Data Security in Cloud using Symmetric Encryption Algorithm

by

Sourabh Parekh
(2016IS-18)

A thesis submitted in partial fulfillment of the requirements for the award of the degree of

Master of Technology

in

CSE (Information Security)

2016-18

विश्वजीवनामृतं ज्ञानम्

ATAL BIHARI VAJPAYEE
INDIAN INSTITUTE OF INFORMATION
TECHNOLOGY AND MANAGEMENT
GWALIOR-474015
2018

Thesis Certificate

I hereby certify that the work, which is being presented in the report/thesis, entitled **Data Security in Cloud using Symmetric Encryption Algorithm**, in fulfilment of the requirement for the award of the degree of **Master of Technology** and submitted to the institution is an authentic record of my/our own work carried out during the period *June-2017* to *May-2018* under the supervision of **Prof. Rajendra Sahu**. I also cited the reference about the text(s) / figure(s) / tables(s) from where they have been taken.

————————————————-

Prof. Rajendra Sahu

Date ——————

-

The final copy of this thesis has been examined by the signatories, and we find that both thecontent and the form meet acceptable presentation standards of scholarly work in the abovementioned discipline.

Candidate's Declaration

I hereby certify that I have properly checked and verified all the items as prescribed in the check-list and ensure that my thesis is in the proper format as specified in the guideline for thesis preparation.
I declare that the work containing in this report is my own work. I understand that plagiarism is defined as any one or combination of the following:

(1) To steal and pass off (the ideas or words of another) as one's own

(2) To use (another's production) without crediting the source

(3) To commit literary theft

(4) To present the new and original idea or product derived from an existing source.

I understand that plagiarism involves an intentional act by the plagiarist of using someone else's work/ideas completely/partially and claiming authorship/originality of the work/ideas. Verbatim copy, as well as the close resemblance to some else's work, constitute plagiarism.
I have given due credit to the original authors/sources for all the words, ideas, diagrams, graphics, computer programmes, experiments, results, websites, that are not my original contribution. I have used quotation marks to identify verbatim sentences and given credit to the original authors/sources.
I affirm that no portion of my work is plagiarized, and the experiments and results reported in the report/dissertation/thesis are not manipulated. In the event of a complaint of plagiarism and the manipulation of the experiments and results, I shall be fully responsible and answerable. My faculty supervisor(s) will not be responsible for the same.

Signature:

Name: Sourabh Parekh

Roll. No: 2016IS-18

Date: 9 May 2018

Abstract

Cloud computing is one of the internet based techniques for complex calculation and scaling of data. Many companies are using cloud-based services. Cloud Computing offers few advantages like the accessibility of data and low-cost services. Data storage is the primary usage of the cloud computing. It is more flexible and authentic for users to retrieve and store their data anywhere and at any time. Security is a crucial role in cloud computing, as customer store their data with cloud storage providers but these providers may be untruthful. Customers feel curious about attacks on the availability and integrity of there data kept in the cloud storage from the attackers and from any security damage to cloud services. This paper proposes an enhanced symmetric-based encryption algorithm to ensure data security in cloud storage.

Tags:

Cloud data storage,Data confidentiality, Data integrity, Privacy, Proof of data possession, Security requirements.

Acknowledgments

I am highly indebted to **Prof. Rajendra Sahu** and obliged for giving me the autonomy of functioning and experimenting with ideas. I would like to take this opportunity to express my profound gratitude to him not only for his academic guidance but also for his personal interest in my report and constant support coupled with the confidence-boosting and motivating sessions which proved very fruitful and were instrumental in infusing self-assurance and trust within me. The nurturing and blossoming of the present work is mainly due to his valuable guidance, suggestions, astute judgment, constructive criticism and an eye for perfection. My mentor always answered the myriad of my doubts with smiling graciousness and prodigious patience, never letting me feel that I am novices by always lending an ear to my views, appreciating and improving them and by giving me a free hand in my report. It's only because of his overwhelming interest and helpful attitude, the present work has attained the stage it has.

Finally, I am grateful to our Institution and colleagues whose constant encouragement served to renew my spirit, refocus my attention and energy and helped me in carrying out this work.

Place: ABV IIITM, Gwalior (Sourabh Parekh)

Date: 9 May 2018

Contents

Chapter

Tables

Table

Figures

Figure

Chapter 1

Introduction

This chapter tells about the basics technology and principles of cloud computing.

1.1 Background

1.1.1 Background Information on Clouds

Data is a valuable resource for organizations and individuals. Their management is an important task and includes assuring the integrity of data. For decades, organizations and individuals have been using computer hardware such as floppy discs, CDs, DVDs, discs, and hard discs to store their data. Introduction of database systems enhanced information management and made it more effective [2].

The most recent decades have made a reality data preparing where information can be handled effectively on huge processing and capacity stages available by means of the Internet [3]. Growths in database frameworks and systems administration empowered the advancement of new registering models. They include grid computing which was developed in the early The 1990s; utility computing and around 2005 they develop cloud computing [2].

"*Cloud computing* (CC) can be defined as a computing model that enables convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management efforts or service provider interactions" [2]. Cloud computing includes the delivery and use of IT infrastructure, platforms and applications of any type inside the form of services which are electronically accessed from the Internet [4]. Just a some examples of applications using cloud services include: online business applications, social networking sites, online file storage, and web-mail [3].

1.1.2 Background Information on Security and Privacy in Clouds

Security can be defined as follows [5]: " *Security is the right not to have one's activities adversely affected via tampering with one's objects.*"

In an equally succinct way, we can define privacy as follows [5]: "*Privacy is the right to have information about oneself left alone.*" Similarly, Rocha et al. [6] define privacy as the selective control of access to "self." Selective control refers to the process where individuals control their interaction and information exchange with others. To assure their privacy, individuals try to control their openness to others. Pearson [6] explains that the level of openness between individuals is determined by their relationship and the value given to the information safeguarded. Privacy can be generally described as the dynamic process whereby individuals regulate the degree of their openness to others.

Classic "CIA" Security Triad. A classic definition of securityin terms of its basic characteristics specify it in terms of the CIA triad; the acronym"CIA" stands for confidentiality, integrity, and availability–three key requirements for any secure system [5]. They are defined as follows:

(1) *Confidentiality*: It is the ability to hide information from those people unauthorized to view it. It is the basis of many security mechanisms protecting not only information but other resources.

(2) *Integrity*: It is the ability to ensure that data is an accurate and unchanged representation of the original information [5].

(3) *Availability*: It ensures that a resource is readily accessible to the authorized user upon the user's request.

This model is very widely applicable in security analysis, from access to a user's Internet history to security of encrypted data across the Internet. [7].

Security and Privacy in Clouds. Over the years, numerous researchers have studied and surveyed the issues of security and privacy in cloud environments. To better comprehend those issues and their connections, technology researchers, and experts have taken advantage of different criteria to establish a comprehensive impression. Gruschka et al. [8] recommend a modeling of the security ecosystem in terms of three cloud system participants: service instance, service user, and the cloud provider. Furthermore, they identify attack categories: a) user to service, b) service to the user, c) user to cloud, d) cloud to the user, e) service to the cloud, and f) cloud to service. While cloud computing is associated with numerous security and privacy problems, it can be made effective by implementing efficacious solutions. In this thesis, we separate cloud computing security issues from its privacy issues.

1.2 CLOUD COMPUTING OVERVIEW

1.2.1 Essential Characteristics of Cloud Computing

Cloud computing is differentiated from other computing paradigms or model by its characteristics. These characteristics are categorized into essential characteristics and common characteristics. Gong et al. [9] enumerate the following five essential characteristics:

(1) *On-demand self-service*: it enables the user to unilaterally provision computing capabilities as server time and network storage [10]. This is possible without the need for human interaction with each service provider. Computing resources are instantly available to users as per their requests.

(2) *Broad network access*: It refers to the situation where the computing capabilities are available to users over the network. Users can access cloud resources through standard mechanisms that enable them to use heterogeneous platforms i.e. they can access cloud resources through mobile phones, laptops, and PCs [6]. Therefore, users dont need to be at specific locations in order to access cloud-based services. Cloud-based services can be accessed from any location any time provided that there is adequate IP networking.

(3) *Resource pooling*: Service providers pool together computing resources so as to satisfy computing needs of multiple users via different physical and virtual resources. The pooled resources (such as servers, storage devices, etc.) are shared across many users. Providers select which resources from the pool to assign to each cloud consumers workload to optimize the quality of service. Sharing facilitates cost reductions because it allows more applications to be served on the computing hardware of the cloud that would be required with dedicated computing resources.

(4) *Rapid elasticity*: This refers to the rapid and elastic provision of computing capabilities to quickly scale out, and rapid release to quickly scale in. The capabilities that are provisioned to consumers are (from the users point of view) unlimited and can be purchased in any quantity at any time. Elastically increases service capacity during busy periods, and reduces capacity during customers off-peak periods, enabling cloud consumers to minimize costs while meeting their service quality expectations.

(5) *Measured service:* This service automatically controls and optimizes resource use. It is done at some level of abstraction appropriate to the type of CC service [10]. This characteristic enables monitoring, controlling and reporting of resource usage and thus enabling fair service purchases.

1.3 Delivery Models for Cloud Computing

Cloud computing delivery models include three levels [11], as shown in Fig. 1.1: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software (application)-as- Service (SaaS).

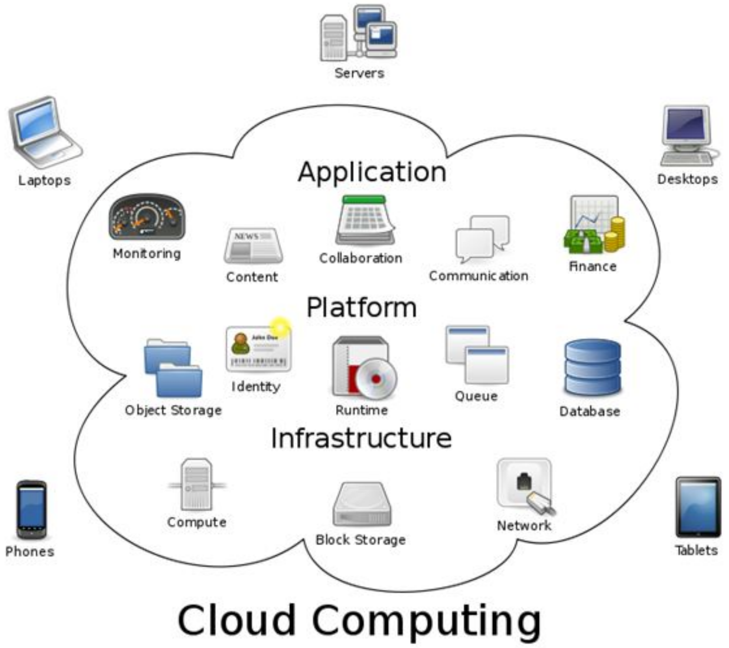


Figure 1.1: Cloud Computing Delivery Models.

1.3.1 Infrastructure as a Service (IaaS)

This CC capability provided to users involves provisioning computing resources and services such as processing, storage, networks, content delivery networks, backup, and recovery, etc., on which users can deploy and run their own software [12]. As shown in Fig. 1.2, IaaS does not give consumers the authority to manage or control the underlying cloud infrastructure or the lower layers of OS but instead allows consumers to have full control over the higher levels of OS, deployed applications; and limited control of networking components, such as host firewalls [13].

IaaS Characteristics: The characteristics of IaaS include [11, 12]

(1) Multiple users on a single piece of hardware.

(2) Resources available as a service.

(3) Dynamic scaling capabilities the cost varies based on the infrastructure selection.

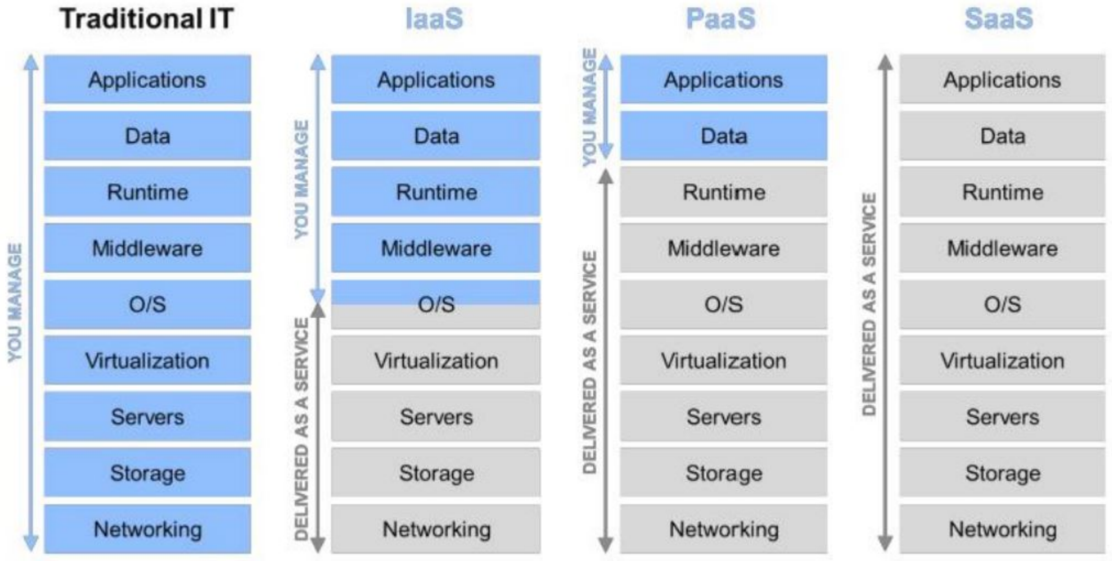


Figure 1.2: IaaS vs. PaaS vs. SaaS (Separation of Responsibilities [1]

IaaS Suitability: IaaS suitable for the following: [11, 12]

(1) Organizations that need a complete control over their software, e.g., for high performing applications.

(2) Startups and small companies that do not wish to spend money and time in procuring hardware and software.

(3) Growing organizations not yet sure which applications they will need, or that expect to evolve in an unpredictable way, and hence do not want to commit to specific infrastructure.

(4) Services that experience volatile demands where highly dynamic scaling up or down in sync with traffic spikes or valleysis critical.

IaaS Examples: Examples of IaaS include Amazon Web Services (AWS), Cisco Metapod, Microsoft Azure, Google Compute Engine (GCE).

1.3.2 Platform as a Service (PaaS)

PaaS gives consumers the ability to deploy onto a cloud infrastructure consumer-created or consumer-acquired applications, which were created using programming languages and tools supported by the CC provider. As shown in Fig. 1.2, consumers are not given the control or authority to manage their underlying cloud infrastructure, i.e., networks, servers, storage, applications, data etc [1]. However, they are given the authority over their deployed applications in an application hosting environment, which helps in running applications in a quick transparent manner. PaaS services include a virtual desktop, web service delivery and development platforms, database service etc., [13].

PaaS Characteristics: The characteristics of PaaS include: [1]

(1) A virtualization technology build on top of PaaS enables acquiring resources on demand and scaling them up/down as needed.

(2) Varying application development and application execution services to facilitate development, testing, deployment and hosting of software applications in an integrated development environment.

(3) Sharing of the same development environment by multiple users.

(4) Integrated web services and databases.

(5) Billing and subscription managed by CC tools.

PaaS Suitability: PaaS is suitable for the following: [1]

(1) Multiple developers working on the development of the same product, or external parties involved in the development process; PaaS brings in the speed and flexibility to the development process.

(2) Organizations following the Agile Methodology for software development; PaaS cease the difficulties associated with the rapid development and iterations of an application [1].

(3) Organizations wishing to spread their capital investment; PaaS reduces the spending on computing infrastructure as well as application development and execution.

Enterprise PaaS Examples: Examples of PaaS include Apprenda.

1.3.3 Software as a Service (SaaS)

With the SaaS delivery model, CC consumers are given the capability to use the CC providers applications running on the cloud infrastructure (in contrast to PaaS, where they run their own applications). In SaaS, the cloud users do not have control or authority to manage the underlying cloud infrastructure or even the individual applications [13]. As shown in Fig. 3, there are possibilities of that user will have limited access to configuring settings related to applications. SaaS services include email and office productivity applications, customer relations management, enterprise resources planning, social networking, data management, etc. [11, 13].

SaaS Characteristics: The characteristics of SaaS include: [11, 12]

(1) Software hosted on a remote server, and always accessible through a web browser over the Internet.

(2) Application managed from a central location.

(3) Application users do not need to worry about hardware or software (updates, patches, etc.)

(4) Any integration with third-party applications is done through APIs

SaaS Suitability: SaaS is suitable for the following: [11, 12]

(1) Applications where the demands spike or fall significantly. For example, tax software is in a high demand during the tax filing season, hotel reservations see a spike during holiday seasons and so on [1].

(2) Applications that require web as well as mobile access. Examples include sales management software, CRM systems.

(3) Short term projects that require collaboration. The pay-as-you-go model makes it convenient to quickly set up a collaborative environment, and quickly close it down.

(4) Start-up businesses that want to quickly launch e-commerce sites without worrying about server configurations and software updates.

SaaS Examples: Google Apps, Salesforce, Workday, Concur, Citrix GoToMeeting, Cisco WebEx.

1.4 Deployment Models of Cloud Computing

There are four deployment models of cloud computing: public, private, community, and hybrid as shown in Fig. 1.3 [14]. Each of these models has different characteristics and implications for the customers [15].

The choice of the deployment model depends on an organizations objectives and business needs. Before selecting a deployment model, an organization is encouraged to review the security, reliability and performance issues associated with the model.

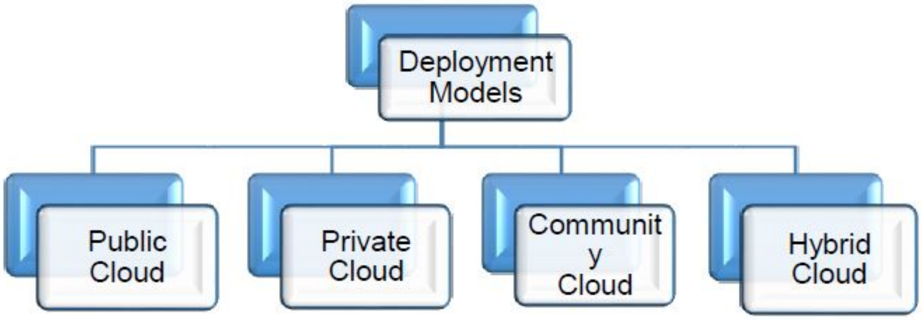


Figure 1.3: Deployment Models for Cloud Computing.

1.4.1 Public Cloud

A *public cloud* is the most used deployment model, and what most people have in mind as "a cloud." Cloud services are available to the general public and are managed by CC service providers.

The providers own and manage their cloud infrastructures. A public cloud has multitenant capabilities and is shared by a large number of customers who have nothing or very little in common. Users data are not publicly visible [14].

The advantages of a public cloud include:

(1) *Low Cost:* The nature of the public cloud is that you only pay for what you use. So as an organization grows or shrinks so do the associated costs. By comparison, a private cloud might require an infrastructure designed to cope with growth (thus more expensive); likewise, no costs saved if the needs shrink. Other significant savings are related to costs associated with the size and work of the in-house IT team.

(2) *Increased Efficiency:* As public clouds have dedicated teams working on maintaining the infrastructure, downtime is less likely to be an issue. On top of this, if applications are hosted by CC provider, updates are usually managed by the provider, saving upgrading expenses.

The disadvantages of a public cloud include:

(1) *Wrong Provider:* There are very real hazards of picking a wrong public cloud provider. If a provider does not keep hardware up to date, users may suffer compliance and execution speed issues.

(2) *Reduced Control:* As the public cloud is controlled by a CC provider, users do not have as much control as in a private cloud.

1.4.2 Private Cloud

A *private cloud* is a dedication to computing infrastructure to a single specific organization or group without sharing with any other organization. The private cloud can be owned or leased. In a private cloud, there are no additional security regulations, legal requirements or bandwidth limitations [7]. However, the service providers and users have optimized the control of infrastructure and security. An organization may opt for private cloud when they feel they are unable to remotely host their data and hence, they seek the help of cloud to enhance their resource utilization and automation [15].

The advantages of private clouds include the following ones:

(1) *Security:* The security is within the organization's control. Although whilst many are quick to credit private clouds as being more secure [14], the vast array of different deployment types and levels of security within private hosting environments makes this an extremely bold statement [15]. The reality for me is that a private cloud is just as susceptible to security risks as a public cloud. The only difference is that a public cloud may be more attractive to infiltrate than a private cloud as there is a wider amount of data in it.

(2) *Performance:* If a private cloud is deployed inside an organization's firewall it increases the performance compared to using the public cloud off premise.

(3) *Control and Flexibility:* Organizations have more control in private clouds and as a result, deploying new applications and make changes can be done in a quick manner.

There are a few disadvantages for private clouds, including the following ones:

(1) *Additional Maintenance:* If a private cloud is not maintained by the software vendor, then it is unlikely that the organization will benefit from the regular updates that are often associated with modern SaaS applications.

(2) *Higher Costs:* Everything related to a private cloud is more expensive. Whether the organization has to purchase the infrastructure or it is still provided by the vendor, it will be more expensive than for public cloud. Also, management costs are higher.

1.4.3 Community Cloud

A *community cloud* should not be confused with a public cloud. In community clouds, resources are available for a number of individuals or groups who have shared interestsin contrast to the public cloud in which users do not have shared common interests.

The computing infrastructure can be either on- or off-site. Cloud resources are owned and managed by one or more of the collaborators in the community [14]. in contrast to a public cloud where resources are owned and managed by an individual provider/owner.

1.4.4 Hybrid Cloud

A *hybrid cloud* is a combination of more than one deployment model [15]. There is a management framework that ensures that the environments appear as a single cloud. Adoption of the hybrid cloud may result from strong requirements for security, price, and performance.

1.5 Problem/Motivation

- Sensitive data for a client is kept on a cloud platform, under the direct control of the cloud not of the client. Securing users data in a cloud is one of the challenges tasks.
- Big companies are also getting interested in cloud-based solutions in order to make their business more robust and scalable. However, there is often a lack of security when realizing such cloud-based solutions.
- This thesis aims to provide guidelines to strengthen the security in the cloud-based infrastructure.

1.6 Objectives

Thesis aims to develop

- Design and develop an effective Symmetric based encryption algorithm for secure data storage in cloud storage.
- To compare the proposed algorithm with the existing algorithm like (substitution cipher, transposition cipher etc).

1.7 Research work flow

The organization of thesis is as follows:

- Chapter 1 discusses motivation of thesis, basics of cloud computing, delivery model and deployment model of cloud computing
- Chapter 2 presents a literature review in the area of data security in cloud computing.
- chapter 3 proposes an Enhanced Symmetric Algorithm that would ensure the security in cloud storage.
- chapter 4 presents the comparison result of proposed Algorithm.
- concludes the research

Chapter 2

Literature review

2.1 Background

2.1.1 SECURITY PROBLEMS IN CLOUD COMPUTING

Clouds can be flexible and cost-efficient. In a cloud infrastructure, sensitive information for a customer is kept on geographically dispersed cloud platforms, under the direct control of the cloud not of the customer. Securing users data in a cloud is one of the most challenging tasks Cloud resources (such as software, platforms, and infrastructure) are vulnerable to abuse, theft, unlawful distribution, harm, or compromise. Among others, there is a risk that users information can be leaked to a competitor. Unauthorized access to data stored in clouds can be minimized through ensuring security.

2.1.1.1 Importance of Security in Cloud Computing

Despite the benefits that an organization enjoys after adopting cloud computing, there are security issues that are a notable barrier to adoption of the technology. After adopting CC, the crucial responsibility for data management and protection belongs to the service provider [6]. [**?**] argue that loss and manipulation of data from unknown sources are prevented through providing secure computing environment, which is defined as a system implemented to control storage and use of data. Secure computing environment reduces the damage on a physical computing device that may result from malware [7].

Cost of using cloud services is significantly reduced in a secure environment. Security enhances performance and reduces chances of damage to data, software, and hardware.

2.1.1.2 Problems: Vulnerabilities, Threats, and Attacks

Cloud computing presents various risks to an organization that has adopted it. Cloud security issues are determined greatly by the cloud service delivery model and deployment model. High-security levels can be more easily achieved in private clouds than in public clouds [8].

- Cloud Authentication Attacks

  Authentication is a process that ensures and confirms correctness and validity of a users credentials (an essential property that is selected for a given authentication process). Authentication begins when a user tries to access information. First, the user must prove his access rights and possess the required essential property selected for the given authentication process [12].In a cloud environment, a user tries to establish a connection with cloud services using his own credentials that authenticate him in order to allow him access to cloud services [13].

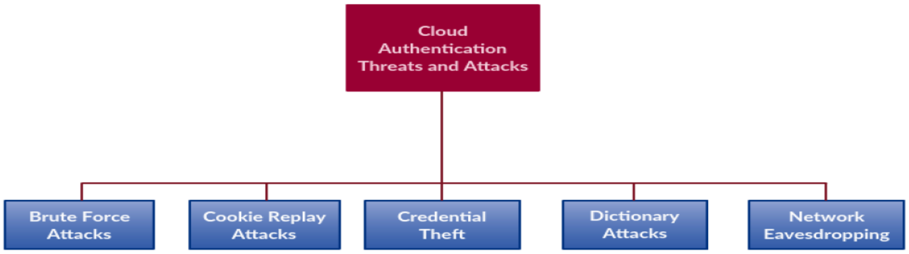


Figure 2.1: Cloud Authentication Threats and Attacks.

Threats and attacks on authentication in a cloud environment, shown in Fig. 2.1, include:

1) Brute Force Attacks: An attacker guesses the credentials of a user.

2) Cookie Replay Attacks: An attacker gains access to a users system through the reuse of a stolen cookie to a session, which contains important confidential information.

3) Credential Theft: An attacker exploits the system and gains access/credentials through data theft, e.g., via phishing.

4) Dictionary Attacks: An attacker guesses credentials by trying, in turn, different terms from the dictionary.

5) Network Eavesdropping: An attacker steals credentials by reading network traffic.

- DOS Attacks

  DOS attacks and mobile terminal security level attacks are quite common. DOS Attacks: Denial-of-Service (DOS) and distributed denial of service (DDOS) are among the major security threats in cloud computing. A DOS attacks occur when an intruder attempts to deny authorized users access to information and cloud services. A DDOS attack involves the use of multiple corrupted systems to target and corrupt a certain cloud in order to induce DOS attacks.

2.1.2 PRIVACY PROBLEMS IN CLOUD COMPUTING

Privacy is a crucial issue in cloud computing because a customers information and business logic must be entrusted to cloud servers owned and maintained not by the customer but by cloud providers [14].

2.1.2.1 Importance of Privacy and Confidentiality in Clouds

Apart from the cost-effectiveness of cloud computing, another property that, when guaranteed, could increase the use of cloud services is protecting the privacy of users data. In other words, customers conviction that a CC provider assures the privacy of their data increases their trust into CC services, and leads to a growth in the use of these services.

The issues of privacy of individuals data in clouds arise when they share it with others are when they are accessed by the provider for unauthorized use. Confidentiality issues result when the provider does not address the loopholes for information leakage or when they share their customers information with others without the authorization of the user. The risks of privacy and confidentiality are influenced by the terms of service and privacy policies implemented by the service providers.

2.1.2.2 Problems: Vulnerabilities, Threats and Attacks

- Data Breaches

  A data breach is a situation where sensitive or protected data of cloud users are viewed, stolen or used by an unauthorized individual [15]. Data breaches cause a significant impact on the users, cloud services providers and government agency.

  Data breaches may lead to permanent data loss. The main security concern in cloud computing relates to data breaches in cloud platforms, which entails both data and computation integrity. Maintain that data integrity entails honest storage of user information on cloud servers. In that case, any data breach, such as data loss or compromise, must be detected. Meanwhile, computation integrity entails the execution of programs without any form of distortion. However, user data remains vulnerable to distortions associated with malicious users, cloud providers, and malware, which require instantaneous detection

2.2 Key related research

2.2.1 SECURITY CONTROLS FOR CLOUD COMPUTING

- **Controls via Effective Encryption**

To enhance security protection, advanced encryption algorithms can be applied to CC. They include:

- Attribute-Based Encryption (ABE)

  ABE comprises either ciphertext-policy ABE or key policy ABE In CP-ABE, the encryptor has the responsibility to control the access strategy. As the strategy increases in complexity, the design of the public key system becomes more intricate, proving the security of the system more difficult. [16] In Key Policy Attribute-Based Encryption (KP-ABE), the attribute sets are used to explicate the encrypted texts as well as the private keys with the itemized encrypted texts that a user leaves behind to decrypt. [17]

  The problem on Attribute-based encryption (ABE) scheme is that data owner needs to use the public key of every authorized user to encrypt data.

  ∗ Key Policy Attribute-based Encryption (KP-ABE):

    KP-ABE scheme can achieve more flexibility to control users and fine-grained access control than ABE scheme.

  ∗ Ciphertext-Policy Attribute-based Encryption(CP-ABE):

    It overpowers the short come of KP-ABE of choosing who can decrypt the data.

- Fully Homomorphic Encryption (FHE)

  FHE in cloud computing allows direct computations on encrypted data. Unfortunately, practical use of this method is limited only to the very simple processing of data, specifically ones limited to adding and multiplying numbers. [18]

  Homomorphic ciphers typically do not provide verifiable computing. In words, you encrypt your data, send it to the cloud and let the cloud compute on it for you. How do you know the cloud performed the correct computation?

Performance is often a disadvantage. Ciphertexts in the ciphers you mention are much larger than the plaintexts, The computations on these large ciphertexts are typically slower than if you just performed the computation on the plaintext itself.

Chapter 3

Methodology

This section introduces the hypothesis and the analytical validation of the proposed solution.

3.1 Mechanism/Algorithm

The Proposed technique to enhance the encryption techniques by integrating substitution cipher and transposition cipher

Encryption Algorithm

(1) (a) Count the No. of Character(**N**) in the plain text.

Plaintext - VIRUSFOUND

N=10 (N= no.of Characters in the Message)

(b) Convert the plain text into equivalent **ASCII** code .

ASCII code value for the plaintext

86,73,82,85,83,70,79,85,78,68

(c) Convert the ASCII code into equivalent **HEXADECIMAL** code .

Hexadecimal code value for the plaintext

56,49,52,55,53,46,4F,55,4E,44

(2) Form a square matrix A of size **S** such that ($S*S \geq N$) and use special symbol # to complete the matrix.

To form a square matrix Form a 4 * 4 matrix. (using value 24(#) to complete the square matrix)

56	49	52	55
53	46	4F	55
4E	44	24	24
24	24	24	24

(3) Transpose the Matrix ($A = A^T$)

56	53	4E	24
49	46	44	24
52	4F	24	24
55	55	24	24

(4) Make a new matrix, write firstly even column (2, 4, 6, ...) values and then odd column(1, 3, 5..) values, Rewrite the matrix, read column wise – write (into a new matrix)row wise. (R1 = 2c1 , R2 =4c2, R3 = 1c1 , R4 = 1c3)

53	46	4F	55
24	24	24	24
56	49	52	55
4E	44	24	24

(5) Generate the S random key and **EX-OR** with each row of the matrix.

53	=	5	3
		0101	0011
key 23	=	0010	0011
		0111(7)	0000(0)

(6) Make a new matrix by writing firstly the last column and then from first onwards.Rewrite the matrix, read column wise – write (into a new matrix)row-wise.

76	16	47	05
70	16	44	6F
65	16	5B	65
6C	16	40	05

(7) Convert the ASCII code into character value.

118	22	71	05
112	22	68	111
103	22	91	101
108	22	64	05

(8) **Cipher Text** is generated by writing the values sequentially in one row.

Encrypted Text: gA@elv@TmG

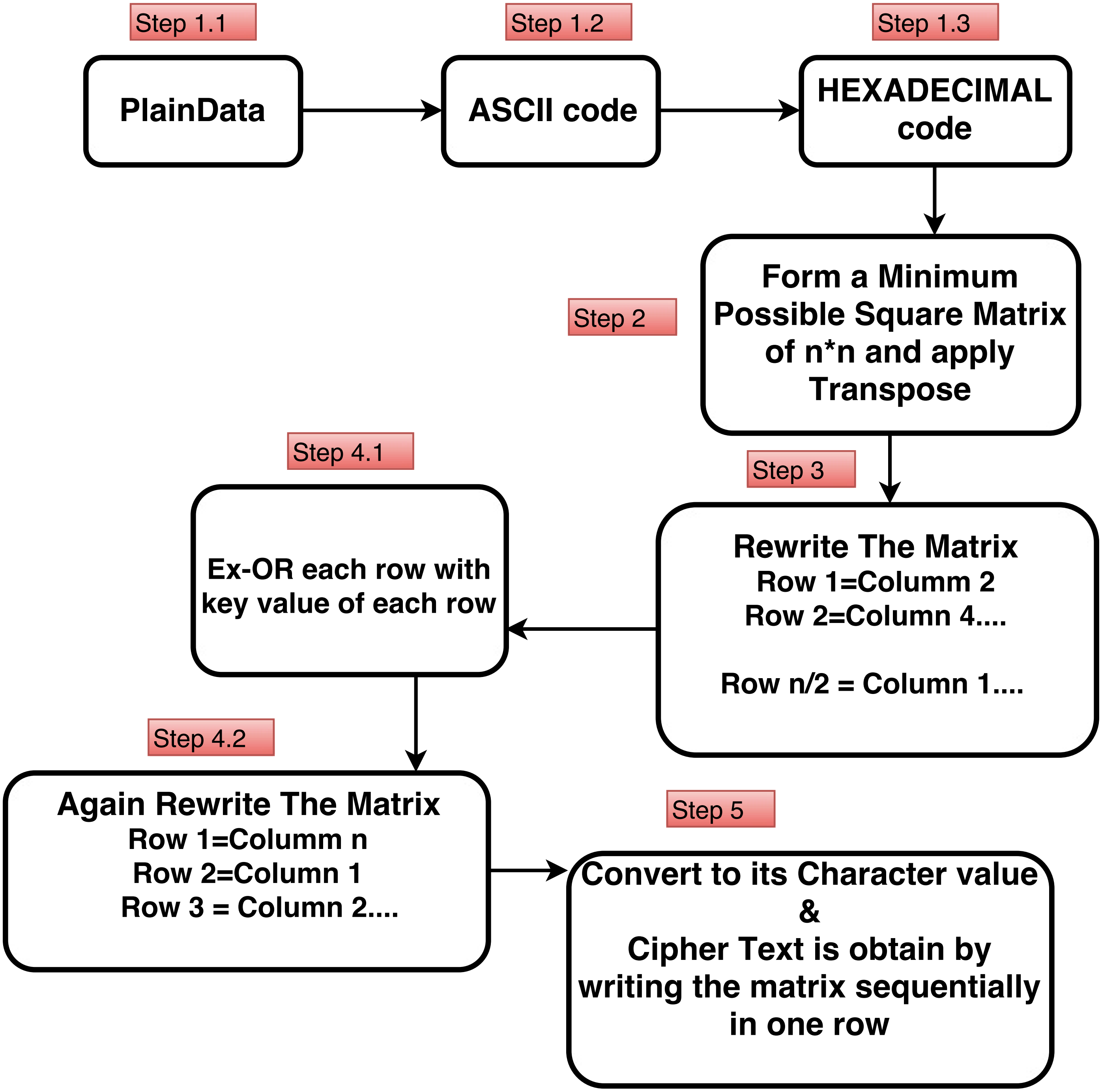


Figure 3.1: Propsed Encryption Algorithm

Decryption Algorithm

(1) (a) Convert the encrypted text into ASCII code.

Encrypted Text: gA@elv@TmG

(b) Form a square matrix A of size S such that (S*S = N)

76	16	47	05
70	16	44	6F
65	16	5B	65
6C	16	40	05

(2) Make a new matrix by writing from 2 rows on-wards to the last row (2,3 .. n) and at-last add the first row and then .. Rewrite the values by reading values row-wise – writing values (into a new matrix) column wise.

70	65	6C	76
16	16	16	16
44	5B	40	47
6F	65	05	05

(3) By using S random key which is generated earlier, **EX-OR** each row of the matrix.

53	46	4F	55
24	24	24	24
56	49	52	55
4E	44	24	24

(4) Make a new matrix by writing firstly $((n\text{-}1)/2 + 1)^{th}$ row then 1st row then $((n\text{-}1)/2 + 2)^{th}$ row then 2nd and so on.. Rewrite the values by reading values row wise – writing the values (into a new matrix) column wise .

56	53	4E	24
49	46	44	24
52	4F	24	24
55	55	24	24

(5) (a) Transpose the Matrix (A = A^T)

(b) Convert the ASCII code into equivalent character value.

(c) **Plain Text/Message** is generated by writing the values sequentially in one row.

Decrypted result: VIRUS FOUND

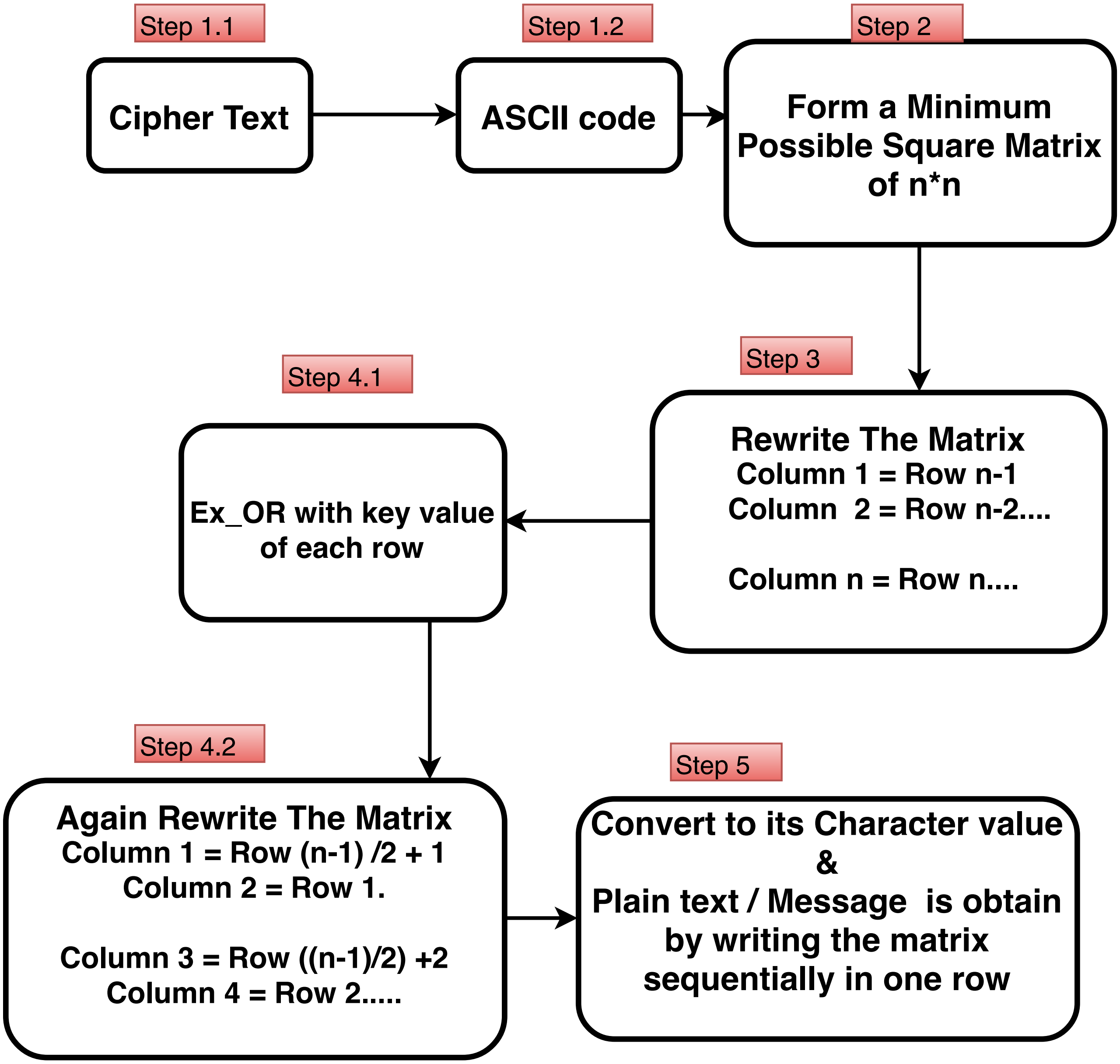
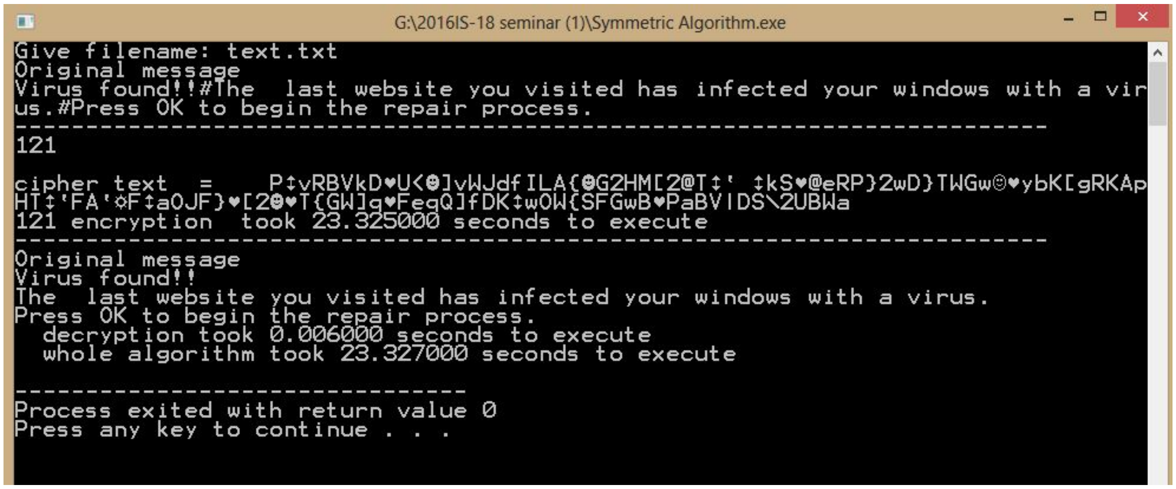

Step 1.1
Cipher Text
Step 1.2
ASCII code
Step 2
Form a Minimum Possible Square Matrix of n*n
Step 3
Rewrite The Matrix
Column 1 = Row n-1
Column 2 = Row n-2....
Column n = Row n....
Step 4.1
Ex_OR with key value of each row
Step 4.2
Again Rewrite The Matrix
Column 1 = Row (n-1) /2 + 1
Column 2 = Row 1.
Column 3 = Row ((n-1)/2) +2
Column 4 = Row 2.....
Step 5
Convert to its Character value
&
Plain text / Message is obtain by writing the matrix sequentially in one row

Figure 3.2: Propsed Decryption Algorithm

Chapter 4

Experiments and results

Enhanced Symmetric Algorithm



```
Give filename: text.txt
Original message
Virus found!!#The  last website you visited has infected your windows with a vir
us.#Press OK to begin the repair process.
-------------------------------------------------------------------------
121

cipher text  =    P↕vRBVkD♥U<☻]vWJdfILA{☻G2HM[2@T↕'  ↕kS♥@eRP}2wD}TWGw☺♥ybK[gRKAp
HT↕'FA'☼F↕aOJF}♥[2☻♥T{GW]q♥FeqQ]fDK↕wOW{SFGwB♥PaBV|DS\2UBWa
121 encryption  took 23.325000 seconds to execute
-------------------------------------------------------------------------
Original message
Virus found!!
The  last website you visited has infected your windows with a virus.
Press OK to begin the repair process.
  decryption took 0.006000 seconds to execute
  whole algorithm took 23.327000 seconds to execute

--------------------------------
Process exited with return value 0
Press any key to continue . . .
```

Figure 4.1: Output: Enhanced Symmetric Algorithm

This section discusses the various experiments pertaining to the proposed algorithm.

4.1 Experiment design

4.1.1 Experiment 1

4.1.1.1 Time Analysis for Encryption

File size(Bytes)	Encryption time(msec)
4	4464
13	7874
27	7974
35	8134
61	8569
120	9300
145	9800
308	10350
540	12145

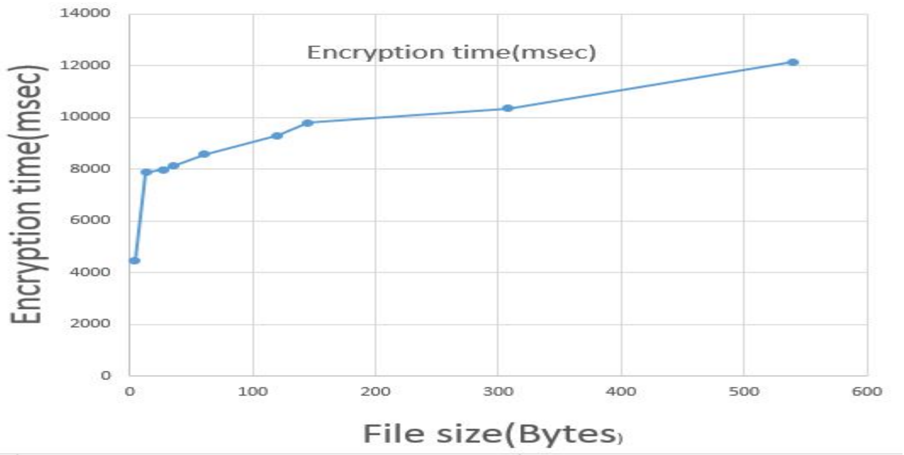


Figure 4.2: Time Analysis for Encryption

4.1.1.2 Results and discussion

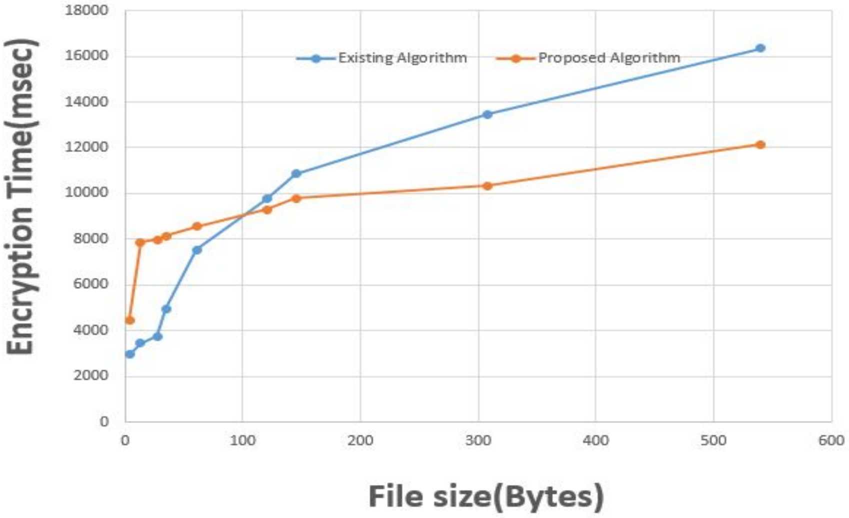


Figure 4.3: Time Comparision of Encryption

Proposed Algorithm has 25% of outcomes than previous methods on the Encryption Phase.

4.1.2 Experiment 2

4.1.2.1 Time Analysis for Decryption

File size(Bytes)	Decryption time(msec)
4	215
13	260
27	370
35	429
61	612
120	915
145	1019
308	1227
540	1437

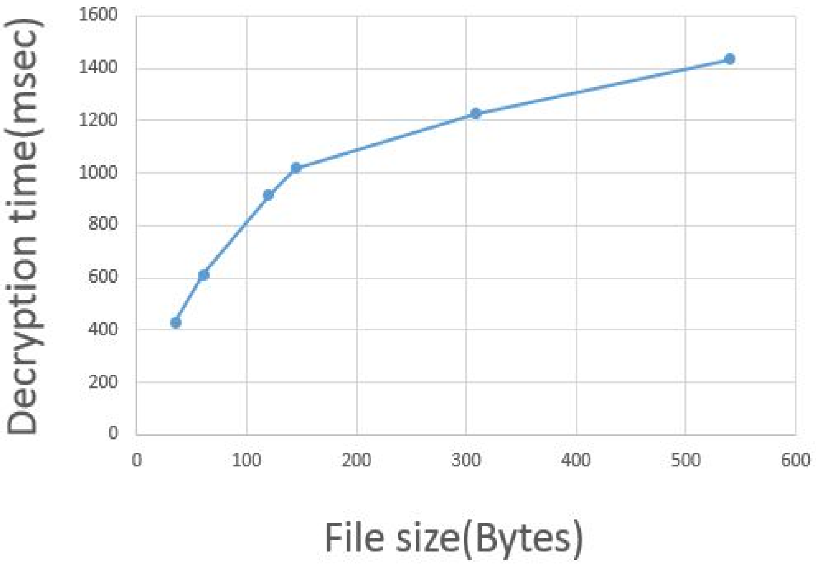


Figure 4.4: Time Analysis for Decryption

4.1.2.2 Results and discussion

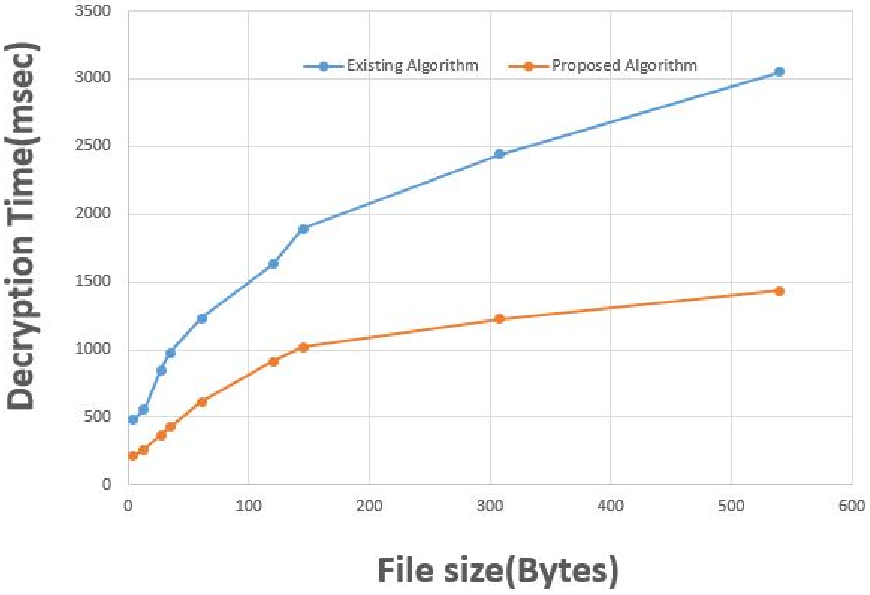


Figure 4.5: Time Comparision of Decryption

Proposed Algorithm has 52% of outcomes than previous methods on the Decryption Phase.

4.1.3 Experiment 3

4.1.3.1 Total Execution Time Analysis

File size(Bytes)	Total time(msec)
4	4714
13	8234
27	8378
35	8593
61	9237
120	10285
145	10845
308	11615
540	13613

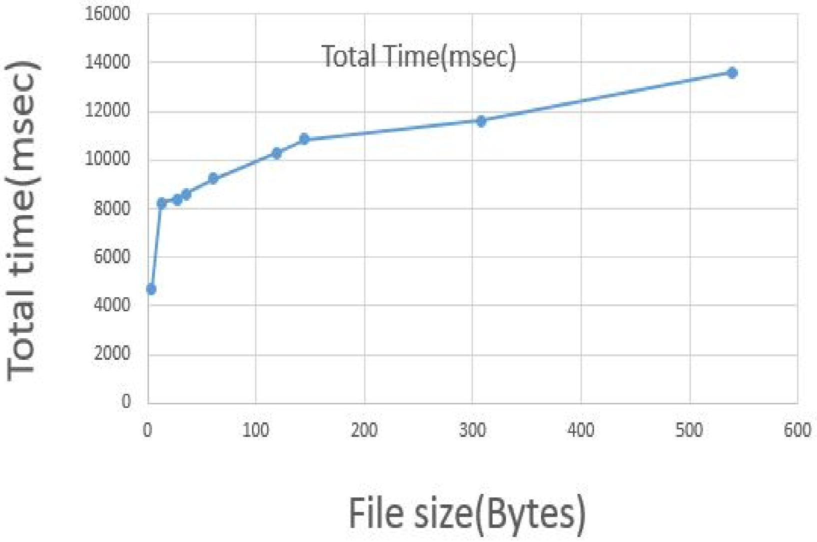


Figure 4.6: Total Execution Time Analysis

4.1.3.2 Results and discussion

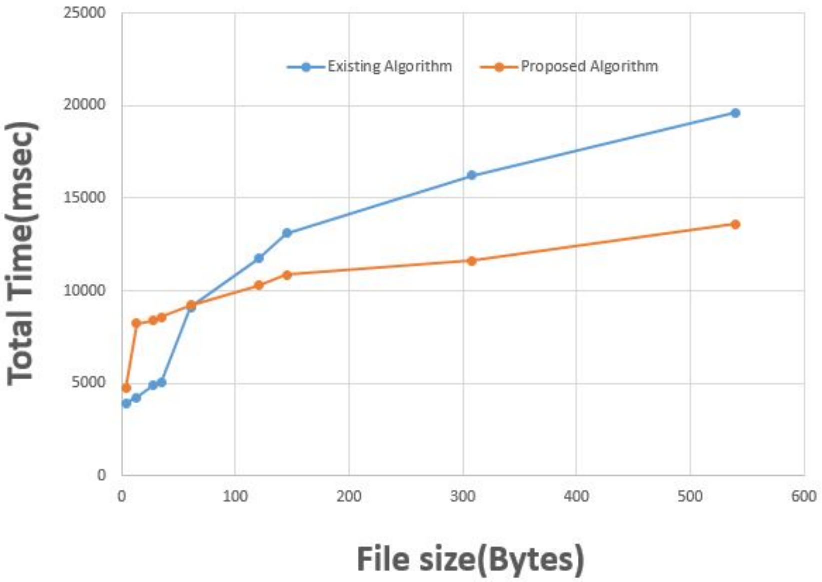


Figure 4.7: Time Comparision of Total time

Proposed Algorithm has 30% of outcomes than previous methods.

Chapter 5

Conclusion

5.1 Conclusion

The cloud computing environment Security and Privacy are important roles in storing data in that location. So many researchers are work in that area. Cryptographic techniques are used to provide secure communication between the user and the cloud. This thesis proposed enhanced symmetric-based encryption algorithm for secure data storage in cloud storage. By applying this encryption algorithm, the user ensures that the data is stored only on secured storage and it cannot be accessed by administrators or intruders.

Bibliography

[1] U. Hoyer and H. Obel. Guide on saas vs paas and iaas — linkedin. `https://www.linkedin.com/pulse/guide-saas-vs-paas-iaas-ulrik-hoyer-hansen-obel/`. (Accessed on 05/08/2018).

[2] Qi Zhang, Lu Cheng, and Raouf Boutaba. Cloud computing: state-of-the-art and research challenges. Journal of internet services and applications, 1(1):7–18, 2010.

[3] Mark I Williams. A quick start guide to cloud computing: moving your business into the cloud. Kogan Page Publishers, 2010.

[4] Chunye Gong, Jie Liu, Qiang Zhang, Haitao Chen, and Zhenghu Gong. The characteristics of cloud computing. In Parallel Processing Workshops (ICPPW), 2010 39th International Conference on, pages 275–279. IEEE, 2010.

[5] Saurabh Singh, Young-Sik Jeong, and Jong Hyuk Park. A survey on cloud computing security: Issues, threats, and solutions. Journal of Network and Computer Applications, 75:200–222, 2016.

[6] Ronald L Krutz and Russell Dean Vines. Cloud security: A comprehensive guide to secure cloud computing. Wiley Publishing, 2010.

[7] Nils Gruschka and Meiko Jensen. Attack surfaces: A taxonomy for attacks on cloud services. In Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on, pages 276–279. IEEE, 2010.

[8] Oscar Dieste, Natalia Juristo, and Mauro Danilo Martínez. Software industry experiments: A systematic literature review. In Proceedings of the 1st International Workshop on Conducting Empirical Studies in Industry, pages 2–8. IEEE Press, 2013.

[9] Lifei Wei, Haojin Zhu, Zhenfu Cao, Xiaolei Dong, Weiwei Jia, Yunlu Chen, and Athanasios V Vasilakos. Security and privacy for storage and computation in cloud computing. Information Sciences, 258:371–386, 2014.

[10] Subashini Subashini and Veeraruna Kavitha. A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications, 34(1):1–11, 2011.

[11] Jose Luis Lucas-Simarro, Rafael Moreno-Vozmediano, Ruben S Montero, and Ignacio M Llorente. Scheduling strategies for optimal service deployment across multiple clouds. Future Generation Computer Systems, 29(6):1431–1441, 2013.

[12] Deyan Chen and Hong Zhao. Data security and privacy protection issues in cloud computing. In Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on, volume 1, pages 647–651. IEEE, 2012.

[13] Siani Pearson. Privacy, security and trust in cloud computing. In Privacy and Security for Cloud Computing, pages 3–42. Springer, 2013.

[14] Eric Bauer and Randee Adams. Reliability and availability of cloud computing. John Wiley & Sons, 2012.

[15] Hongji Yang. Software reuse in the emerging cloud computing era. IGI Global, 2012.

[16] Kadam Prasad, Jadhav Poonam, Khupase Gauri, and NC Thoutam. Data sharing security and privacy preservation in cloud computing. pages 1070–1075, 2015.

[17] Nesrine Kaaniche and Maryline Laurent. Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms. Computer Communications, 111:120–141, 2017.

[18] N Saravana Kumar, GV Rajya Lakshmi, and B Balamurugan. Enhanced attribute based encryption for cloud computing. Procedia Computer Science, 46:689–696, 2015.

[19] Mark D Ryan. Cloud computing security: The scientific challenge, and a survey of solutions. Journal of Systems and Software, 86(9):2263–2268, 2013.

[20] Abdul Salam, Zafar Gilani, and Salman Ul Haq. Deploying and Managing a Cloud Infrastructure: Real-World Skills for the CompTIA Cloud+ Certification and Beyond: Exam CV0-001. John Wiley & Sons, 2015.

[21] Stefano MPC Souza and Ricardo S Puttini. Client-side encryption for privacy-sensitive applications on the cloud. Procedia Computer Science, 97:126–130, 2016.

11

ORIGINALITY REPORT

11%	8%	3%	6%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to ABV-Indian Institute of Information Technology and Management Gwalior Student Paper	4%
2	scholarworks.wmich.edu Internet Source	4%
3	Submitted to University of Technology, Sydney Student Paper	<1%
4	calhoun.nps.edu Internet Source	<1%
5	Shweta Kaushik, Charu Gandhi. "Cloud data security with hybrid symmetric encryption", 2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT), 2016 Publication	<1%
6	N. Veeraragavan, L. Arockiam, S. S. Manikandasaran. "Enhanced encryption algorithm (EEA) for protecting users' credentials in public cloud", 2017 International	<1%

	Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET), 2017 Publication	
7	Submitted to Middlesex University Student Paper	<1%
8	elib.uni-stuttgart.de Internet Source	<1%
9	addtech.com.au Internet Source	<1%
10	Submitted to Kingston University Student Paper	<1%
11	uwspace.uwaterloo.ca Internet Source	<1%
12	amath.colorado.edu Internet Source	<1%
13	www.dtic.mil Internet Source	<1%
14	efe.com.vn Internet Source	<1%
15	eprints.nottingham.ac.uk Internet Source	<1%
16	dspace.lboro.ac.uk Internet Source	<1%

17	"Big Data Analytics", Springer Nature, 2018 Publication	<1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	Off		