomplish the same goal, AES-GCM has been utilized.

7.2 FUTURE WORK

This work describes a mechanism that generates an encrypted file with a file size of up to 200 MB while maintaining good performance. Future work might be planned so as to optimize the performance of generating encrypted files for larger files. Additionally, an attractive user interface could be created.

The advanced implementation can employ user-controlled encryption in which the consumers have complete control over the keys to carry out the process of encryption and decryption. Regularly used services and platform can adopt this strategy.

For future development, we suggest emphasizing on comprehensive practical analysis and testing to assess the possibility for more improvements.

REFERENCES

- [1] The Computing Using Cloud Retrieved From <https://blog.knoldus.com/know-about-cloud-computing-architecture/>
- [2] Various Components of Cryptosystem Retrieved From <https://www.tutorialspoint.com/cryptography/cryptosystems.htm>
- [3] Various Types of Cryptography Retrieved From <https://shodhganga.inflibnet.ac.in/bitstream/10603/256887/8/4.chapter%201.pdf>
- [4] The Basic Process of Encryption Retrieved From <https://www.okta.com/identity-101/password-encryption/>
- [5] The Basic Process of Symmetric Encryption Retrieved From <https://sectigostore.com/blog/types-of-encryption-what-to-know-about-symmetric-vs-asymmetric-encryption/>
- [6] The Basic Process of Asymmetric Encryption Retrieved From <https://sectigostore.com/blog/what-is-asymmetric-encryption-how-does-it-work/>
- [7] The Basic Process of Hashing Retrieved From <https://www.okta.com/identity-101/hashing-vs-encryption/>
- [8] Hemalatha, N., et al. "A comparative analysis of encryption techniques and data security issues in cloud computing." *International Journal of Computer Applications* 96.16 (2014).
- [9] Saranya, R. Gowthami, and A. Kousalya. "A comparative analysis of security algorithms using cryptographic techniques in cloud computing." *International Journal of Computer Science and Information Technologies* 8.2 (2017): 306-310.
- [10] Sugumaran, M., B. Bala Murugan, and D. Kamalraj. "An architecture for data security in cloud computing." *2014 World Congress on Computing and Communication Technologies*. IEEE, 2014.

- [11] Islam, N. K. V., and M. K. V. Riyas. "Analysis of various encryption algorithms in cloud computing." *International Journal of Computer Science and Mobile Computing* 6.7 (2017): 90-97.
- [12] Kartit, Zaid, et al. "Applying encryption algorithm for data security in cloud storage." *International Symposium on Ubiquitous Networking*. Springer, Singapore, 2015.
- [13] Semwal, Pradeep, and Mahesh Kumar Sharma. "Comparative study of different cryptographic algorithms for data security in cloud computing." *2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA)(Fall)*. IEEE, 2017.
- [14] Albugmi, Ahmed, et al. "Data security in cloud computing." *2016 Fifth international conference on future generation communication technologies (FGCT)*. IEEE, 2016.
- [15] Rao, R. Velumadhava, and K. Selvamani. "Data security challenges and its solutions in cloud computing." *Procedia Computer Science* 48 (2015): 204-209.
- [16] Kaur, Manpreet, and Rajbir Singh. "Implementing encryption algorithms to enhance data security of cloud in cloud computing." *International Journal of Computer Applications* 70.18 (2013).
- [17] Hussaini, Sheena. "Cyber security in cloud using blowfish encryption." *Int. J. Inf. Technol.(IJIT)* 6.5 (2020).
- [18] Mishra, Nishit, et al. "Secure framework for data security in cloud computing." *Soft computing: Theories and applications*. Springer, Singapore, 2018. 61-71.
- [19] Khan, Shakeeba S., and R. R. Tuteja. "Security in cloud computing using cryptographic algorithms." *International Journal of Innovative Research in Computer and Communication Engineering* 3.1 (2015): 148-155.
- [20] Kaur, Mandeep, and Manish Mahajan. "Using encryption algorithms to enhance the data security in cloud computing." *International Journal of Communication* 1.02 (2013): 130.

- [21] Musa, Abu, and Ashiq Mahmood. "Client-side Cryptography Based Security for Cloud Computing System." 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS). IEEE, 2021.
- [22] da Rocha, Marciano, et al. "Secure cloud storage with client-side encryption using a trusted execution environment." arXiv preprint arXiv:2003.04163 (2020).
- [23] Islam, Md Mahidul, Md Zahid Hasan, and Rifat Ali Shaon. "A Novel Approach for Client Side Encryption in Cloud Computing." 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE). IEEE, 2019.
- [24] Henziger, Eric, and Niklas Carlsson. "The overhead of confidentiality and client-side encryption in cloud storage systems." Proceedings of the 12th IEEE/ACM International Conference on Utility and Cloud Computing. 2019.
- [25] Souza, Stefano MPC, and Ricardo S. Puttini. "Client-side encryption for privacy-sensitive applications on the cloud." Procedia Computer Science 97 (2016): 126-130.
- [26] Surv, Niteen, et al. "Framework for client side AES encryption technique in cloud computing." 2015 IEEE International Advance Computing Conference (IACC). IEEE, 2015.
- [27] Rahmani, Hossein, et al. "Encryption as a Service (EaaS) as a Solution for Cryptography in Cloud." Procedia Technology 11 (2013): 1202-1210.
- [28] Moghaddam, Faraz Fatemi, Omidreza Karimi, and Maen T. Alrashdan. "A comparative study of applying real-time encryption in cloud computing environments." 2013 IEEE 2nd International Conference on Cloud Networking (CloudNet). IEEE, 2013.
- [29] https://en.wikipedia.org/wiki/Client-side_encryption
- [30] A. Musa and A. Mahmood, "Client-side Cryptography Based Security for Cloud Computing System," 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS), 2021, pp. 594-600, doi: 10.1109/ICAIS50930.2021.9395890.
- [31] <https://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/gcm/gcm-spec.pdf>

- [32] <https://realpython.com/python-time-module/>
- [33] <https://www.geeksforgeeks.org/python-getpass-module/>
- [34] <https://pycryptodome.readthedocs.io/en/latest/src/random/random.html>
- [35] <https://pycryptodome.readthedocs.io/en/latest/src/introduction.html>
- [36] <https://pycryptodome.readthedocs.io/en/latest/src/cipher/modern.html#gcm-mode>
- [37] <http://xcall.vodafone.co.uk/>
- [38] <https://www.rapidtables.com/tools/line-graph.html>