SECURITY IN CLOUD COMPUTING

BY

MD SHAFIQUL ISLAM

ID: 173-25-609

This Report Presented in Partial Fulfillment of the Requirements for the Degree of Masters of Science in Computer Science and Engineering

Supervised By

Md. Zahid Hasan
Assistant Professor & Coordinator of MIS
Department of Computer Science and Engineering
Daffodil International University

DAFFODIL INTERNATIONAL UNIVERSITY

DHAKA, BANGLADESH

12 DECEMBER 2018

APPROVAL

This report titled **"Security in Cloud Computing",** submitted by MD SHAFIQUL ISLAM, ID NO: 173-25-609 to the Department of Computer Science and Engineering, Daffodil International University, has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of M.Sc. in Computer Science and Engineering and approved as to its style and contents.

BOARD OF EXAMINERS

_____

Dr. Syed Akhter Hossain — **Chairman**
Professor and Head
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

_____

Dr. Sheak Rashed Haider Noori — **Internal Examiner**
Assistant Professor and Associate Head
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

_____

Md. Zahid Hasan — **Internal Examiner**
Assistant Professor & Coordinator of MIS
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

_____

Dr. Muhammad Shorif Uddin — **External Examiner**
Professor
Department of Computer Science and Engineering
Jahangirnagar University.

DECLARATION

I hereby declare that, this thesis has been done by me under the supervision **Md. Zahid Hasan, Assistant Professor & Coordinator of MIS, Department of CSE,** Daffodil International University. I also declare that neither this thesis nor any part of this thesis has been submitted elsewhere for award of any degree or diploma.

Supervised by:

_____

Md. Zahid Hasan
Assistant Professor & Coordinator of MIS
Department of CSE
Daffodil International University

Submitted by:

_____

Md Shafiqul Islam
ID: 173-25-609
Department of CSE
Daffodil International University

ACKNOWLEDGEMENT

First I express my heartiest thanks and gratefulness to almighty God for His divine blessing makes me possible to complete this report successfully.

I really grateful and wish my profound my indebtedness to **Md. Zahid Hasan, Assistant Professor & Coordinator of MIS**, Department of CSE Daffodil International University, Dhaka. Deep Knowledge & keen interest of my supervisor in the field of Computer Science to carry out this thesis. His endless patience, scholarly guidance, continual encouragement, constant and energetic supervision, valuable advice at all stage have made it possible to complete this thesis paper.

I would like to express my heartiest gratitude to **Dr. Syed Akhter Hossain** , Head of Department of Computer Science and Engineering, for giving me an opportunity to carry out the research work, without him I should not reached my goal and also to other faculty member and the staff of CSE department of Daffodil International University.

I would like to thank my entire course mate in Daffodil International University, who took part in this discuss while completing the course work.

Finally, I must acknowledge with due respect the constant support and patients of my parents.

DEDICATION

I dedicate my dissertation work to my family and many friends. A special feeling of gratitude to my loving parents**,** to my mother **Mst Mafia Akter** a strong and gently soul who taught me to trust in Allah, believe in hard work and that so much could be done with little. To my father **Oahidozzaman** for earning an honest living for us and for supporting and encouraging me to believe in myself. Also I need to thank my friend Riyazul Kabir for his encouragement.

ABSTRACT

Cloud system involves transferring data from client to server, server to client and processing, storage data in server. As a result of which, data needs to be protected and secure while transferring through the network and in the server of service providers. Cloud system is an emerging technology in which security is the most challenging issue. Due to data security issue with cloud computing many business organization have fear in storing their data in Cloud. So the most challenging task of the business organization is to provide high security for their data since the data are sensible related to their business.

This paper tries to summarize general characteristics and trusted security of cloud computing which will help the development and adoption of this rapidly evolving technology. This paper explores some of the basics and privacy issues of cloud computing. We demonstrate a new type of attack that is called “Man in the Cloud” (MITC) Attack. To ensure the security of data, In this paper we proposed a method of providing security that can be prevent “Man in the Cloud ”(MITC) Attack. In this paper we use RSA encryption and decryption algorithm plus auto generated random code verification system to provide two steps security in file synchronization in cloud computing or mobile cloud computing (MCC).

TABLE OF CONTENTS

CONTENTS **PAGE NO**

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Introduction

This is the right off the bat some portion of the hypothesis paper. In this segment I will at first portray an introduction of Cloud figuring. The basic business advantage models being sent, (for instance, programming, stage, and establishment as an organization) and fundamental sending models used by master centers and customers to use and keep up the cloud organizations, (for instance, the private, open, system, and cream fogs) are inspected. Moreover introduced are the points of interest and troubles related with appropriated processing. By then I will indicate and give brief discussion about the insurance and security of the endeavor targets and the technique for doing the assignment. Finally, the short depiction the undertaking structure will be referenced toward the complete of the section.

1.2 Motivation

In the season of web and ebb and flow development, by far most of the IT associations are endeavoring to help their business and win money. In any case, the Infrastructure, stage and support of changed writing computer programs is a noteworthy issue. Disseminated registering has give all game plans in basic way. Disseminated registering has ascended as an unmistakable response for give unobtrusive and straightforward access to externalized IT (Information Technology) resources. An extending number of affiliations (e.g., ask about centers, adventures) advantage from Cloud figuring to have their applications. Through virtualization, Cloud preparing can address with the comparable physical structure an immense client base with different computational necessities. Instead of past models (Clusters and Grid enlisting), Cloud handling isn't application-orchestrated anyway advantage arranged; it offers on intrigue virtualized resources as quantifiable and billable

utilities.

Nevertheless, appropriated processing is the key primary purpose in various associations in this way, the noteworthy stress in the disseminated registering is giving the security of their data in the cloud. Mooring data is progressively basic because of the essential thought of appropriated figuring and the a great deal of complex data it passes on worries concerning data assurance and security are exhibiting the more broad take-up of disseminated processing organizations.

1.3 Objectives

The rule purpose of this investigation work is to perceive and appreciate the security issues which impact the execution of conveyed processing. Furthermore, to appreciate the security strategies which are being used to alleviate these security issues. Thusly showing the standard principles for the cloud master communities and furthermore cloud customers [27].

The essential focuses of this examination are:

In the fundamental stage RSA encryption estimation will be associated and in the second stage Feistel encryption computation will be associated on the yield data, i.e., figure substance of first stage. After positive stage, mixed data will be sent for transmission. In this paper we endeavor to make more grapple cloud organizations and data transmission by using RSA figuring notwithstanding auto made sporadic code or versatile code check structure when data is exchanging and downloading.

1.4 Research questions

1: What are the diverse security methodologies being used by the principle appropriated

processing providers, to envision dynamic and uninvolved ambushes when the data is being traded between the cloud and an adjacent framework?

2: What are the diverse security frameworks being used to envision unapproved access to data inside the cloud?

3: What are the genuine security challenges we expect in future conveyed figuring?

4: How might we have the capacity to manage security issue that are typical in future appropriated processing?

1.5 Report layout

The entire report is designed with six important chapters. In the first chapter introduction and main objective of the research is reflecting. In the second chapter the background of this research study will be shown. In the third chapter the security risks and issues of cloud of this research study will be shown. In the fourth chapter it will be shown which methodology is being used to set the expected output. In the five chapter the survey result and discussion is taking place. In the last chapter the research will come to its conclusion with future works reflection.

CHAPTER 2

BACKGROUND

2.1 Introduction

According to NIST, ―Cloud figuring is a model for engaging unavoidable, profitable, on-ask for arrange access to a typical pool of configurable enlisting resources (e.g., frameworks, servers, storing, applications, and organizations) that can be immediately provisioned and released with insignificant organization effort or pro association interaction‖ [4]. Dispersed figuring is a strategy for passing on different sorts of organizations over the Internet. Circulated registering settles the enthusiasm of figuring resources (e.g., CPU, RAM, etc) for getting ready occupations. Starting late, the enthusiasm for getting ready jobs has extended to hundreds or thousands of CPU focuses [5].

2.2 What is cloud computing?

Distributed computing is a strategy for conveying various types of administrations over the Internet. It very well may be a product application (e.g., Gmail) conveyed over the Internet. It tends to be a stage (e.g., Google App Engine) over which clients can compose an application. It very well may be a working framework (e.g., Amazon EC2 gives OS) [8] where clients can make their own stage and programming. Every one of these administrations can be gotten to through an Internet association.

Appropriated registering engages associations to eat up a procedure resource, for instance, a virtual machine (VMs), amassing or an application, as an utility essentially like power instead of building and keep up figuring establishments in house [1].The accompanying figure 2.1 demonstrate a fundamental distributed computing condition.

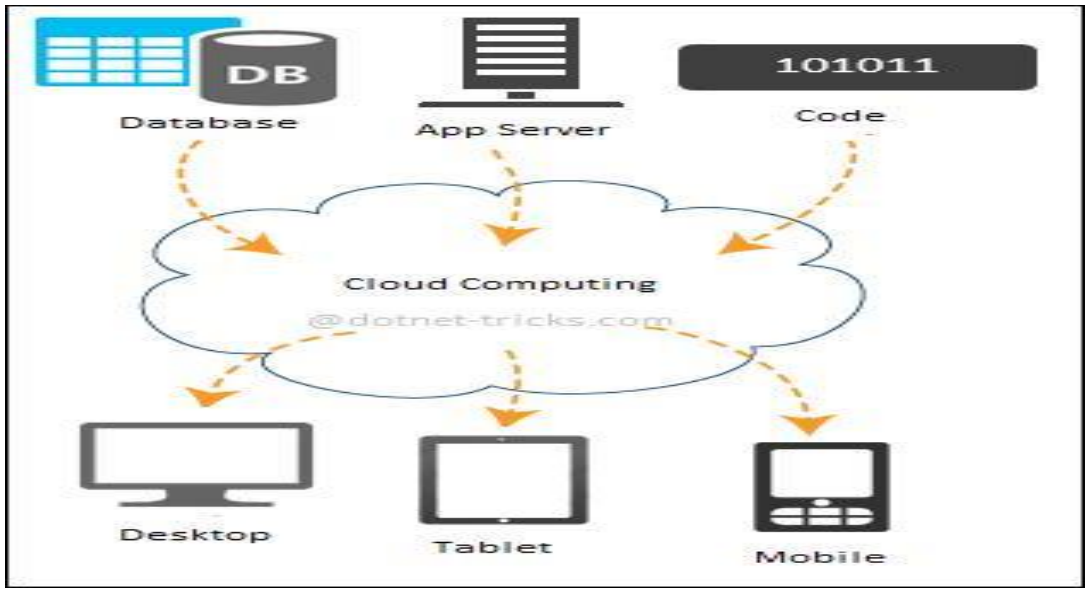

Figure 2.1: A basic cloud computing environment [26].

2.3 Favorable circumstances of Cloud Computing

Some most critical favorable circumstances of distributed computing are given underneath.

- Reduced Cost.
- Self-service provisioning.
- Elasticity.
- Pay per use.
- Full virtualization.
- Automatic software updates.
- Flexibility.

2.4 Essential characteristics

Essential characteristics are given below.

2.4.1 On-request self-benefit

A buyer can independently plan handling limits, for instance, server time and framework accumulating, as required normally without requiring human relationship with every expert association's [1].

Figure 2.2: A cloud computing environment [26]

2.4.2 Expansive system get to

Capacities are available over the framework and got to through standard instruments that advance use by heterogeneous thin or thick client stages (e.g., phone, PCs, and individual modernized associates (PDAs)) [1].

2.4.3 Asset pooling

The provider's figuring resource are pooled to serve different customers using a multi-tenant illustrate. With different physical and virtual resources logically allotted and reassigned by buyer ask. There is a sentiment of region opportunity in that the supporter overall has on control or data over the right zone of the enabled resources anyway may

need to show territory at a bigger measure of consultation (e.g., country state, or server cultivate). Occurrences of advantages fuse limit, taking care of, memory, organize information exchange limit and virtual machines [1].

2.4.4 Fast adaptability

Capacities can be rapidly and adaptably provisioned, on occasion thus, to quickly scale out and immediately released to quickly scale in. To the buyer, the capacities open for provisioning as often as possible appear, apparently, to be unfathomable and can be gotten in any sum at whatever point [1].

2.4.5 Estimated Service

Cloud systems normally control and streamline resource use by using a metering capacity at some component of reflection legitimate to the kind of organization (e.g., limit, getting ready, information exchange limit, and dynamic customer accounts). Resource utilize can be checked, controlled, and nitty gritty offering straightforwardness to both the provider and buyer of the utilized organization [1].

2.5 Cloud deployment strategies

Cloud deployment strategies are given below.

2.5.1 Open cloud

In essential terms, open cloud organizations are depicted as being available to clients from a pariah master association by methods for the Internet. The articulation "open" does not continually mean free, in spite of the way that it will in general be free or really sensible to use. An open cloud does not infer that a customer's data is uninhibitedly recognizable; open cloud vendors usually give a passageway control framework to their customers. Open fogs

give an adaptable, fiscally insightful expects to pass on courses of action [2] [3].The following figure 1.2 show open cloud structure.

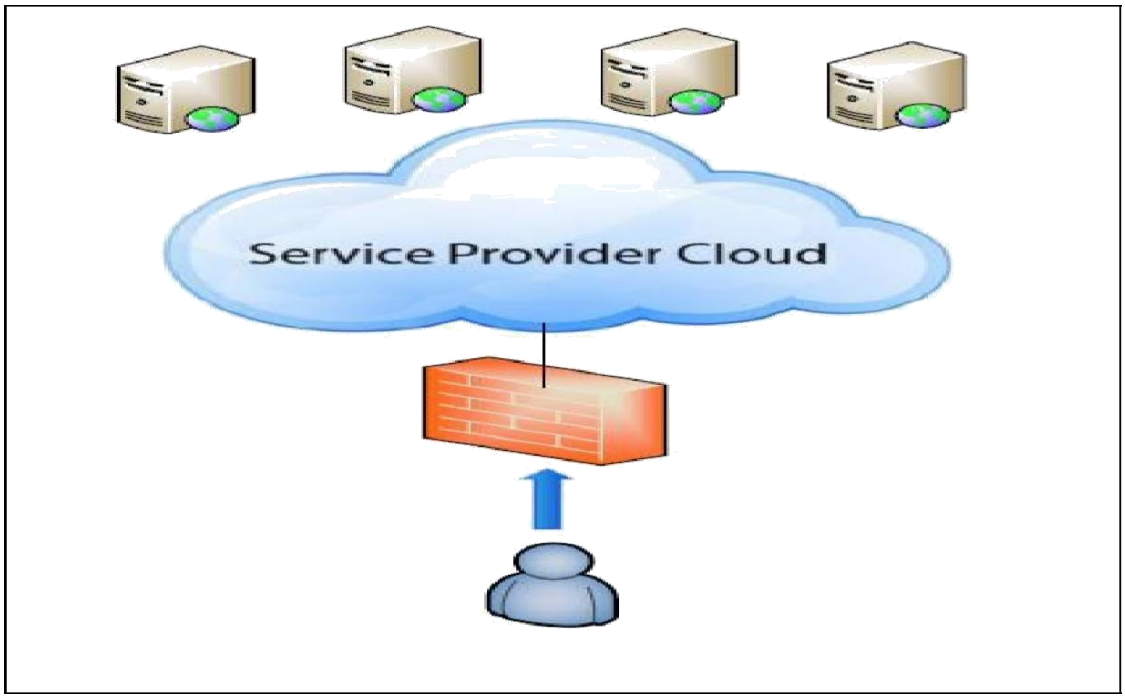

Figure 2.3: Open Cloud

2.5.2 Private cloud

A private cloud offers an impressive part of the upsides of an open appropriated figuring condition, Such as being adaptable and advantage based. The differentiation between a private cloud and an open cloud is that in a private cloud-based organization, data and methodology are managed inside the relationship without the restrictions of framework transmission limit, security exposures and legal requirements that using open cloud organizations may include. In like manner, private cloud organizations offer the provider and the customer progressively essential control of the cloud structure, improving security and quality since customer get to and the frameworks used are restricted and allocated [2]

[3].The following figure 1.3 show private cloud structure.

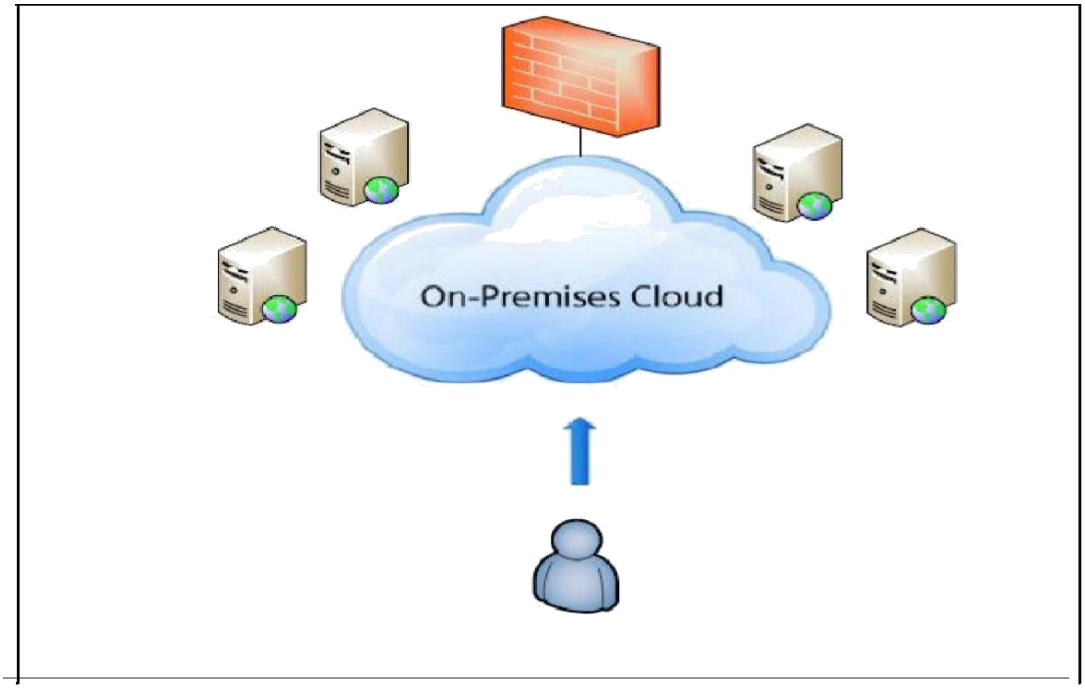

Figure 2.4: Private Cloud

2.5.3 Network cloud

A social order cloud is shared among something like two affiliations that have practically identical cloud essentials.

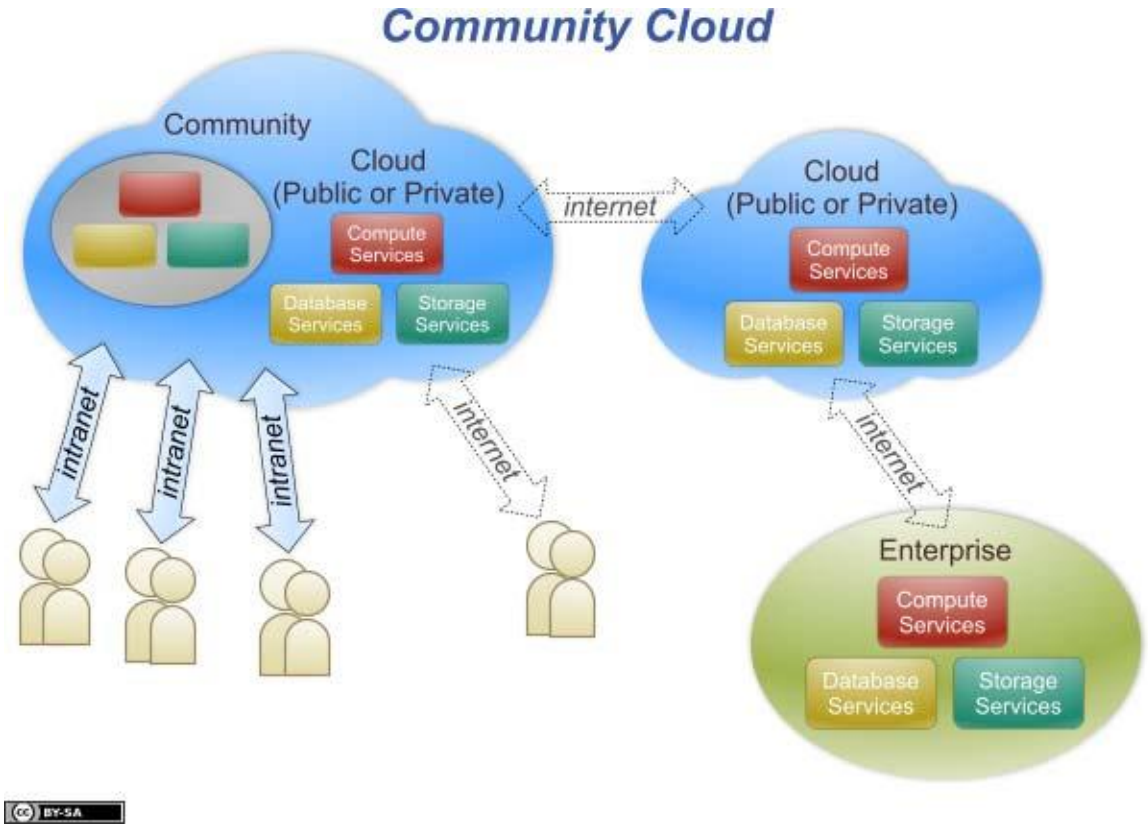

Figure 2.5: Network cloud [28]

2.5.4 Hybrid cloud

A cream cloud is a mix of an open and private cloud that interoperates. In this model customers typically re-suitable non business-essential information and dealing with to individuals when all is said in done cloud, while keeping business-fundamental organizations and data in their control [2].

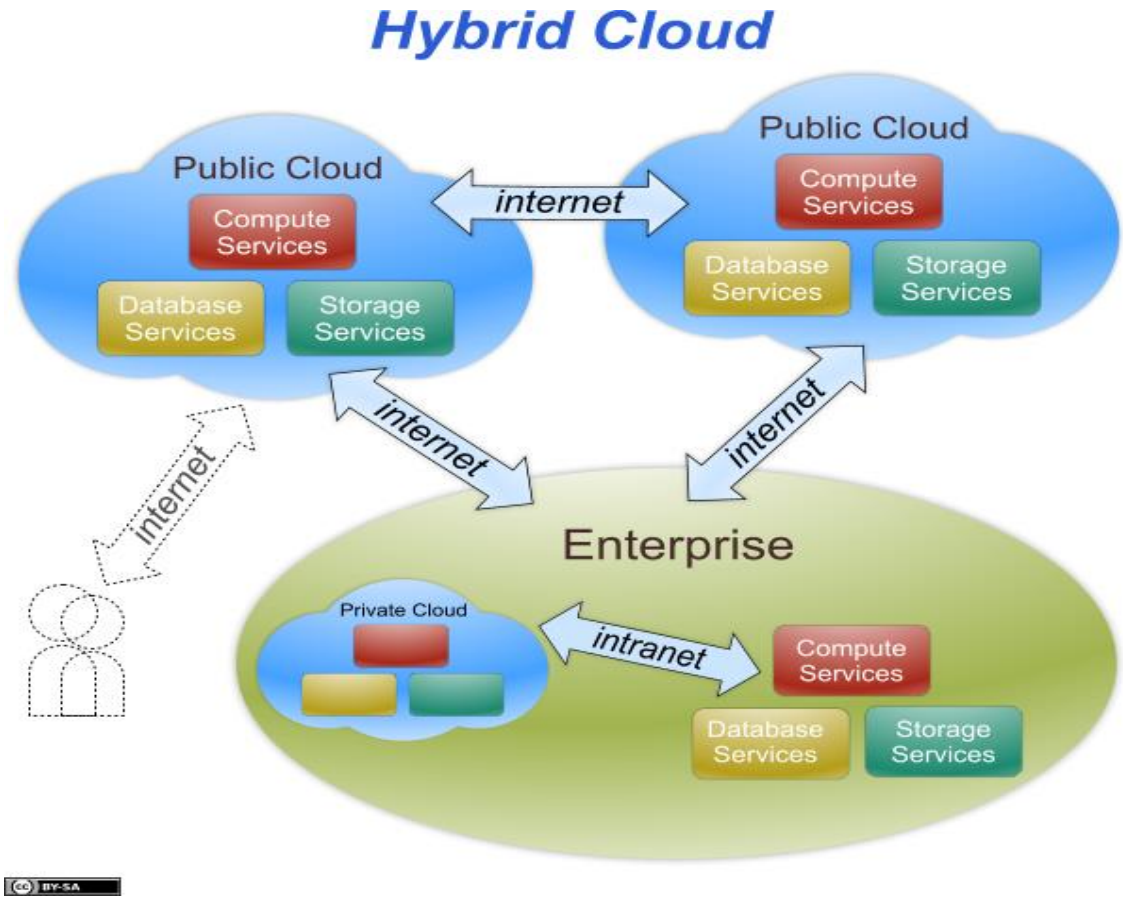

Figure 2.6: Hybrid cloud [28]

2.6 Cloud service models

This fragment of the paper delineates the diverse cloud advantage models. Cloud can be passed on in three models these are IAAS, PAAS, and SAAS [6]. The going with figure 2.7 show Cloud Service Models.

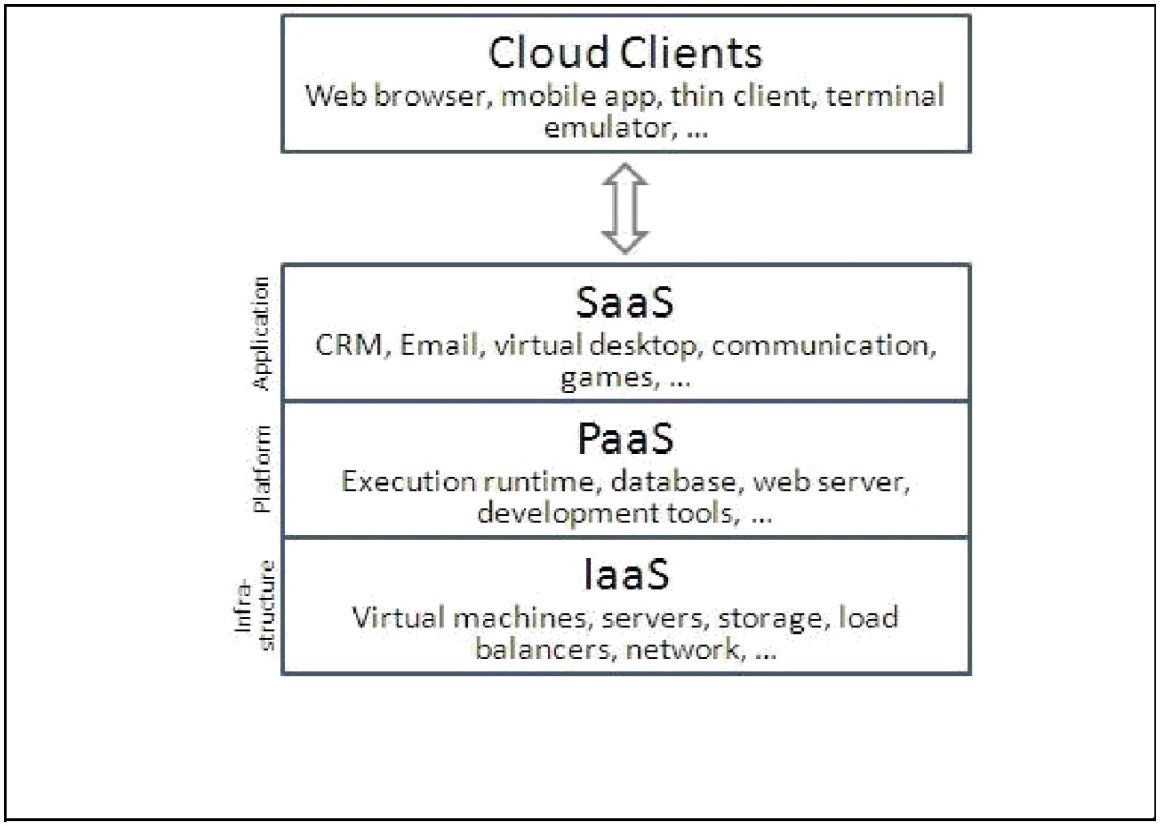

Figure 2.7: Cloud Service Models

2.6.1 IAAS

• Foundation as an organization passes on a phase virtualization redistributed organization. The customer can control nature as an organization. IAAS empowers affiliations and planners to grow their IT structure on an on-ask for start. For example, if a man needs to keep up an online business, there is no convincing motivation to set up his/her very own IT system. Or maybe he/she can rent a virtual machine. A couple of cases of IAAS providers are;

• Amazon Elastic Compute Cloud (EC2): gives customers an extraordinary virtual machine

(AMI) that can be passed on and continue running on the EC2 establishment [7].

• Amazon Simple Storage Solution (S3): gives customers access to intensely flexible limit resources

• Go Grid: outfits customers with access to logically versatile enlisting and limit resources, and also dedicated servers

• IBM Computing on Demand (CoD): outfits customers with access to astoundingly configurable servers notwithstanding regard included organizations, for instance, data storing

• Microsoft Live Mesh: outfits customers with access to a scattered record system; coordinated at individual use

• Rackspace Cloud: outfits customers with access to intensely flexible figuring and limit resources, and also untouchable cloud applications and gadgets

2.6.2 PAAS

This kind of circulated registering gives enhancement condition as an organization. The purchaser can use the merchant's equipment to develop his very own program and pass on it to the customers through Internet and servers. The client controls the applications that continue running in nature, anyway does not control the working structure, hardware or framework establishment on which they are running [2].

Some PAAS examples are;

• Akamai Edge Platform: gives an extensive dispersed registering stage on which associations can send their web applications, has a vast spotlight on investigation and

observing.

• Force .com: from salesforce.com (a SaaS supplier), furnishes clients with a stage to construct and run applications and segments purchased from AppExchange6 or custom applications [16].

• Google App Engine: furnishes clients with a total improvement stack and enables them to run their applications on Google's foundation [8].

• Microsoft Azure administrations stage: Provides clients with on-request figure and capacity benefits and additionally an improvement stage dependent on Windows Azure.

• Yahoo! Open procedure (Y!OS): furnishes clients with a methods for creating web applications over the current Yahoo! Stage and in doing as such utilizing a critical bit of the Yahoo! Assets.

2.6.3 SAAS

SaaS is programming that is possessed, conveyed and oversaw remotely by at least one suppliers and that is offered in a compensation for each utilization way. In SaaS, the foundation and stages are as of now in store in cloud, utilized just pick the product which they can redoes. This is the completely business arrangement.

Some SAAS examples are;

• Google Apps: gives online office devices, for example, email, schedule, and record the executives.

• Salesforce.com: gives a full client relationship the executives (CRM)6 application.

• Zoho.com: Provides an expansive suite of online applications, for the most part for big business utilize.

2.7 Related work

In [9] Rachna Arora et. al. examined different security issues, component and difficulties of distributed computing. Creators of paper [10] exhibited figure cloud where they demonstrated 5 layers of security estimation for scrambling information for cloud. Prior to sending the information through media, information will be scrambled and information will remain put away in server as encoded. In paper [11] gave security to three viewpoints, of security privacy, Integrity and validation of information stockpiling in the cloud. MD5 calculation proposed for trustworthiness of the information. In paper [12] Providing Data Security in Cloud Computing utilizing open key cryptography proposed a technique by actualizing RSA calculation. In paper [13] Hybrid RSA encryption calculation is proposed for security of information in cloud framework.

Gartner 2008 perceived seven security issues that ought to be tended to before undertakings consider changing to the disseminated figuring model. They are according to the accompanying: (1) favored customer get to - information transmitted from the client through the Internet speaks to an explicit dimension of danger, because of issues of data ownership; attempts should contribute vitality winding up increasingly familiar with their providers and their controls anyway much as could be normal before designating some irrelevant applications first to test the water, (2) regulatory consistence - clients are in charge of the security of their answer, as they can pick between providers that allow to be reviewed by pariah affiliations that check measurements of security and providers that don't (3) data territory - depending upon contracts, a couple of clients may never understand what country or what region their data is discovered (4) data disengagement - encoded information from different associations may be secured on the proportionate hard circle,

so a part to segregate data should be passed on by the provider. (5) recovery - every provider should have a failure recovery tradition to guarantee customer data (6) adroit help - if a client presumes broken development from the provider, it probably won't have various authentic courses look for after an examination (7) whole deal common sense - suggests the ability to pull back an assention and all data if the present provider is obtained out by another firm [14].

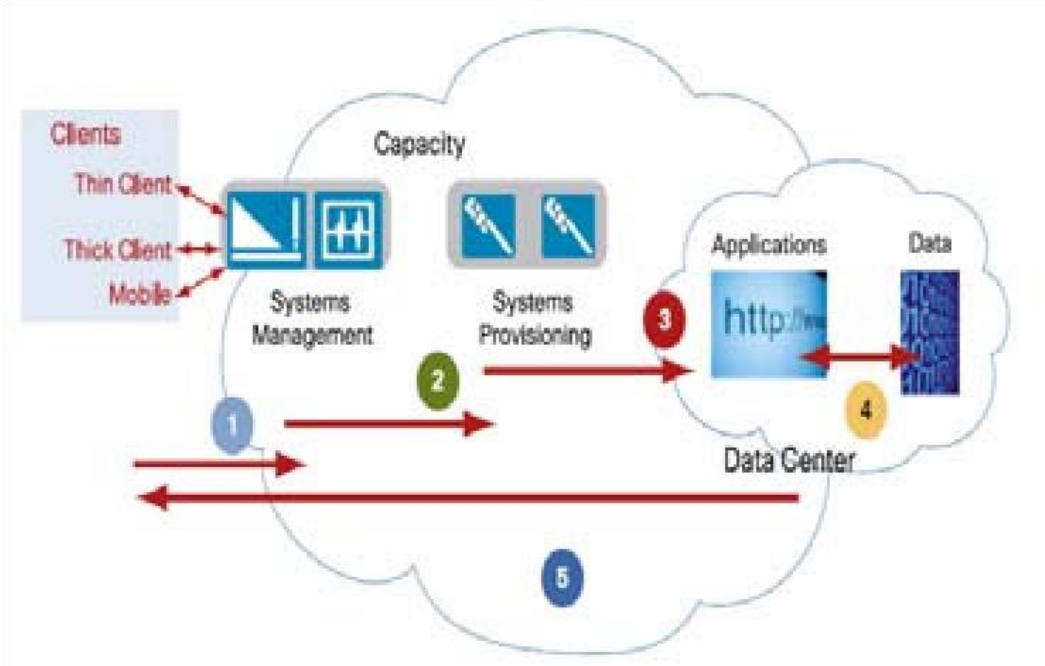

Figure 2.8. Cloud computing Workflow [29]

2.8 Research summary

All these papers and related work methods can may be provide security in cloud computing during data transfer and encryption and decryption. But it can be make more secure and provide high level security.

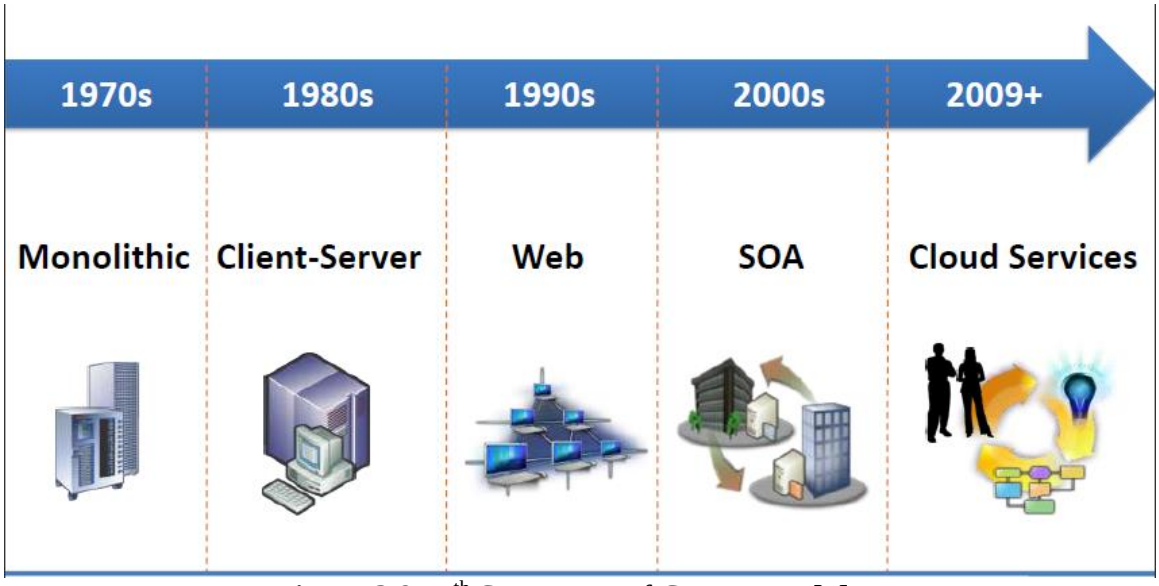

Figure 2.9. 5th Generation of Computing [2]

2.9 Scope of the problem

• Most security issues originate from:

- Loss of control
- Lack of trust (instruments)
- Multi-occupancy
- Borderless processing

• Self-directed fogs still have security issues, yet not related to above

2.10 Challenges

- Security
- Costing model
- Charging model
- Service level assention
- Cloud interoperability issue

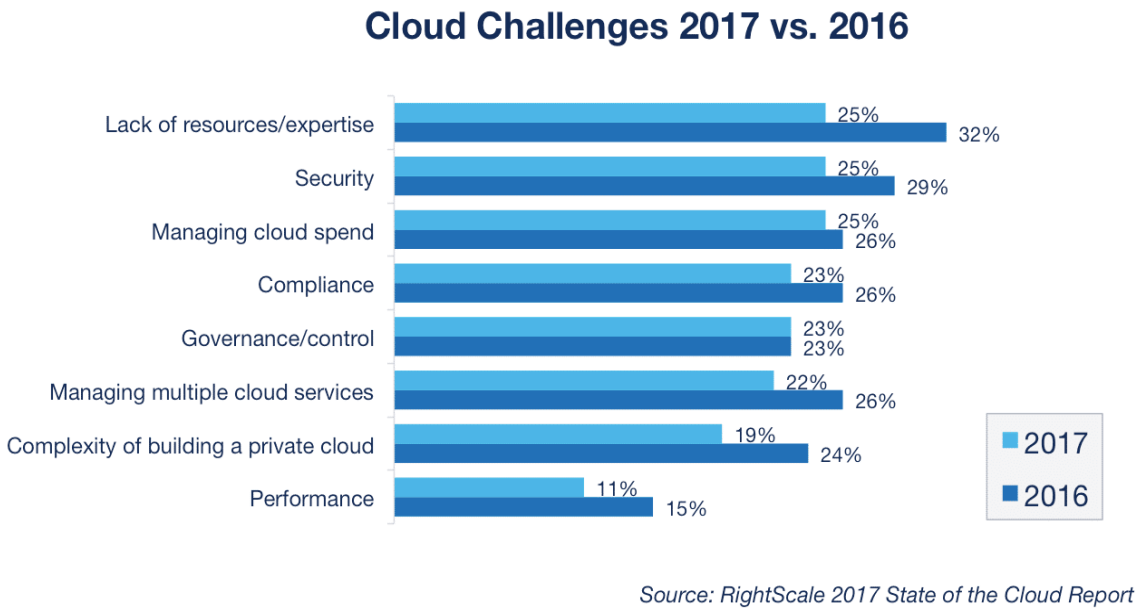

Figure 2.10. Cloud challenges 2017 vs 2016 [30]

CHAPTER: 3

SECURITY RISKS AND ISSUES OF CLOUD COMPUTING

3.1 Introduction

In this area of suggestion paper we look at about security threats and a couple of issues of circulated processing. Security remains a basic stress for associations thinking about cloud allotment especially open cloud gathering. Open cloud providers share their fundamental gear system between different customers, as open cloud is a multi-occupant condition.

As demonstrated by Cloud Security Alliance (CSA), in excess of 70 percent of the world's associations by and by work at any rate to some degree on the cloud. Starting late the "Cloud Security Spotlight Report" showed that "90 percent of affiliations are to a great degree or decently stressed over open cloud security." These stresses run the range from feebleness to caught records to poisonous insiders to full-scale data bursts. Top security stresses for cloud-based organizations you should think about [15].

Despite the fact that cloud suppliers will in general work admirably at security on their end, you should in any case be cautious with your own inward security arrangements. Some security issues are outside the extent of a cloud supplier, and you should make sure to avoid potential risk against such things.

3.2 Security Issues

- **Data Breach**

A data crack is a scene in which delicate, guaranteed or private data has possibly been seen, stolen or used by an individual unapproved to do thusly. An examination coordinated by the Ponemon Institute entitled " Man In Cloud Attack" reports that in excess of 50 percent

of the IT and security specialists reviewed believed their affiliation's wellbeing endeavors to guarantee data on cloud organizations are low [17].

• Hijacking of Account

The improvement and execution of the cloud in various affiliations has opened a radical new game plan of issues in record seizing. Attackers by and by can use your (or your laborers') login information to remotely get to sensitive data set away on the cloud; besides, aggressors can defile and control information through laid hold of capabilities [17].

• Secure data trade

Most of the movement going between your framework and whatever advantage you're getting to in the cloud must explore the Internet. Guarantee your data is constantly going on a protected channel; just interface your program to the provider by methods for a URL that begins with"https."

Furthermore, your data should constantly be encoded and checked using industry standard traditions, for instance, IPsec (Internet Protocol Security), that have been delivered expressly to guarantee Internet development.

• User get to control

Data set away on a cloud provider's server can be gotten to by a laborer of that association, and you have none of the average personnel controls over those people. In any case, consider carefully the affectability of the data you're allowing out into the cloud. Second seek after inspect firm Gartner's proposition to approach providers for focal points about the all inclusive community who manage your data and the element of access they have to it.

• Secure programming interfaces

The Cloud Security Alliance (CSA) endorses that you think about the item interfaces, or APIs, that are used to associate with cloud organizations. "Reliance on a frail course of action of interfaces and APIs opens relationship to a collection of security issues related to protection, uprightness, openness, and obligation," says the social event in its Top Threats to Cloud Computing report. CSA endorses making sense of how any cloud provider you're pondering fuses security every single through it organization, from affirmation and access control procedures to activity checking approaches.

• Secure set away data

Your data should be securely mixed when it's on the provider's servers and remembering that it's being utilized by the cloud advantage. In Q&A: Demystifying Cloud Security, Forrester alerts that few cloud providers ensure protection for data being used inside the application or for disposing of your data. Ask potential cloud providers how they secure your data when it's in movement and in addition when it's on their servers and gotten to by the cloud-based applications. Find, as well, if the providers securely dispose of your data, for example, by eradicating the encryption scratch.

• Data partition

Each cloud-based organization shares resources, specifically space on the provider's servers and distinctive parts of the provider's establishment. Hypervisor writing computer programs is used to make virtual compartments on the provider's gear for all of its customers. Regardless, CSA observes that "ambushes have surfaced starting late that objective the common development inside Cloud Computing conditions." So, investigate the compartmentalization frameworks, for instance, data encryption, the provider uses to balance access into your virtual holder by various customers.

3.3More attacks

- DoS attacks.
- Insider Threat.
- Malware Injection.
- Denial of Service Attacks.
- Shared Vulnerabilities.

The following figure 3.1 show different kinds of attack or vulnerabilities by type in percentage [18].

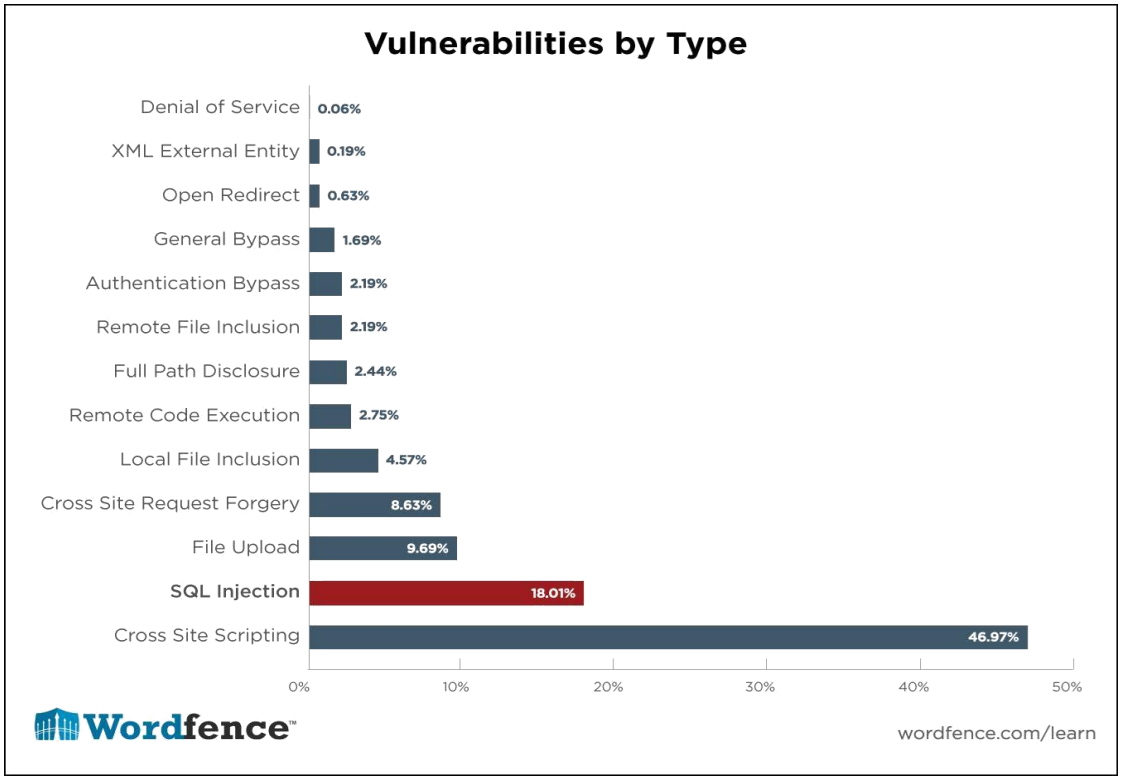

Figure 3.1: Vulnerabilities by type in percentage.

CHAPTER 4

RESEARCH METHODOLOGY

4.1 Introduction

In this hypothesis paper, we basically display another kind of ambush that is call "Man in the Cloud" (MITC) Attack. These MITC strikes rely upon standard archive synchronization organizations (For instance, Google Drive and Dropbox) as their structure for course and control (C&C), data exfiltration, and remote access.

Since most associations either enable their clients to utilize document synchronization benefits, or even depend on these administrations as a feature of their business tool stash, we believe that MITC assaults will end up pervasive in nature. Therefore, we urge endeavors to move the focal point of their security exertion from forestalling diseases and endpoint assurance to anchoring their business information and applications at the source.

4.2 Man in the cloud (MITC) attacks

At Black Hat USA 2015, Imperva discharged a report that clarified another kind of assault vector that permits cybercriminals to get to information and archives put away in well known document synchronization administrations, for example, Google Drive. Named "man-in-the-cloud assaults," programmers can take information, and also control access to clients' entire Drives and every one of the records inside [19].

The report cautioned this is a tremendous hazard factor for undertakings and shoppers, particularly since the MITC assaults don't depend on trading off accreditations and they don't require noxious code or endeavors. Rather, cybercriminals invade end-client

machines, take synchronization tokens specifically from the PC's vault and place them on various gadgets. Google Drive does not mind which machine utilizes the token, as long as it's genuine, so cybercriminals will have finish access to and authority over the related Drive.

4.3 working principle

Man in the cloud (MITC) assaults most extreme time occurred between record synchronization.

Synchronization, similarly as with Microsoft's Live Mesh or Apple's MobileMe, enables substance to be revived over various gadgets. For example, on the off chance that you have a spreadsheet on your PC and, transfer it to the capacity benefit, whenever you check your PDA, that record will be downloaded onto it and greatest time assailant assault between this time.

This somewhat straightforward assault empowers the aggressor to share the unfortunate casualty's document synchronization account. The assailant is then ready to get to documents which are synchronized by the person in question and contaminate these records with pernicious code. The assault comprises of running the Switcher instrument referenced above on the unfortunate casualty's machine [19]. This can be cultivated through a drive-by-download misuse or through an increasingly clear Phishing attack. The going with figure 4.1 show Quick Double Switch Attack.

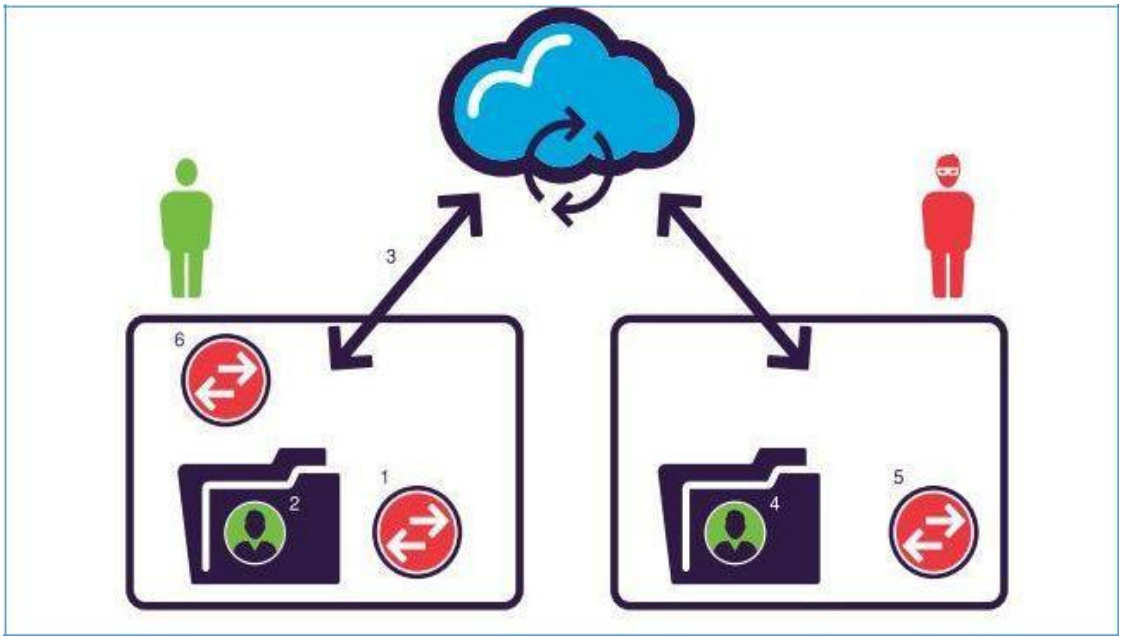

Figure 4.1: Quick Double Switch Attack

• The aggressor traps the individual being referred to (using social planning, for example) or utilizations an undertaking in order to execute the Switcher. The Switcher by then plants the aggressor's synchronization token into the Drive Application.

• At the point when this first switch is done, the Switcher copies the main synchronization token into the coordinated up envelope.

• The Drive Application adjusts with the aggressor's record.

• The aggressor at that point has ownership of the unfortunate casualty's synchronization token.

• The assailant at that point utilizes the stolen synchronization token to associate with the injured individual's document synchronization account (utilizing, for instance, the Switcher apparatus on the aggressor's machine).

• The Switcher instrument keeps running for the second time on the injured individual's machine (subsequently, "twofold switch") reestablishing the first synchronization token of

the person in question, basically reestablishing the Drive Application to its unique state [19].

4.4 Detection

It is very hard to distinguish a Man in the Cloud assault itself. There is a login procedure against the cloud benefit utilizing an alternate synchronization token (client). With no further setting around this occasion, the IDS or Proxy logs will at most demonstrate that an apparently real cloud adjust happened. Independent from anyone else that does not warrant an alert. A vigilant client could investigate the login geo area history by means of the cloud distinctive stages entrance, however that isn't the most dependable identification strategy [20].

There is a greatly improved possibility of recognizing the real social building assault by means of an email AV entryway, or the resulting Switcher malware documents situated on the objective host. Customary or conduct Antivirus arrangements ought to have the capacity to manage the majority of these contaminations. The advantage of depending on these advancements is that the assault is recognized from the get-go all the while and by then, it could at present be blocked, either physically or naturally

4.5 Prevention

The best method to keep the social designing assault that is probably going to go before the MITC assault is a mix of a thorough security mindfulness preparing and sufficient specialized controls [20].

4.6 Proposed Method

In this paper our proposed method is to use RSA encryption and decryption algorithm plus

mobile or auto generated code verification system to provide two steps security in file synchronization in cloud computing or mobile cloud computing (MCC).

4.7 Implementation Requirement

Initially we actualize our proposed technique in programming C in code square IDE, and we demonstrate how it work. Code Blocks is a free, open-source cross-organize IDE that supports different compilers including GCC, Clang and Visual C++. It is made in C++ using wxWidgets as the GUI tool compartment. Using a module designing, its capacities and features are described by the gave modules [21].

4.8 Challenges

Because of generate auto code and put it again for verification its needs more time to execute. But this proposed method can provide high level security.

CHAPTER 5

EXPERIMENTAL RESULTS AND DISCUSSION

5.1 (RSA) algorithm

In 1977, three authorities, Ron Rivest, Adi Shamir, and Len Adleman, made RSA calculation at MIT. RSA calculation [22] has been named subject to these three researchers. RSA Algorithm uses two keys open and private and which are hilter kilter since one is used for encryption and another is used for unscrambling.

The all inclusive community key encryption system has generally three phases:

- Key Generation
- Encryption
- Decryption

Key Generation

Before the data is encoded, Key age should be done. This technique is done between the Cloud master center and the customer. [23]

Steps:

• Pick two specific prime numbers a and b. For security purposes, the entire numbers p and q should be picked carelessly and should be of relative piece length.

• Enlist n = p * q

• Process Euler's totient work, Ø(n) = (p-1) * (q-1).

• Presently choose d as seeks after: d = e - 1(mod Ø(n)) i.e., d is multiplicative turn around

of e mod Ø(n).

• d is kept as Private-Key part, with the objective that d * e = 1 mod Ø(n).

• The Public-Key involves modulus n and individuals as a rule type e i.e., (e, n).

• The Private-Key contains modulus n and the private model d, which must be kept secret i.e., (d, n).

Encryption

Encryption is the route toward changing over extraordinary plain substance (data) into figure content (data).

Steps:

• Cloud authority association should give or transmit the Public-Key (n, e) to the customer who needs to store the data with him or her.

• Client data is by and by mapped to an entire number by using a settled upon reversible tradition, known as padding plan.

• Information is encoded and the resultant figure content (data) C can't avoid being: C = me (mod n)

• This figure message or mixed data is directly secured with the Cloud authority association.

Decoding

Decoding is the way toward changing over the figure content (information) to the first plain content (information).

Steps:

• The cloud customer requests the Cloud authority community for the data.

• Cloud authority association checks the validness of the customer and gives the mixed

data i.e., C.

• The Cloud customer by then unscrambles the data by figuring, m = Cd (mod n).

• When m is recovered, the customer can get the primary data by exchanging the padding plan.

5.2 Experimental results

Test information for actualizing RSA calculation [24].

Key Generation

• We have picked two unquestionable prime numbers p=17 and q=11

• Compute n=p*q, thusly n=17*11=187.

• 3. Process Euler's totient work, Ø(n)=(p-1)*(q-1), Thus Ø(n)=(17-1)*(11-1) =16*10= 160

• 4. Pick any entire number e, with the ultimate objective that 1 < e < 160 that is co prime to 160. Here, we picked e=7

• Compute d, d = e - 1(mod Ø(n)), Thus d=7-1(mod 160) = 23.

• Thus the Public-Key is (e, n) = (7, 187) and the Private-Key is (d, n) = (23,187).

This Private-Key is kept puzzle and it is known just to the customer.

Encryption

• The Public-Key (7, 187) is given by the Cloud pro community to the customer who wish

to store the data.

• Let us consider that the customer mapped the data to a number m=88.

• Data is encoded now by the Cloud authority association by using the relating Public-Key which is shared by both the Cloud pro community and the customer. C = 887(mod 187) = 11 [25].

• This mixed data i.e., figure content is by and by secured by the Cloud pro association

Decoding

• When the customer requests for the data, Cloud authority community will confirm the customer and passes on the mixed data (If the customer is considerable).

• The cloud customer by then unscrambles the data by figuring, M = cd(mod n) M=1123(mod 187) = 88 [25].

• Once the M regard is gotten, customer will get back the main data [21].

5.3 Process of proposed method

In the following flowchart figure 5.1 shows the step by step process of my proposed work.

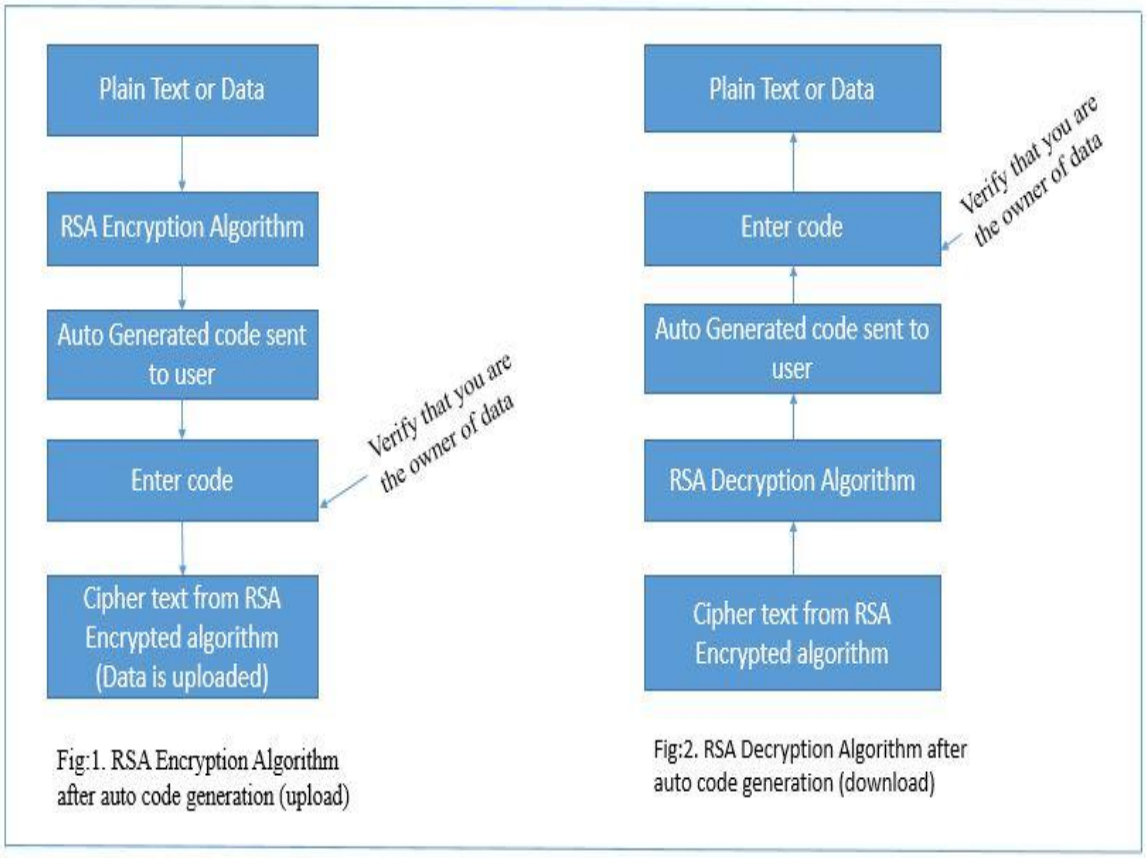

Figure 5.1: Flowchart of proposed method.

5.4 Discussion

Encryption is the route toward changing over one of a kind plain substance or data into figure content. Exactly when customer needs to store the data with him or her Cloud, master association should give or transmit the Public-Key (n, e) to the customer. Before data is mixed and the resultant figure content (data) C is controlled by the system :C = me (mod n) there is an auto created code send to the approve customer to his/her versatile. When he/she enter the right code then the figure message or mixed data is secured with the Cloud master community.

Decoding is the way toward changing over the figure content (information) to the first plain content (information). At the point when the client demands for the information, there is an auto produced code send to the validate client to his/her portable.

When he/she enter the correct code at that point Cloud specialist organization will conveys the scrambled information or figure content. The cloud client at that point unscrambles the information by registering, M = Cd (mod n). In the event that client enter the wrong code, information will be not appeared.

5.5 Implemented Output:

The following figure 5.2 show the implemented output screen of my proposed method.

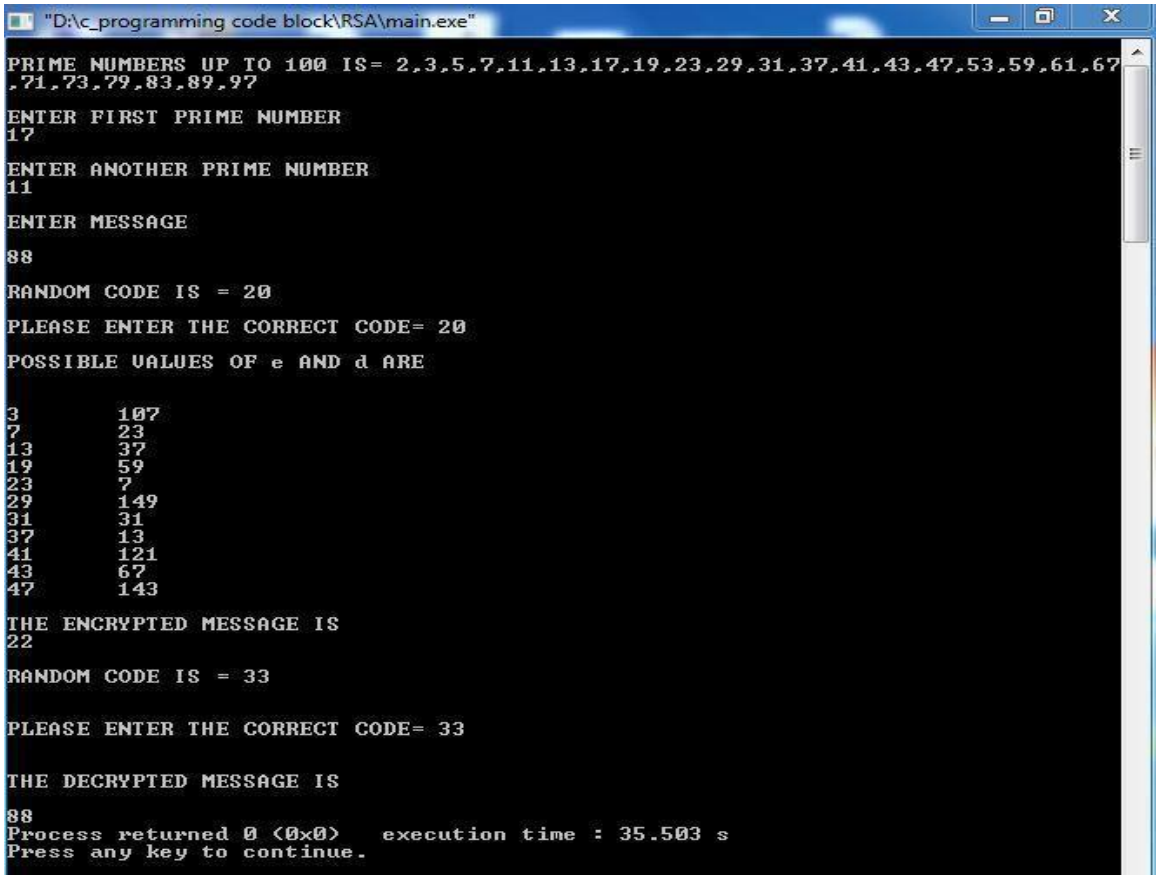

Figure 5.2: output screen.

CHAPTER 6

CONCLUSION

6.1 Conclusion

Conveyed processing is up 'til now another advancement where the cloud organizations are immediately accessible as on a pay for each usage start. Security of the Cloud relies upon trusted in preparing and cryptography. Simply the confirmed and endorsed customer can get to the data, paying little mind to whether some unapproved customer gets the data by chance or purposely and if gets the data similarly, customer can't unscramble the data and get back the main data from it. Just applying RSA calculation, scrambled information for cloud does not keep up a high security level. As the estimation of open key is shared, i.e., the estimation of e is known, there is high probability of deciding the estimation of d and decode the scrambled information. Thus, in this paper my proposed strategy gives more elevated amount of security in "Man in the cloud" assault in distributed computing by utilizing

RSA calculation in addition to auto produced code confirmation framework. Along these lines, if the attacker needs to get the information by unscrambling the last mixed message, will be difficult to get the correct plain text or data.

6.2 Implication for Further Study

In future we try to implement this proposed method in android base or web applications.

Because then the random number will be send to the valid user’s mobile number or email then he /she will put the correct number. If the valid used will put the correct value then they will seen or transfer message or data. Because of doing this data will be more secure and Man in the cloud attack will be reduce as the reason of two step security.

REFERENCES

[1] J.SRINIVAS1, K.VENKATA SUBBA REDDY2, Dr.A.MOIZ QYSER3 "CLOUD COMPUTING BASICS" <https://www.researchgate.net/publication/255994786_CLOUD_COMPUTING_BASICS>

[2] *J.srinivas, k.venkata subba reddy and dr.a.moiz qyser,* "cloud computing basics" international journal of advanced research in computer and communication engineering vol. 1, issue 5, july 2012 issn: 2278 – 1021.

[3] *Hwang, j.park,* "Decision factors of enterprises for adopting grid computing, grid economics and business models", 4th international workshop, GECON, 2007.

[4] *Peter mell, Timothy grance,* "The NIST definition of cloud computing" NIST special publication, online available at << http://dx.doi.org/10.6028/NIST.SP.800-145 >>

[5] *Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia*, "A View of Cloud Computing" Technical report no UCB/EEcs-2009-28, Feb 10,2009.

[6] *Amit kumawat,* (Jul 10,2013) "Cloud service model" online available at << http://www.cmswire.com/cms/information-management/cloud-service-models-iaas-saas-paas-how- microsoft-office-365-azure-fit-in-021672.php >>

[7] Amazon--, Amazon Elastic Compute Cloud (EC2), Amazon Web Services LLC, Tech. Rep., 2009. Online available at << http://aws.amazon.com/ec2/ >>

[8] Google, ―google app engine: run your web apps on google's infrastructure. Online available at << https://cloud.google.com/appengine/docs/ >>

[9] *Rachna Arora, Anshu Parashar,* "Secure User Data in Cloud Computing Using Encryption Algorithms", International Journal of Engineering Research and Applications (IJERA), ISSN: 2248-9622, Vol. 3, Issue 4, pp.1922-1926, Jul-Aug 2013, pp.1922-1926

[10] *Manpreet Kaur, Rajbir Singh.*, "Implementing Encryption Algorithms to Enhance Data Security of Cloud in Cloud Computing", International Journal of Computer Applications, Volume 70, No.18, May 2013.

[11] *Galli,H, Padmanabham.P,* "Data Security in Cloud using Hybrid Encryption and Decryption",

International Journal of Advanced Research in Computer Science and Software Engineering , Volume 3, Issue 10, October 2013.

[12] *Parsi Kalpana, Sudha Singaraju*, "Data Security in Cloud Computing using RSA Algorithm"

International journal of research in IJJRCCT Computer and communication technology, ISSN 2278-5841, Vol 1, Issue 4, September 2012.

[13] *Nandita Sengupta*, "Designing of Hybrid RSA Encryption Algorithm for Cloud Security" International Journal of Innovative Research in Computer and Communication Engineering *(An ISO 3297: 2007 Certified Organization)* Vol. 3, Issue 5, May 2015 (An ISO 3297: 2007 Certified Organization.

[14] Kuyoro S. O., Ibikunle F. & Awodele O 'Cloud Computing Security Issues and Challenges'

https://www.researchgate.net/publication/285011991_Cloud_Computing_Security_Issues_and_Challenges.

[15] *Joy Ma*, (Dec 14, 2015) "Security" Online available at << https://www.incapsula.com/blog/top-10-cloud-security-concerns.html >>

[16] Online available << at http://sites.force.com/appexchange/home>>, last accessed on 10-10-2018 at 10:00 pm

[17] *Joy Ma*, (Dec 14, 2015) " Top 10 security concerns for cloud base services" Online available at https://www.incapsula.com/blog/top-10-cloud-security-concerns.html.

[18] Online available at https://www.wordfence.com/learn/how-to-prevent-cross-site-scripting-attacks/

[19] *Stallings, W,* "Cryptography and Network Security Principles and Practice", Prentice Hall. Online available at << https://www.imperva.com/docs/HII_Man_In_The_Cloud_Attacks >>

[20] *Frank Siemons*, "How to detect and prevent a man-in-the-cloud attack" Online available at << http://searchcloudsecurity.techtarget.com/tip/How-to-detect-and-prevent-a-man-in-the-cloud- attack>>

[21] Code block IDE, online available at << www.codeblocks.org >>

[22] *Amandeep Kaur, Sarpreet Singh*, "An Efficient data storage security algorithm using RSA Algorithm" Volume 2, Issue 3, March 2013 ISSN 2319 – 4847. At www.ijaiem.org.

[23] *N.padmaja, priyanka koduru*, "providing data security in cloud computing using public key cryptography". International journal of engineering sciences research-ijesr. Vol 04, special issue 01, 2013.

[24] Online key generation .Online available at <<

http://www.mobilefish.com/services/rsa_key_generation/rsa_key_generation.php >> ,last accessed on 11-8-2018 at 11:00 am

[25]Online mod calculator, online available at << https://www.mtholyoke.edu/courses/quenell/s2003/ma139/js/powermod.html >> last accessed on 11-9-2018 at 8:00 pm

[26]www.google.com/search?q=A+basic+cloud+computing+environment+pic&oq=A+basic+cloud+computing+environment+pic&aqs=chrome..69i57j69i64l2.17492j0j7&sourceid=chrome&ie=UTF-8

[27] https://www.diva-portal.org/smash/get/diva2:830736/FULLTEXT01.pdf

[28] https://www.cs.northwestern.edu/~ychen/classes/msit458-w10/cloudComputingSec_p3.pptx

[29] https://www.researchgate.net/publication/267697749_Security_Challenges_in_Cloud_Computing

[30]https://www.google.com/search?q=Cloud+challenges+2017+vs+2016&tbm=isch&source=iu&ictx=1&fir=oM6FWXRg8vmiDM%253A%252CHm2P-A5KBJSaSM%252C_&usg=AI4_-kQqV1naLbERrfp2PaOni1iqFiZ-mA&sa=X&ved=2ahUKEwiky-m824bfAhXUXysKHSEbDYYQ9QEwAnoECAUQBA#imgrc=oM6FWXRg8vmiDM: