Title

A project report submitted as part of the requirements for the award of the degree of

Bachelor in Technology (B.TECH.)

in

Computer Science and Engineering

by

RAHUL PADOLE

MIS No:112015095

Semester: IV

Computer Science and Engineering

Indian Institute of Information And Technology Pune

Near Bopdev Ghat, Kondhwa Annexe, Yewalewadi, Pune, Maharashtra 411048

APRIL 2022

BONAFIDE CERTIFICATE

This is to certify that the project report entitled **"Enhancing Security in Cloud Computing"** submitted by **RAHUL PADOLE** bearing the **MIS No:112015095**, in completion of his project work under the guidance of **Dr. Ritu Tiwari maam** is accepted for the project report submission in partial fulfillment of the requirements for the award of the degree of Bachelor of Technology in Computer Science and Engineering in the Department of Computer Science and Engineering , Indian Institute of Information Technology, Pune, during the academic year 2021-22.

Project viva-voce held on 29/10/2022

Internal Examiner **External Examiner**

ACKNOWLEDGEMENT

I would like to thank the people who helped me directly and indirectly in the completion of this project work.

First and foremost, I would like to express my gratitude to our beloved director, **Dr. Anupam Shukla**, for providing his kind support in various aspects.

I would like to express my gratitude to my project guides **Dr. Sanjeev Sharma**, Assistant Professor, Department of CSE, for providing excellent guidance, encouragement, inspiration, constant and timely support throughout this M.Tech project.

I would like to express my gratitude to the head of department **Dr. Tonmoy Hazra**, Head of Department CSE, for providing his kind support in various aspects.

who gave me the golden opportunity to assemble this wonderful report on "Security in Cloud Computing". I would also like to extend my gratitude my friends who help me a lot in finishing this report within the limit.

Abstract

In the twenty-first century, scientific computing has progressed from a fixed to a distributed work environment. The use of cloud computing is growing at an exponential rate nowadays. Cloud Computing (CC) is a current trend that allows access to business applications from anywhere by simply connecting to the Internet. Cloud computing provides dynamically virtualized and scalable resources based on a network built with a large number of distributed computers rather than local computers or remote servers. Meanwhile, the use and application of Cloud Computing is rapidly expanding, resulting in the creation of a slew of new IT industries by combining traditional computing technologies. Data suggests that switching to Cloud Computing institutions reduces annual expenditure and maintenance to a greater extent. However, there are a variety of obstacles that come with the various benefits of Cloud Computing. Among these are security concerns. This report focuses on researching and analyzing Cloud Computing technology in terms of concept and security, as it is still a developing technology with great convenience and portability for exchanging information over the Internet via various platforms. Furthermore, because cloud computing is so reliant on the global Internet, it is becoming a primary target for Internet threats such as malware or viruses, technical vulnerability, and negligent behavior patterns. As a result, the report also addresses the most pressing security and privacy concerns in cloud computing. Finally, the report suggests potential solutions and improvements to technical issues, as well as future developments

Keywords : Cloud Computing, Security, Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA), Hybrid Algorithm, Hash functions, Secure Hash Algorithm (SHA256), Encryption, Cryptography, availability, confidentiality, integrity, authorization, and non-repudiation.

TABLE OF CONTENTS

List of Figures

Chapter 1

Introduction

1.1 Overview Of Cloud Computing

As a result of the internet's tremendous success in recent years, computing resources are now more freely available. As a result, Cloud Computer, a novel computing idea, became a reality. Cloud computing is defined as a distributed architecture for providing on-demand computer resources and services by centralising server resources on a scalable platform. Cloud computing, or the provision of computer resources as a service, is a technological revolution that allows for flexible IT use at a low cost and on a pay-per-use basis. Cloud computing's main purpose is to maximise overall computer capacity. It has established a new paradigm that allows users to dynamically save or construct applications and access them from anywhere and at any time via the Internet. Traditional service providers must take two different methods in the Cloud Computing world. These are infrastructure and service providers. Infrastructure providers are in charge of managing cloud platforms and leasing resources on a need-to-know basis. Service providers rent resources from infrastructure providers to serve end customers. Cloud computing has attracted major corporations such as Google, Microsoft, and Amazon, and is widely recognised as having a substantial impact on today's IT business. Since the 1980s, information technology has seen another major shift, this time from mainframe to client-server paradigm. Many well-known IT organisations have used and applied Cloud Computing research and development in the past due to its commercial importance and breakthrough technology. Data from local repositories is transferred to a remote data centre when a customer chooses to use cloud services.

Cloud service providers' services can be used to access or manage data in remote places.

This indicates that data must be transferred to a remote server through the internet in order for a user to store or process it in the cloud. This data processing and storage must be done with considerable caution to avoid data breaches. Despite the fact that cloud computing has created tremendous opportunity for today's IT industry, there are still a number of issues to be addressed.

1.2 Identifying the Problem

Data saved in local repositories is transferred to a remote data centre when a consumer chooses cloud services. Cloud service providers' services can be used to access or manage data in remote places. This indicates that data must be communicated to a remote server via a channel in order for a user to store or process it in the cloud (internet). These are some of the most important issues in cloud computing:

Privacy: The host company can access the user data with or without authorization. At any time, the service provider has access to the data stored in the cloud.

Security: They could change or even erase data by accident or on purpose. Third-party storage and security are involved in cloud-based services. Can one assume that a cloud-based company will protect and secure one's data if they use their services for a low or no cost? They may disclose user information to third parties. Security is a serious threat to the cloud.

Abuse: When providing cloud services, it should be ensured that the client is not purchasing cloud computing services for nefarious purposes. In 2009, a banking Trojan used the popular Amazon service illegally as a command-and-control channel to distribute software updates and malicious instructions to PCs infected with the malware. As a result, hosting companies and servers must take appropriate precautions to address these issues.

Recovery of lost data in contingency: Before subscribing any cloud service provider goes through all norms and documentations and checks whether their services match your requirements and sufficient well-maintained resource infrastructure with proper upkeep. Once you subscribe to the service you almost hand over your data into the hands of a third party. If you are able to choose a proper cloud service then in the future you don't need to worry about the recovery of lost data in any contingency. Malicious users can gain access to transmitted data in the cloud by intercepting the user-to-remote location connection. He can also hack into users' accounts and gain access to sensitive information by opening a malicious account with the same service provider (via the virtualized infrastructure provided by cloud computing). Because cloud computing provides a wide range of services to a diverse set of users (nave, expert, malicious, etc.), the risk of data loss when working in cloud computing systems is enormous.

1.3 Existing Technology

RSA algorithm is the most widely used public key cryptography algorithm for encryption and decryption by many vendors today. This is the first generation algorithm that was used for providing data security. It can be used to encrypt a message without the need to exchange a secret key separately. The RSA algorithm can be used for both public key encryption and digital signatures. Its security is based on the difficulty of factoring large integers. Party A can send an encrypted message to party B without any prior exchange of secret keys. A just uses B's public key to encrypt the message and B decrypts it using the private key, which only he knows. RSA can also be used to sign a message, so A can sign a message using their private key and B can verify it using A's public key

1.4 Aim

This report aims to identify security challenges for cloud computing adoption, as well as real-world solutions for challenges that lack proper mitigation strategies, as identified through a literature review.

1.5 Objectives

1.Identify existing cloud computing security issues and their solutions in the literature.

2.Identify the challenges for which no mitigation strategies have been defined.

3.Collect solutions/guidelines/practices from organisations in response to a challenge that has more references but no mitigation strategies proposed (identified in literature).

4.List solutions/practices/guidelines to the cloud computing security challenge that has no identified mitigation strategies.

1.6 Motivation

Most of the people uses social media like Facebook (Meta), Instagram, Snapchat, Twitter, etc. People there share their personal data resource such as photos, video, and especially texts. These resources are credited as end-to-end encrypted ie. anyone except the sender and receiver cannot access the information but recently a spyware named "PEGASUS" was able to read text, tracking calls, collecting passwords, location tracking, accessing the target device's microphone and camera, and harvesting information from apps. Again in April 2021, Facebook was booked for data breaching of the users.Data from 533 million people in 106 countries was published on a hacking forum. Such Incidence made me curious how my data is treated by companies and how secure is my data. And what can we do in order to have secure data exchange.

Chapter 2

Background Of Cloud Computing

2.1 History

In the 60's John McCarthy said that "computation may someday be organized as a public utility". This is just a concept attached to cloud computing. Development of ARPANET (Advance Research Projects Agency Network) by J.C.R.Licklider in 1960's which helped to connect (for sharing, transferring, etc.) In the 80's, companies realized that servers based on normal computers could be installed at lower cost than mainframes. Also, this gave users a sense of greater control over their actions. At the finish of the dot.com bubble, finish of the 90's, normally all data centres were using less than 10 percent of their capabilities. At 1999 Salesforce.com began to delivery services to enterprises by their own website and pioneered the concept of software as a service. In 2002 Amazon launched Amazon Web Services (AWS), a suite that included storage, computation and other services. In 2006 Amazon launched Elastic Compute Cloud (EC2) to small companies and let users run their own computer applications in the cloud. In 2008, Eucalyptus was launched, being the first open-source AWS API compatible platform for deploying private clouds. In 2009 Google began to offer enterprise applications based in browser as Google Apps On July 29, Yahoo, HP, and Intel published an associated research program in U.S.A, Germany and Singapore, targeting on building 6 data centres as research platform. In 2008,, Microsoft created Microsoft Azure which is a Cloud Computing platform and infrastructure, offering applications and services establishment, implementation and management via Microsoft data centres (Microsoft Azure, 2008). In July 2010, NASA, Rackspace, AMD, Intel and Dell proclaimed an open-source project, “OpenStack”. Soon, IBM and Oracle announced their cloud “IBM Smart Cloud” and “Oracle Cloud” in 2011 and 2012 (Wikipedia,2015).

2.2 Definition

The word cloud it’s used to describe this kind of computing because of the metaphor used for describe networks, a cloud that underlie all the technology that is above and the user don’t know it exists and don’t need to know it. For the most famous encyclopedia in Internet, Wikipedia, cloud computing is: “Computation, software, data access, and storage services that do not require end-user knowledge of the physical location and configuration of the system that delivers the services” **NIST (National Institute of Standards and Technology)** denes cloud computing as follows: Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of conjurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction”.

2.2.1 Benefits of CC

Reduced Cost: Because cloud technology is implemented incrementally (step by step), organisations save money overall. Increased Storage: Massive amounts of data can be stored. Flexibility:r It allows for the outsourcing of an entire organisational segment or a portion of it. Greater mobility: Information can be accessed whenever and wherever it is needed. Shift in IT focus: Organizations can concentrate on innovation rather than worrying about maintenance issues such as software updates or computing issues. According to an ITC survey conducted in 2008 and 2009, many companies and individuals are noticing that Cloud Computing is proving to be beneficial when compared to traditional computing methods.

2.2.2 Characteristics of Cloud Computing

On-demand self-services: Users can provision, monitor, and manage computing resources as needed. Broad network access: Computing services are typically delivered through standard networks and heterogeneous devices. Elasticity that responds quickly: Computing services should have IT resources that can scale out and in on an as-needed basis. Resource pooling: Typically, computing services are delivered via standard networks and heterogeneous devices.

2.2.3 Features Of Cloud Computing

Firstly, the large-scale deployment draws the attention, in terms of statistic, worldwide IT companies such as like Amazon, Apple, Cisco, Google, HP, Lenovo, Microsoft, IBM, etc. have implemented a large number of severs for Cloud Computing. Among them, Google has over 1 million servers; Amazon, IBM, Microsoft and Yahoo has hundreds of thousands of servers, which ensures the unpredictable computation capability for the users around the world.

Secondly, the benefit of virtualization is significant. It supports users access from anywhere on any terminal. All the requested resources come from the "Cloud" instead of tangible entities.

Thirdly, the "Cloud" is a highly reliable resource. It is more credible to use the "Cloud" than local computers. Meanwhile, the "Cloud" is versatile, because it does not focus on certain application. Service on demand is another critical feature of the "Cloud". The cost performance is incredibly high. So, users can completely enjoy the perfect services of the "Cloud" regardless of high level of consumption and long period of computing.

2.3 Cloud architecture

Cloud computing is becoming increasingly important as a result of the expansion of virtualization. However, current cloud computing cannot support a complex enterprise environment. The cloud architecture can be divided into four layers based on an analysis of existing cloud products.

2.3.1 Presentation layer

This layer is used by many cloud computing data centres to display the content that users require as well as the experience of services in a user-friendly interface. Primarily through the use of five technologies: HTML, JavaScript, CSS, Flash(frequently applied RIA technology), Silverlight (this RIA technology is from IT giant Microsoft.)

2.3.2 Intermediate layer

This layer serves as a link between the previous and subsequent layers. It provides multiple services in the downstream infrastructure layer that owns resources, such as cache service and REST service, which can supply both the presentation layer and is referred to by primarily five technologies: Representational State Transfer : is a protocol that is commonly used with HTTP. Multiple lesseesis: accomplished by assigning a single application sample to a number of organisations. Parallel processing: to process a large amount of data, a massive X86 cluster is required to achieve a massive scale of parallel processing. Application server: this is a cloud-based optimised server. Distributed cache: it speeds up response time. ”Memcached” is the most well-known model.

2.3.3 Infrastructure layer

It is used to protect computing and storage resources for users in the upstream Intermediate layer. Four technologies are commonly used: Virtualization: It can achieve the goal of running multiple virtual machines. VMware, ESX, and the open source Xen virtual machine technologies are all full-fledged X86 virtual machine technologies. Distributed storage: It can handle a large amount of data while keeping it manageable. Relational database: an optimised original relational database designed to meet the requirements of extensibility and management. NoSQL: it is used to dispose of certain targets that relational databases cannot handle.

2.3.4 Management layer

The services on this layer are vertical and provide multiple management or maintenance technologies for the three layers mentioned above, in accordance with these aspects: Account management: It provides a secure and convenient environment. SLA monitoring: when monitoring the services and applications of virtual machines at various layers. Security management protects data, applications, accounts, and other IT resources from attacks by hackers and malware. Management of operations and maintenance: This technology focuses on implementing specialisation and atomization to the operating and maintenance processes in order to reduce costs.

2.4 Deployment of Clouds

To fully comprehend the cloud's operation mechanism, it is necessary to first introduce the various types of deployment. The following are some of the most common ways to utilize the cloud.

2.4.1 Private cloud

A private cloud is designed for a single client or organisation to effectively control data, security, and service quality. Private resources are the core value of private cloud. A private cloud,is typically built behind a firewall, making it more secure than a public cloud. Furthermore, a private cloud has the advantage of maintaining data management and safety regulations without interfering with the management process, whereas a public cloud will have a significant impact on it (Microsoft, 2013).

2.4.2 Public cloud

The term ”public cloud” usually refers to the cloud provided by third-party cloud service providers and accessed via the Internet. In comparison to other storage methods, it provides a reliable and secure data storage centre. Local computers may be physically damaged, infected with viruses or hackers, or subjected to malicious action by someone with access to the computer.Besides, due to the large number of users in public cloud, it is quite convenient to share files or storage with others as well as access giant number of public resources. (Microsoft, 2013).

2.4.3 Hybrid cloud

A hybrid cloud is a collection of multiple clouds that exist as separate entities while also being linked together. As a result, combining a public cloud and a private cloud provides the ideal solution to this contradictory situation: hybrid cloud. It has the security features of a private cloud, preserving internal critical data in local data center, and it can also use computing resources from the public cloud to complete work efficiently and effectively.

2.5 Service Models

Many service models have been proposed for delivering cloud computing services, but three are particularly popular: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). These models are also referred to collectively as the SPI model. In the following subsections, we will go over the SPI model and a more generalised model, XaaS.

2.5.1 Software as a Service (SaaS)

SaaS refers to delivering the services of applications and programs installed on distant servers deployed over the internet that run behind the firewall on your local area network or personal computer. SaaS users do not have control over the cloud infrastructure.Salesforce.com, Rackspace, and SAP Business ByDesign are examples of SaaS providers.

2.5.2 Platform as a Service (PaaS)

PaaS is a type of SaaS that differs from SaaS, PaaS provides a development environment that includes a programming language, tools, and an operating system that hosts both completed and in-progress cloud applications. It enables developers to create and deploy applications without having to worry about the number of processors or memory requirements of the applications. PaaS providers include Google App Engine, Microsoft Windows Azure, and Force.com.

2.5.3 Infrastructure as a Service (IaaS)

IaaS refers to the provision of virtualized resources such as processing, storage, networking, and other computing resources on-demand via virtual machines (VMs). IaaS makes extensive use of virtualization to ad hoc integrate or decompose physical resources to meet the resource demand of an unpredictable workload by establishing independent VMs that are isolated both from the underlying hardware and from other VMs. As a result, it is also known as platform virtualization as a service. It aims to transform application software architecture so that multiple instances from different cloud customers can run on the same application. IaaS providers such as Amazon EC2, GoGrid, and Flexiscale are examples.

2.5.4 Anything as a Service (XaaS)

Aside from SPI models, numerous service models have been proposed, and they are collectively referred to as Anything as a Service, or XaaS. Hardware as a Service (HaaS), Data Storage as a Service (DaaS), Commerce as a Service (CaaS), Virtual Cluster as a Service (ViteraaS), Description Model as a Service (DEMODS), Analytics as a Service (AaaS), Testing as a Service (TaaS), Web Service Testing as a Service (WSTaaS), Information Technology as a Service (ITaaS), Big Data as A few of these models are hybrids of two or more layers of an SPI model that add functionality to the cloud computing environment.

Chapter 3

Typical Utilization Of Cloud Computing

Technologies that are attached to cloud Computing.

3.1 Web Services

It‘s explained before that cloud computing it‘s based in the offer of services, Normally two applications written in different languages and executed in different operating systems are not able to communicate between them, but exists a group of protocols and standards for exchanging information between different applications, no matter in which language are written or in which operating system is running. XML, SOAP, WSDL, UDDI, WS-Security.

3.2 Cloud computing security

It's a set of policies about the security in the cloud focused on computer, network and mostly information protection. These policies are about: 1. Data of one user have be totally isolate from data of another. 2. Access to data have to be always available for the users, 3. All the services delivered in the cloud have to be secure and data have to be encrypted.. 4. Virtualization for O.S, install one O.S inside of another one by using a virtual machine.With this option we can run different O.S in the same machine.

3.3 Data Centers

Data centres are typically used by businesses that require a large amount of data storage and processing. Data Centers must have a plethora of security policies in place, as well as redundancies in data, power, and communication supply.

3.4 Virtualization of computers

Virtualization is an abstraction of the resources of a machine between the hardware and the operating system, making a virtual version of a resource being possible to share it. Virtualization also allows building so-called sandboxes. Sandboxes assure a higher degree of security and reliability by providing a mechanism to run programs safely.

3.5 Green IT

It's the fashion to maximize the efficiency of the computational resources to minimize the environmental impact. Also includes the deployment of ecologic products. Some technologies included in Green It are cloud computing, grid and data centers.

3.6 Grid

Infrastructure that integrates different systems from different institutions like if it was only one (computers, networks, databases, etc) allowing the collective use. This is the difference with cloud computing, because in cloud all the infrastructure is managed by one organization although each cloud can dynamically use others clouds too.

3.7 Virtual Appliance

It's a virtual machine compressed into a file that can be run inside the host using a programme like Xen or VmWare. In most cases, this VM is created with an operating system and some applications installed for one of the following purposes: - Virtual machines. - Firewalls and routers - Observation.

3.8 Load Balancing

It is capable of distributing work processes evenly across two or more computers, allowing resources to be used more efficiently and thus increasing performance and availability. A load balancer can automatically deal with varying amounts of work capacity by adapting its distribution decisions based on when a request is made.

3.9 Internet of Things

The core value of the Internet of Things is still an Internet technology that extends and expands its network. In the application field, cloud computing is always combined with the Internet of Things to create an inter-connected, massive data provided and integrated in the service platform. For example, applied computer technology, network communication technology, video analyzing technology, access control technology, sensor technology, wireless technology, database technology, cloud storage, and cloud computing.

3.10 Cloud storage

Cloud Storage entails aggregating massive and diverse storage devices in the network while implementing cooperative work that provides data storage and business access using cluster applications, network technology, or distributed file systems. When dealing with large amounts of data storage and management, the cloud computing system necessitates a large number of storage devices; thus, the cloud computing system becomes a cloud storage system. As a result, the primary benefit of cloud storage is data storage and management. This new storage solution provides access via the Internet at any time and from any location.

3.11 Cloud gaming

Cloud gaming is a type of game that is based on cloud computing. With the cloud gaming mode, all games run on the server end, and game graphics that have already been rendered are sent to users via network transmission. Clients do not need to buy high-end CPUs and graphics cards to play games; they only need basic video decompression capability.

3.12 Cloud Computing Platform

3.12.1 Google Apps

It‘s an office suite offered as a service (SaaS) that everybody can use through a web server. Includes the next applications: Gmail, Google Docs, Google Groups, Google Sites.

3.12.2 Google App Engine

It‘s a platform for the deployment and hosting of web applications (PaaS). These applications are hosted and running in Google Datacentres. It permits to deploy programs in Java (and all technologies that use JVM as Ruby) and Python, and the usage of different frameworks.

3.12.3 Amazon EC2

It's a service (IAAS) that allows users to rent and run any virtual image with any software installed. It's a scalable server, users can ask for more capacity and the response is given in some minutes. It's completely compatible with other Amazon services like S3 and brings the possibility of paying for hours or for running instances. It offers 10 different kinds of virtual machines with different processors

3.12.4 MICROSOFT

Microsoft is also in the cloud, offering software plus services, which is a variation that consists of some services hosted in the cloud . This provides the user with benefits such as the ability to run applications online while keeping data on the client's personal computer. The services offered are centred on communication. They provide: Microsoft Exchange Online, SharePoint Online, Office Communications Online, Microsoft Forefront .

.

Chapter 4

Problem Statement

4.1 Problem Statement

When saving data in the cloud, it is important to ensure that the data is correctly stored and can be retrieved later. Because the amount of data saved by the cloud for a client might be large, retrieving all of it is impossible (and potentially very expensive) if the goal is only to ensure that it is stored correctly. As a result, the need for building Encryption Algorithms For Cloud Security models/protocols is pressing.

4.2 A. Cryptography

It is a science that is used to protect sensitive data. Cryptography's primary security service is confidentiality, which renders data invisible to unauthorised users. The following are cryptosystem components:

1. Plaintext: Data in its original form, to be protected during transmission and storage. Cipher text is the unreadable form of plaintext that results from the encryption operation. Encryption Algorithm: A mathematical procedure used to transform plaintext to cypher text. 2. Decryption Algorithm: It reverses the encryption algorithm, converting cypher text to plaintext. 3. Encryption Key: This is a value utilised by the sender in conjunction with the algorithm to transform plaintext to encrypted text. Decryption Key: This is a value utilised by the receiver in conjunction with the algorithm to convert cypher text to plaintext.

4.3 B. Encryption Algorithms For Cloud Security.

Encryption algorithms have vital role in the field of cloud security. Many algorithms are available for cloud security. Most useful algorithms for cloud security are discussed below.

4.3.1 1. Data Encryption Standard(DES)

The National Institute of Standards and Technology's Data Encryption Standard (DES) is a symmetric-key block cypher (NIST). It encrypts and decrypts with a single key (secret key). It works with 64-bit data blocks and a 56-bit key. The round key has a size of 48 bits. Two permutations (P-boxes) and sixteen Feistel rounds make up the DES algorithm.

4.3.2 2. Advanced Encryption Standard (AES)

The National Institute of Standards and Technology (NIST) developed AES, a symmetric-key block encryption (NIST). AES is the most widely used symmetric encryption algorithm. It does computation on bytes rather than bits, and treats a plaintext block of 128 bits as 16 bytes. These 16 bytes are organised into four columns and four rows for matrix processing. It uses substitutions and permutations to act on the full data block. The number of transformation rounds required in the encryption process is specified by the key size for an AES cypher. Possible keys and number of rounds are as following: 10 rounds for 128-bit keys. 12 rounds for 192-bit keys. 14 rounds for 256-bit keys.

4.3.3 3. Rivest-Shamir-Adleman(RSA)

RSA is a public key cypher invented in 1977 by Ron Rivest, Adi Shamir, and Len Adlemen. It is the most widely used asymmetric key cryptography algorithm. This technique employs a variety of data block sizes and key sizes. Asymmetric keys are used for both encryption and decryption. It generates the public and private keys using two prime numbers. These two distinct keys are used for both encryption and decryption. This algorithm is divided into three stages: key generation (using two prime integers), encryption, and decryption. RSA is now utilised in hundreds of software packages for key exchange, digital signatures, and the encryption of tiny blocks of data. This technique is primarily used for secure communication and authentication over a public communication channel.

4.3.4 4. Homomorphic Algorithm

It is an encryption algorithm that performs extraordinary computation on encrypted data (cypher text) and returns encrypted results. This algorithm is capable of resolving a wide range of security and confidentiality challenges. This algorithm acts on encrypted data through encryption and decryption at the client and supplier sites. This can mitigate risk while sending data between a client and a service provider by concealing plaintext from the provider, who functions solely on ciphertext. Homomorphic encryption enables sophisticated mathematical operations to be performed on encrypted data without the use of the original data.

4.3.5 5. Secure Hash Algorithm

In numerous applications, hash functions are utilised for digital signatures, data integrity, password protection, message authentication, pseudo-random number creation, key derivation, and cryptographic protocols. The message digest is computed using hash function algorithms as a defined length cryptography hash for a given data.

Chapter 5

Methodology

The term ”availability” refers to the capacity of cloud users to use the system in a predictable manner. According to this study, one of the feasible protective options for safeguarding cloud storage is to use combination cryptography encryption algorithms such as the hybrid algorithm (RSA and AES) and hash functions. The hybrid algorithm proposes/provides greater security, scalability, and speed than a secure system can. By adopting the hybrid method, the performance of AES and RSA has been improved. The hybrid encryption algorithm combines the strengths of each type of encryption, including the safety of asymmetric encryption and the speed of symmetric encryption. Furthermore, utilising SHA256 to generate a signature with the hybrid algorithm will accomplish the integrity necessary to improve the level of security in cloud data storage. A. Generate the public key using a symmetric algorithm (AES) This algorithm generates a public key used for encrypting data in the cloud

B. Using an asymmetric algorithm (RSA) To generate the secret key. The secret key is used for encrypting the public key.

C. Generating the signature Secure Hash Algorithm (SHA256) will be used to generate the signature, which will be sent to the recipient with the encrypted file.

D. Signature verification and decryption The following steps should be done by the recipient to verify the signature and decrypt the file 1) Extracts the message digest of the key file information by using the same hash function. 2) Compute the message digest of the information that has been signed 3) If both message digests are matching, the signature is valid and then he can decrypt the file.

Chapter 6

Literature Review

A lot of studies and researches have been done to enhance the security of cloud computing storage and environment using encryption and other techniques.

Vanishreeprasad. S and Mrs. K N Pushpalatha (2015) have improved the data security by proposing an architecture that integrates the cryptographic algorithms, Advanced Encryption Standard (AES) algorithm and the Hash function, SHA-2. */M. Meenakumari and G. Athisha (2014) have introduced to achieve data integrity and confidentiality during sending data in the cloud by using the technique of combining encryption algorithm (AES) with the hash function (MD5). B. Sowmya Sri (2013) has proposed a technique for sending data securely in a cloud storage system by using Erasure coding for encoding and RSA, AES algorithms for encryption. Uma Somani, Kanika Lakhani, and Manish Mundra (2010) have Implemented Cloud Storage Methodology to assess Data in the cloud by the Implementation of digital signature with RSA algorithm in a secure manner. Kamara et al. (2010) presented secure cloud storage by using encryption techniques. Using these techniques at first, the data will be indexed then by using symmetric algorithms (AES) with a unique key it will be encrypted. Then by using attribute encryption scheme and searchable encryption, the unique key and index are encrypted.

Chapter 7

Results and Data Analysis

7.0.1 Results and Discussion

Using different data input sizes (34, 67, and 93) kb, the execution time of encryption for Hybrid and Hybrid-SHA256 algorithms are listed in Table I and the execution time of decryption is listed in Table II. As shown in the experimental results listed in Table I II; it is found that the encryption and decryption phases using the proposed hybrid-SHA256 algorithm outperforms the Hybrid algorithm in security but it consumes more time than the other.

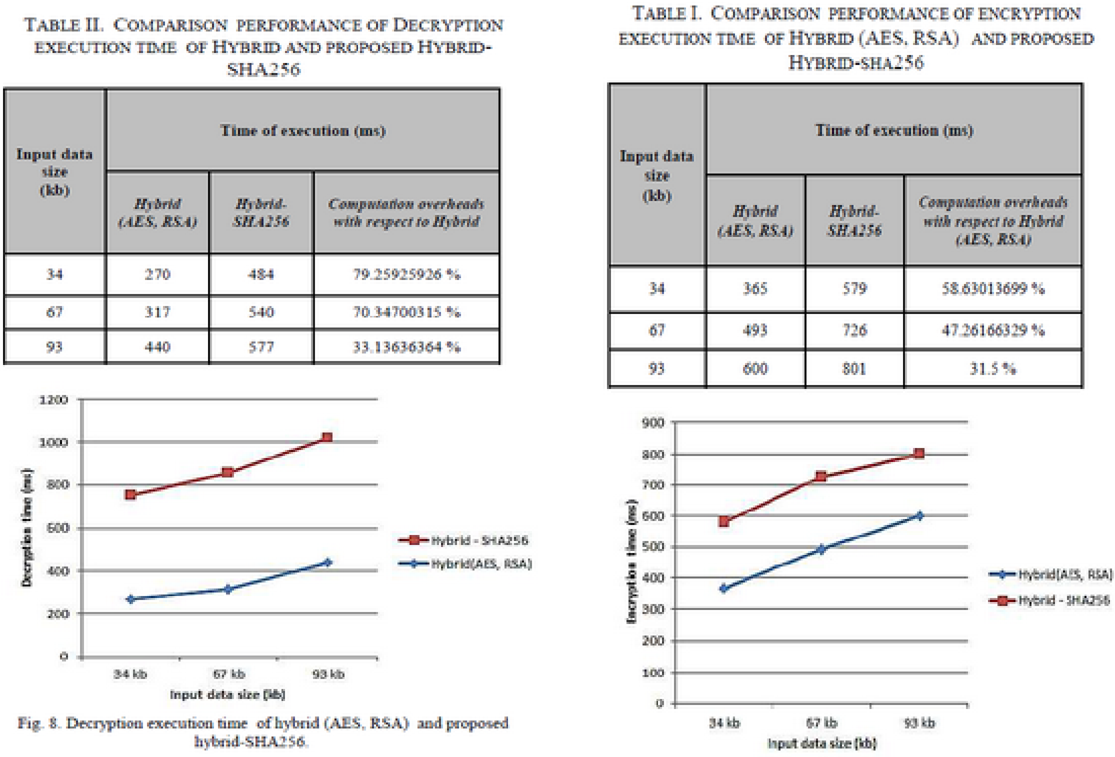

TABLE II. COMPARISON PERFORMANCE OF DECRYPTION EXECUTION TIME OF HYBRID AND PROPOSED HYBRID-SHA256

Input data size (kb)	Time of execution (ms)		
	Hybrid (AES, RSA)	*Hybrid-SHA256*	*Computation overheads with respect to Hybrid*
34	270	484	79.25925926 %
67	317	540	70.34700315 %
93	440	577	33.13636364 %

Fig. 8. Decryption execution time of hybrid (AES, RSA) and proposed hybrid-SHA256.

TABLE I. COMPARISON PERFORMANCE OF ENCRYPTION EXECUTION TIME OF HYBRID (AES, RSA) AND PROPOSED HYBRID-SHA256

Input data size (kb)	Time of execution (ms)		
	Hybrid (AES, RSA)	*Hybrid-SHA256*	*Computation overheads with respect to Hybrid (AES, RSA)*
34	365	579	58.63013699 %
67	493	726	47.26166329 %
93	600	801	31.5 %

Figure 7.1

The overhead time is defined as the ratio between hybrid-SHA256 to hybrid (AES, RSA) algorithm while measuring its performance with respect to hybrid (AES, RSA) algorithm.

The optimum result obtained from encryption phase is approximately 32 percent with respect to hybrid (AES, RSA) algorithm, and the optimum results obtained for decryption phase is nearly 33 percent with respect to hybrid (AES, RSA) algorithm.

The figures show a comparison of total time between hybrid algorithm and new proposed hybrid-SHA256. When comparing with hybrid, proposed model requires more time for encryption and decryption. Whereas proposed model is more secure encryption algorithm than hybrid, because the proposed model includes hashing and digital signature concept, which is more difficult for the intruder to find the plain text from the secret message. Moreover, proposed model provides the three security primitives – confidentiality, integrity, and nonrepudiation.

Encryption algorithms; symmetric (AES), asymmetric (RSA) and hybrid algorithms are the most algorithms used to encrypt data in the cloud storage in order to make the data more secure from theft. A hash function is the best way to achieve the integrity of data in the cloud environment. Using a combination of cryptography encryption algorithms such as AES and RSA with SHA256 is one of secure and convenient technique for secure data via cloud storage services and achieve the confidentiality, integrity and non-repudiation. In the future, we will try to apply this method using GPU scheduling concepts to reduce the execution time for encryption and decryption phases.

Chapter 8
Conclusion

8.1 CONCLUSION

Cloud computing is world emerging, next generation technology in the field of information technology. It has numerous advantages but some challenges still exist in this technology. Security is the most challenging issue in this technology. In this paper we have discussed various encryption algorithms to overcome this security issue, deals with advantages and disadvantages of these algorithms. A hash function is the best way to achieve the integrity of data in the cloud environment. Using a combination of cryptography encryption algorithms such as AES and RSA with SHA256 is one of secure and convenient technique for secure data via cloud storage services and achieve the confidentiality, integrity and non-repudiation.

8.2 Future Work

Most important future work identifies here is that there are concrete standards for cloud computing security still missing. There are some open cloud manifesto standards and few efforts made by the cloud security alliance to standardize the process in the cloud. In addition to this the cloud computing with such great offering such as storage, infrastructure and application designing capabilities on the go to the IT industry still fail to have proper standards for interoperability with other cloud service providers. This failure to provide concrete security standards, common underlying framework for data migration and global standards for cloud interoperability, make the leading technology 0loud computing" still a vulnerable option for aspiring users.

8.3 References

Reference

1. RESEARCH PAPER ON CLOUD COMPUTING by Mrs. Ashwini Sheth1, Mr. Sachin Bhosale2, Mr. Harshad Kadam3.

2. A Review Paper on Cloud Computing by Aakash Tyagi in 2018

3. Interface development for Eucalyptus based cloud by Albert Folch in 2011

4. Cloud Computing Evaluation,How it Differs to,Traditional IT Outsourcing by Debora Di Giacomo and Tino Brunzel in 2010.

5. A Study on Cloud Computing Security Challenges by Santosh Bulusu and Kalyan Sudia in 2013

6. THE CONCEPT OF CLOUD COMPUTING AND THE MAIN SECURITY ISSUES IN IT by Yang Ou in 2015.

7. Trust Based Security for Cloud Systems by Dinesh Sriram and Murali Medisetty.

8. A Review of Various Security Techniques in Cloud computing by Kulwinder Kaur in 2018

9. A Hybrid Hashing Security Algorithm for Data Storage on Cloud Computing by Noha MM. AbdElnapi , Fatma A. Omara and Nahla F.Omran in april 2016.

10. Enhancing Security in Cloud Storage using ECC Algorithm by Ravi Gharshi1, Suresha2.

11. RSA (algorithm), https://en.wikipedia.org/wiki/RSA$_{(}cryptosystem$)

12. https://www.techtarget.com/searchcloudcomputing/definition/cloud-computing

13. https://azure.microsoft.com/en-in/overview/what-is-cloud-computing/

14. https://en.wikipedia.org/wiki/Amazon$_Web_Services$