

A Cloud based Data Integrity and Confidentiality System

By

ShowmikZaman Chowdhury

ID: 183-17-385

Department of Management Information System (MIS)

Daffodil International University, Dhaka

This Report Presented in Partial Fulfillment of the Requirements for the Degree of
Master of Science in Management Information System.

Supervised By

Professor Dr. Md. Ismail Jabiullah

Professor

Department of CSE

Faculty of Science and Information Technology

Daffodil International University



DAFFODIL INTERNATIONAL UNIVERSITY

DHAKA, BANGLADESH

DECEMBER 2019

APPROVAL

This Thesis Titled “A Cloud based Data Integrity and Confidentiality System”, submitted by **Showmik Zaman Chowdhury** to the Department of Management Information System, Daffodil International University, has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of Master of Science in Management Information System and approved as to its style and contents.

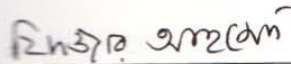
BOARD OF EXAMINERS



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
Associate Professor and Associate Head
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University



Dr. Fizar Ahmed
Internal Examiner
Assistant Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University



Dr. Mohammad Shorif Uddin
External Examiner Professor
Department of Computer Science and Engineering
Jahangirnagar University

ACKNOWLEDGEMENT

First I express my heartiest thanks and thankfulness to all-powerful Allah for his awesome gift makes me conceivable to finish the last year venture/temporary job effectively. I am extremely thankful and wish my significant obligation to **Professor Dr. Md. Ismail Jabiullah , Department of CSE, Daffodil International University, Dhaka**. Profound information and unmistakable fascination of my administrator in the field of "**A Cloud based Data Integrity and Confidentiality System**" causes me to complete this proposal paper. His unending tolerance, academic direction, ceaseless consolation, consistent and lively supervision, useful analysis, important exhortation, perusing numerous mediocre draft and redressing them at all stage have made it conceivable to finish this proposal.

I would like to express my heartiest gratitude to **Dr. Syed Akhter Hossain, Professor and Head, Department of CSE**, for his kind help to finish my thesis and also to other faculty members and the staff of MIS department of Daffodil International University.

I might want to thank my whole course mates in Daffodil International University, who participated in this talk about while finishing the course work.

At last, I should recognize with due regard the steady help and patients of my folks.

Certification

I hereby declare that, this thesis has been done by me under the supervision of Professor **Dr. Md. Ismail Jabiullah, Professor, Department of Computer Science and Engineering**, 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:



Professor **Dr. Md. Ismail Jabiullah**,
Professor
Department of CSE
Daffodil International University

Submitted by:



Showmik Zaman Chowdhury
ID: 183-17-385
Department of MIS
Daffodil International University

ABSTRACT

Distributed computing alludes to a framework wherein data preparing and capacity can appear some good ways from any gadget. Research appraises that supporters worldwide will arrive at 15 billion through the finish of 2014 and 18 billion by means of at the completing of 2016. Because of developing utilization of gadgets the necessity of distributed computing in gadgets ascend, which advances Cloud Computing. All contraptions require tremendous carport usefulness and most extreme CPU speed. As we're putting away records on cloud there can be an issue of certainties security. As there might be chance identified with information carport numerous IT specialists are not indicating their enthusiasm for the heading of Cloud-Computing. To guarantee the clients' records rightness inside the cloud, appropriate here we're giving a powerful component striking element of data uprightness and privacy. This methodology proposed an answer which utilizes the AES set of rules and component of hash work together with different cryptography contraption to offer better security to the data put away on the cloud. This model can't best settle the issue of carport of monstrous realities, anyway also guarantee that it will give information get passage to oversee instruments and ensure sharing records documents with secrecy and uprightness.

Table of Contents

INDEX	PAGE NO
APPROVAL.....	i
CERTIFICATION.....	ii
ACKNOWLEDGEMENT.....	iii
ABSTRACT.....	iv
Chapter 1: Introduction	(1-4)
1.1 Introduction	1
1.2 Motivation	2
1.3 Objective	3
1.4 Expected outcome	3
1.5 Report Layout	4
Chapter 2: Literature Reviews	(5-6)
2.1 Introduction	5
2.2 Related Works	5
2.3 Comparative Studies	6
2.4 Challenges	6
Chapter 3: Background Analysis	(7-13)
3.1 AE	7
3.2 Hash algorithm	10
3.3 Cloud section of the system	11
3.4 Cloud Computing Technology	12
3.5 Cloud Computing Technology Managed	12
3.6 Cloud Storage Managed & Cloud Service Providers Store	13

Chapter 4:Proposed model	(14-18)
4.1 Proposed Schema	14
4.2 Flow Diagram	14
4.3 Concept	15
4.4 DWT SVD Based Image Steganography	17
4.5 Integrity Check Using TheSha 512 Hash Function	18
Chapter 5: EXPERIMENTATION AND RESULT	(19-22)
5.1 Experimental Results	19
5.2 Cover and Secret Images	19
5.3 Results of the Encryption-based AES Algorithm	21
5.4 Robustness Test of the Proposed Method	22
Chapter 6: Conclusion	(24)
6.1 Conclusion	24
6.2 Scope of the Problem References	24
References	25

LIST OF FIGURES

Figure 3.1.1: Advanced Encryption Standard (AES)	7
Figure 3.2.1: Hash Function	9
Figure 3.2.2: Hashing Algorithm	10
Figure 3.2.3: Hashing Rules	10
Figure 3.3.1: Cloud Computing	11
Figure 3.5.1: Cloud Computing Resource Process	12
Figure 3.6.1: Cloud Service Providers Store	13
Figure 4.2.1: Flow Diagram	14
Figure 4.3.1: Process of The Encrypting And Embedding Algorithm	15
Figure 4.3.2: Process of Retrieving The Secret Image Algorithm	16
Figure 5.2.1: Cover and secret images	19
Figure 5.3.1: Encrypted and decrypted secret image	21
Figure 5.4.1: StegoAnd Extracted Images	22
Figure 5.4.2: Reliability Test	22

LIST OF TABLE

Table 1: Cryptographic Performance	21
Table 2: Embedding and Extraction Time	2

CHAPTER 1

INTRODUCTION

1.1 Introduction

Putting away data remotely inside the cloud in a bendy on-request way gets alluring favorable circumstances expressions of carport and calculation. A great deal of works had been done on structuring faraway insights respectability confirming conventions that may get section to measurements uprightness to be checked without totally downloading the realities. In any case, those type of strategies manage the respectability of scrambled content or plain content. The issue is that acting calculations on scrambled data is a troublesome task. Rather, measurements might be anonym zed to decorate private ness. Anonymization alludes to a private ness redesign system that interprets measurements with the goal that you can make the data useless to anybody other than the realities owner. Distributed computing offers new type of the contributions to clients to completely utilize the favors of Cloud Computing. Here delicate realities is spared and handled outside the contraptions on a concentrated figuring stage put in mists. The essential trouble in the utilization of distributed computing is verifying the realities of character put away on cloud. The information/document of a client might be sensitive; any unapproved individual can do modifications in it, to harm the measurements. So the main issue of cloud Issuer Company is to offer the security of data/archives made and controlled on a gadget or cloud server. To secure information of individual, encryption is utilized to relentless data inside the cloud. New help structures are fundamental to adapt to the wellbeing issues of the clients for the use of cloud methods. In this investigations paper the end objective is to consent a fused structure/answer for achieving the information security on cloud condition in different attainable circumstances, all together that this innovation might be executed in uses of bendy nature with none blemish.

1.2 Motivation

Startups have many reasons for moving from an intranet-based, capital-buy structured version of IT infrastructure to a software-fashion call for and cloud-based totally issuer. These include the subsequent:

Scalability – Cloud computing allows startups control moving computing necessities through manner of providing greater flexibility in the computing offerings they buy. A cloud-based definitely IT infrastructure is more versatile – considerably in phrases of scalability – than is local, intranet-primarily based infrastructure.

Reliability – Because cloud providers can assemble extra redundancy proper into a machine than a agency can assemble into its personal intranet, the cloud dealer can unfold its infrastructure investment expenses across its complete patron base, allocating assets as essential.

Virtualization – Because cloud-primarily based IT infrastructure may be virtualized and geographically dislocated, startups are free of getting to keep in mind the bodily region of its IT infrastructure and statistics centers in corporation operations alternatives.

Affordability – Under conventional infrastructures, startups won't gather – or have economic wherewithal to buy – certain features which may be often furnished to cloud computing customers at remarkable discounts. How do these blessings skip on to startups and different small companies? Because the marginal charge to the cloud computing business enterprise of many functions (consisting of more safety) may be very low (or even negligible), otherwise unaffordable services can be supplied without spending a dime to startups the use of cloud computing alternatives.

1.3 Objectives

Putting away data remotely inside the cloud in a bendy accessible if the need arises for way acquires engaging favorable circumstances terms of capacity and calculation. A superior unpracticed insights anonymization plot is proposed which spares the computational vitality and capacity spot of the client through acting anonymization and deanonymization in the safe enclave. CC (distributed computing) manages new kind of the contributions to clients to truly utilize the advantages of Cloud Computing. Here tricky insights is spared and handled outside the gadgets on a concentrated processing stage situated in mists. The fundamental issue inside the use of distributed computing is verifying the information of individual put away on cloud. This variant can't best treatment the issue of carport of huge insights, yet in addition guarantee that it'll give records get to control instruments and make certain sharing certainties documents with privacy and uprightness.

1.4 Expected Outcome

This methodology proposed an answer which utilizes the AES set of rules and instrument of hash highlight close by different cryptography gear to offer better wellbeing to the records spared at the cloud. This model can't best take care of the issue of carport of large data, anyway likewise guarantee that it'll convey data get section to oversee instruments and guarantee sharing information documents with secrecy and uprightness.

1.5 Report Layout

The layout of this report is described below:

- In chapter 1 I have covered the introduction to my Thesis, motivation for building this kind of system, objectives and goals of the A Cloud based Data Integrity and Confidentiality System, what I have planned or the expected outcome of the application and the ultimate layout of this report.
- In chapter 2 I have added some related works and some studies that helped me a lot in this application. I also included the problems and challenges that I faced during the research development phase.
- In chapter 3 I have talked about AES, Hash algorithm, Cloud section of the system, Cloud-Computing-Technology, Cloud-Computing-Technology Managed, and Cloud Storage Managed & Cloud Service Providers Store.
- In chapter 4 I have specified the whole process of this system using some Proposed Schema, Concept, Secret Image Encryption, DWT-SVD-based Image Steganography, Integrity Check Using the SHA-512 Hash Function.
- In chapter 5 I included the specification that I have described about Introduction of Experiment, Experimental Results, Results of the Encryption-based AES Algorithm, Robustness Test of the Proposed Method.
- In chapter 6 I have added the conclusion and challenges details and analysis Scope of the Problem.

CHAPTER 2

Literature Review

2.1 Introduction

In this chapter I will dialogue about the associated works, case studies, scope of the problem, challenges. After solving the plan I have commenced analyzing on some different related packages and case studies. Summarize of those are delivered on this bankruptcy.

2.2 Related Works

El-Makkaoui et al. offered an more potent encryption scheme, known as Cloud (RSA), based totally at the Rivest-Shamir Adleman (RSA) set of rules. Cloud (RSA) utilizes two discrete keys: assessment and private keys. The assessment key $e = (M)$ is used to put into effect operations on encrypted statistics thru a 3rd birthday party. The non-public key $pr = (M, e, okay)$, which is thought high-quality to the information proprietor, is utilized to encode and decode information. The safety of the private key is primarily based on two factors: i) The hassle of figuring out the high factorization of (M) ; ii) The root problem of Cloud (RSA). Regardless of whether the factorization of (M) is given, unscrambling the figure content encoded utilizing the Cloud (RSA) encryption conspire is uncommonly hard because of the reality $(e$ and sufficient) are private. Mandala et al. proposed a crypto-stego approach, in which the steganography approach embedded non-public records through way of the usage of a pixel-mapping approach. The encryption and decryption machine uses a genetic set of rules, which competencies crossover and mutation operations. Cryptography and steganography moreover use a mystery key, that's generated with the aid of combining sure functions of the spread picture and the mystery key of the individual. Bhandari et al. Proposed a scheme referred to as hybrid encryption (RSA) together with AES via improving the safety fashionable of the RSA set of rules. Wang et al. provided degradation and encryption strategies for Portable Network Graphics (PNG). In particular, the prefix and noise generation strategies had been advanced for PNG degradation. In addition, a changed generalized Feistel scheme modified into developed for encrypting PNG. Although existing structures have accomplished confidentiality, they stay unsuccessful in

retaining facts integrity. Consequently, a constant gadget should be advanced to attain powerful performance through preserving confidentiality with records integrity.

2.3 Comparative Studies

After reviewing some other similar approaches and their case studies I have sorted common features and unique features of each. Most of them are built for specific purpose for their own demand.

2.4 Challenges

A) The Solution Prevent Data Leakage The cloud is a multi-tenant surroundings, in which resources are shared. It is likewise an outside birthday celebration, with the capacity to get admission to a purchaser's facts. Sharing garage hardware and setting data in the palms of a provider seems, intuitively, to be volatile. In addition, secure harbor and privacy laws make manage over your records essential. Whether it happens due to get proper of entry to by using manner of presidency businesses, a malicious hacker attack or maybe an accident, records leakage might be a excellent safety or privacy violation.

B) Unique Cloud Credentials Access to a given pool of storage is primarily based on credentials, and if we're lumped collectively with a few other set of clients and percentage the same credentials, there is a danger that certainly one of them might also need to gain the ones credentials and get proper of entry for your records. They would now not be capable of decipher it, assuming it's far encrypted, however they may delete the files.

C) Holds the Crypto Keys There is a danger that customers will no longer want to spark off the cryptography, which then compromises safety. Key manage should be so easy that users aren't even privy to it: Encryption must be computerized. There need to be no manner to show it off. This manner, if there may be no insecure mode, then there may be no danger of someone through twist of fate sending unencrypted, inclined information to the cloud.

Chapter - 3

Background analysis

3.1 Advanced Encryption Standard (AES)

Propelled Encryption Standard (AES) calculation no longer least difficult for security however also for first class pace. Both equipment and programming execution are faster regardless. New encryption in vogue supported by method for NIST to supplant DES. Scrambles records squares of 128 bits in

10, 12 and 14 round contingent upon key length as demonstrated in Figure 3.1.1. It might be applied on various stages explicitly in little gadgets. It is carefully analyzed for parts wellbeing applications.

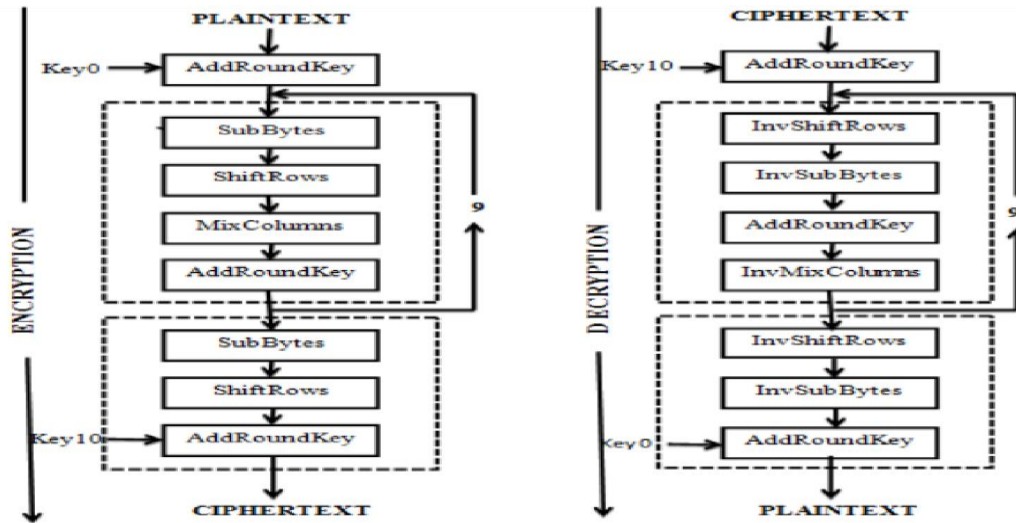


Figure 3.1.1: Advanced Encryption Standard (AES)

Algorithm Steps:

I. These means used to encode 128-piece square

1. These means used to encode 128-piece square.
2. Introduce nation cluster and add the underlying round key to the beginning exhibit.

Perform spherical = 1 to nine: Execute Usual Round.

Four. Execute Final Round.

Five. Corresponding cipher text chunk output of Final Round Step ii. Usual Round:

Execute the subsequent operations which may be described above. 1. Sub Bytes

2. Shift Rows

3. Blend Columns four. Include Round Key, the utilization of K (circular) iii. Last Round: Execute the ensuing tasks which can be characterized previously.

1. Sub Bytes
2. Shift Rows
3. Add Round Key, the usage of K (10)

IV. Encryption: Each spherical includes the following four steps:

- I. Sub Bytes: The principal change, Sub Bytes, is utilized at the encryption web site on the web. To substitution a byte, we translate the byte as two hexadecimal digits.
- II. Move Rows: In the encryption, the change is known as Shift Rows. Iii. Blend Columns: The Mix Columns change works on the section level; it changes every segment of the usa to a the present segment.
- III. Include Round Key: Add Round Key continues each segment in turn. Include Round Key furnishes a round key expression with each usa segment framework; the activity in Add Round Key is lattice option. A definitive advance incorporates XO Ring the yield of the past 3 stages with four terms from the significant thing plan. Also, the last round for encryption does now not include the "Blend sections" step. [8]

IV. Decryption:

Decoding includes switching every one of the means taken in encryption utilizing reverse highlights like: Inverse elective bytes, Inverse move lines, Add round key, and Inverse mix segments. The 0.33 advance comprises of XO Ring the yield of the past two stages with 4 words from the significant thing motivation. What's more, the staying round for decoding does never again include the "Reverse mix segments" step.

3.2 Hash function

Hash capacities are amazingly valuable and show up in about all realities security applications. A hash trademark is a scientific capacity that changes over a numerical information cost into each other packed numerical expense. The contribution to the hash include is of discretionary span yet yield is for the most part of fixed term.

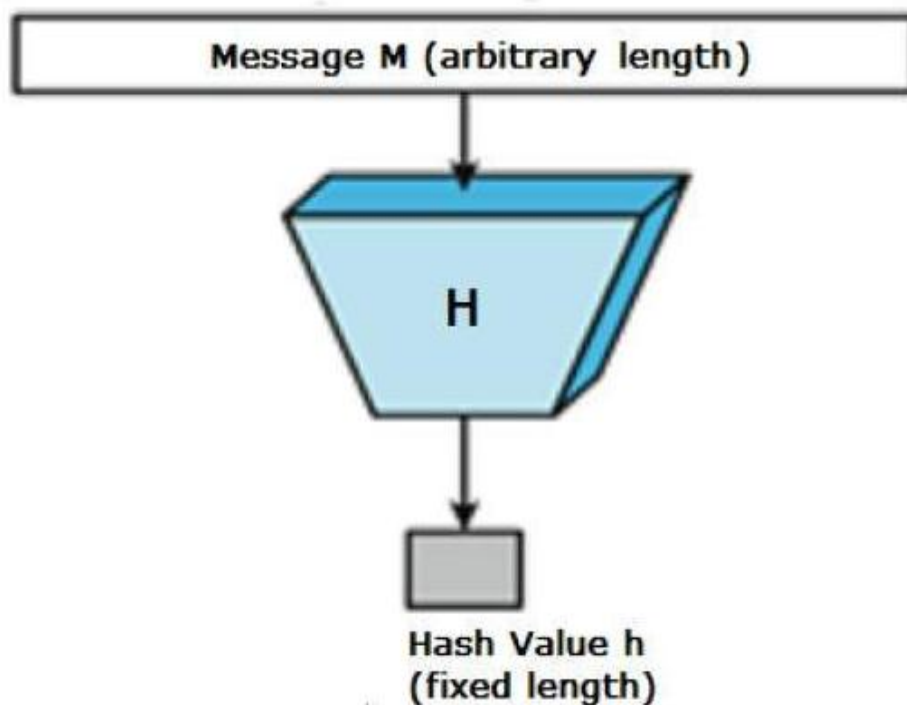


Figure 3.2.1: Hash Function

Hashing Algorithms

At the core of a hashing is a scientific trademark that works on two steady length squares of records to make a hash code. This hash work administrative work the piece of the hashing calculation. The size of every record square differs relying upon the calculation. Regularly the square sizes are from 128 bits to 512 bits. The accompanying occurrence shows hash include –

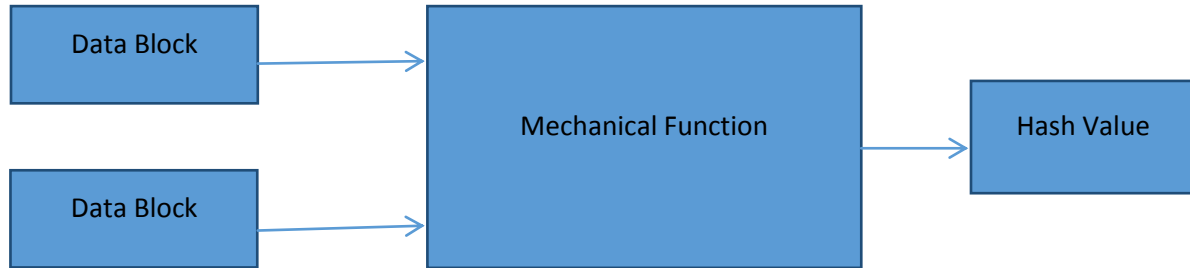


Figure 3.2.2: Hashing Algorithm

Hashing set of rules includes rounds of above hash trademark like a square figure. Each round takes an enter of a fixed length, normally a total of the latest message square and the yield of a definitive circular. This procedure is rehashed for the same number of rounds as are required to hash the total message. Schematic of hashing set of rules is delineated in the accompanying model –

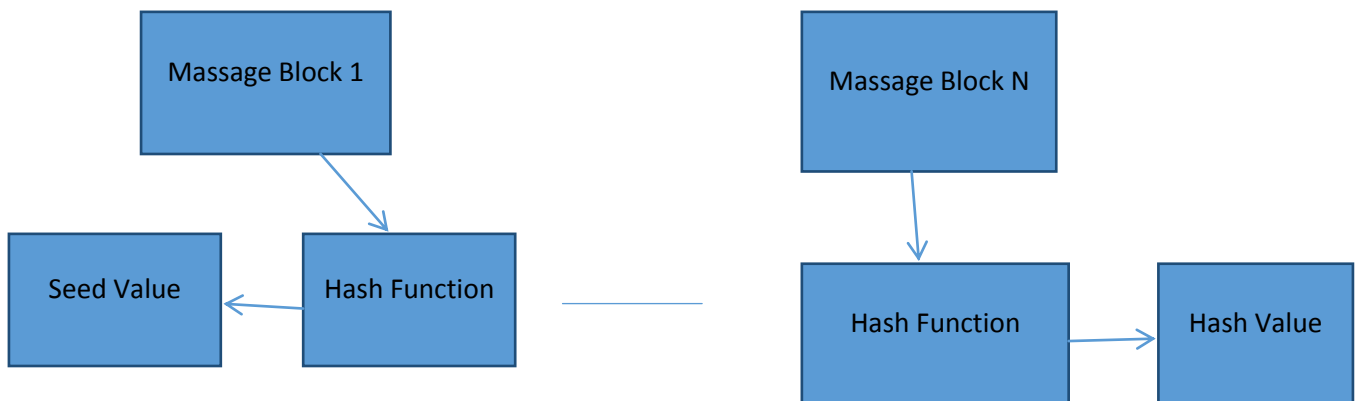


Figure 3.2.3: Hashing Rules

Since, the hash expense of first message square turns into an enter to the second hash activity, yield of which changes the final product of the 1/3 activity, etc. This impact, alluded to as a torrential slide effect of hashing. Torrential slide sway outcomes in altogether exceptional hash esteems for 2 messages that change by utilizing even a solitary tad of insights. Comprehend the distinction between hash trademark and set of rules adequately. The hash include produces a hash code by method for taking a shot at two squares of fixed-length twofold records. Hashing calculation is a framework for the utilization of the hash work, determining how the message could be harmed up and the manner in which the results from past message squares are fastened together.

3.3 Cloud Section of The System

They are linked to every different thru a network, typically the Internet. The System is the aspect of the laptop person or patron. The System is ‘the cloud’ phase of the machine.

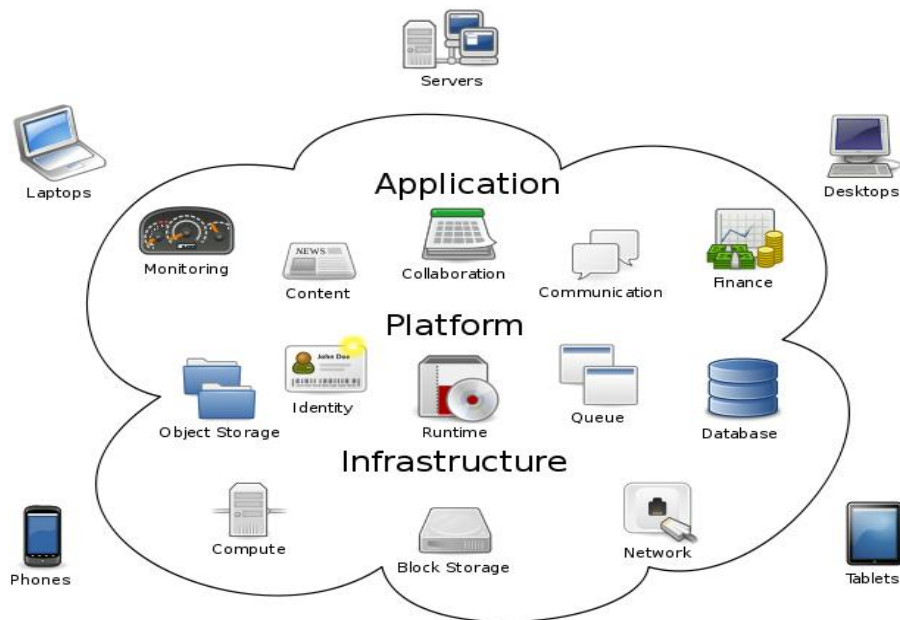


Figure 3.3.1: Cloud Computing

The System comprises of the buyer's PC or workstation network. Likewise the application indispensable to get to the distributed computing framework. It isn't fundamental that every one distributed computing frameworks have the equivalent individual interface. On the System of the

cloud period framework, there are different PCs, servers and realities carport structures that make up the cloud. A distributed computing framework should likely incorporate any pc program, from actualities handling to video games. For the most part, every application may have its own submitted server.

3.4 Cloud Computing Technology

Enormous organizations regularly require heaps of virtual carport gadgets. Distributed computing frameworks need at any rate times the measure of capacity contraptions to keep up buyer insights put away. That is because of the truth the ones gadgets once in a while harm down. A cloud apparatus makes duplicates of customers' information, to hold it on different contraptions. This methodology of making duplicates of insights as a reinforcement is called repetition. Find out around 7 distributed computing security hazards in component, by method for tapping on the hyperlink featured.

3.5 Cloud Computing Technology Managed

Distributed computing is an Internet-based figuring rendition which offers a few resources through Cloud Service Providers (CSP) to Cloud Users (CU) accessible if the need arises for premise without looking for the hidden framework and pursues pay-in step with-use premise. It enables virtualization of physical assets so one to can improve proficiency and achievement of numerous duties at the indistinguishable time.

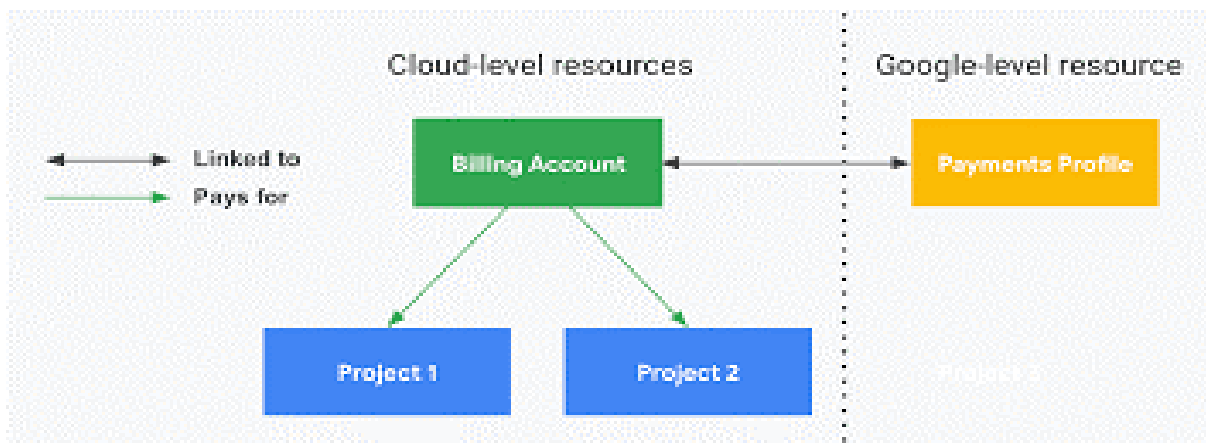


Figure 3.5.1: Cloud Computing Resource Process

A critical server manages the cloud device. Its reason is to manage traffic and customer needs to make certain the entirety runs smoothly. It pursues a set of rules referred to as protocols and uses a unique form of software known as center ware. Middle ware permits networked computers to speak with each different.

3.6 Cloud Storage Managed & Cloud Service Providers Store

Cloud Computing Environment (CCE) offers several deployment fashions to symbolize numerous training of cloud owned thru enterprise or institutes.

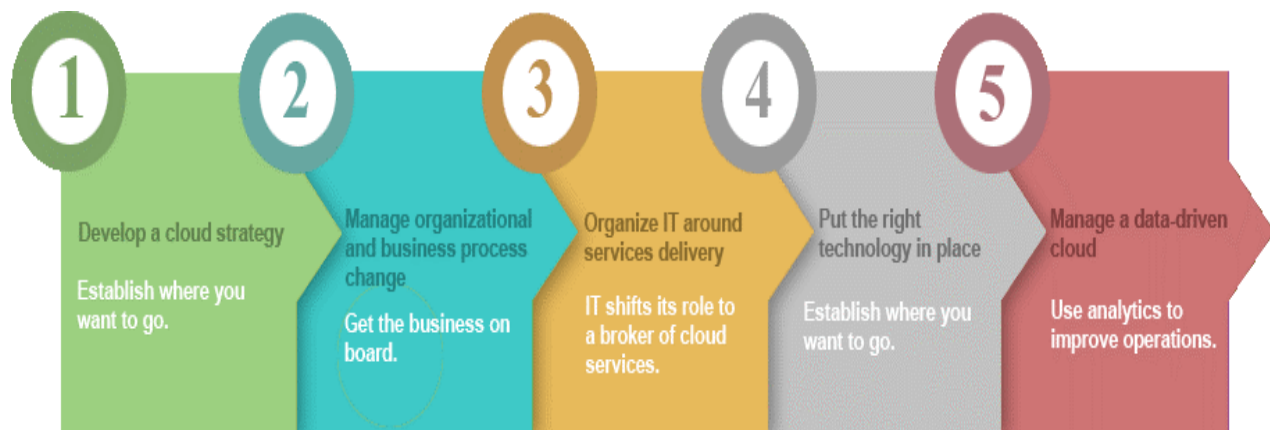


Figure 3.6.1: Cloud Service Providers Store

If the cloud Carrier Company or cloud Technology Company has more than one customers, there's probably to be an excessive demand for storage vicinity.

It's feasible to 'idiot' a bodily server into thinking that it's truly more than one servers, each strolling its personal independent running tool. This method is referred to as server virtualization, which reduces the want for physical machines. This technique maximizes the output of character servers. So there we've were given it – a completely quick take a look at what cloud computing involves and the manner it really works. Also a few use cases and dangers for this all of sudden growing era, noted considerably as 'the cloud'.

CHAPTER 4

PROPOSED MODEL

4.1 Proposed Scheme

The basic concept of the proposed scheme is described in Section four.2. The encrypted secret picture is provided in Section four. Three. The steganography approach is discussed in Section 4.four. Finally, integrity check the usage of the SHA-512 hash function is supplied in Section 4.five

4.2 Flow diagram

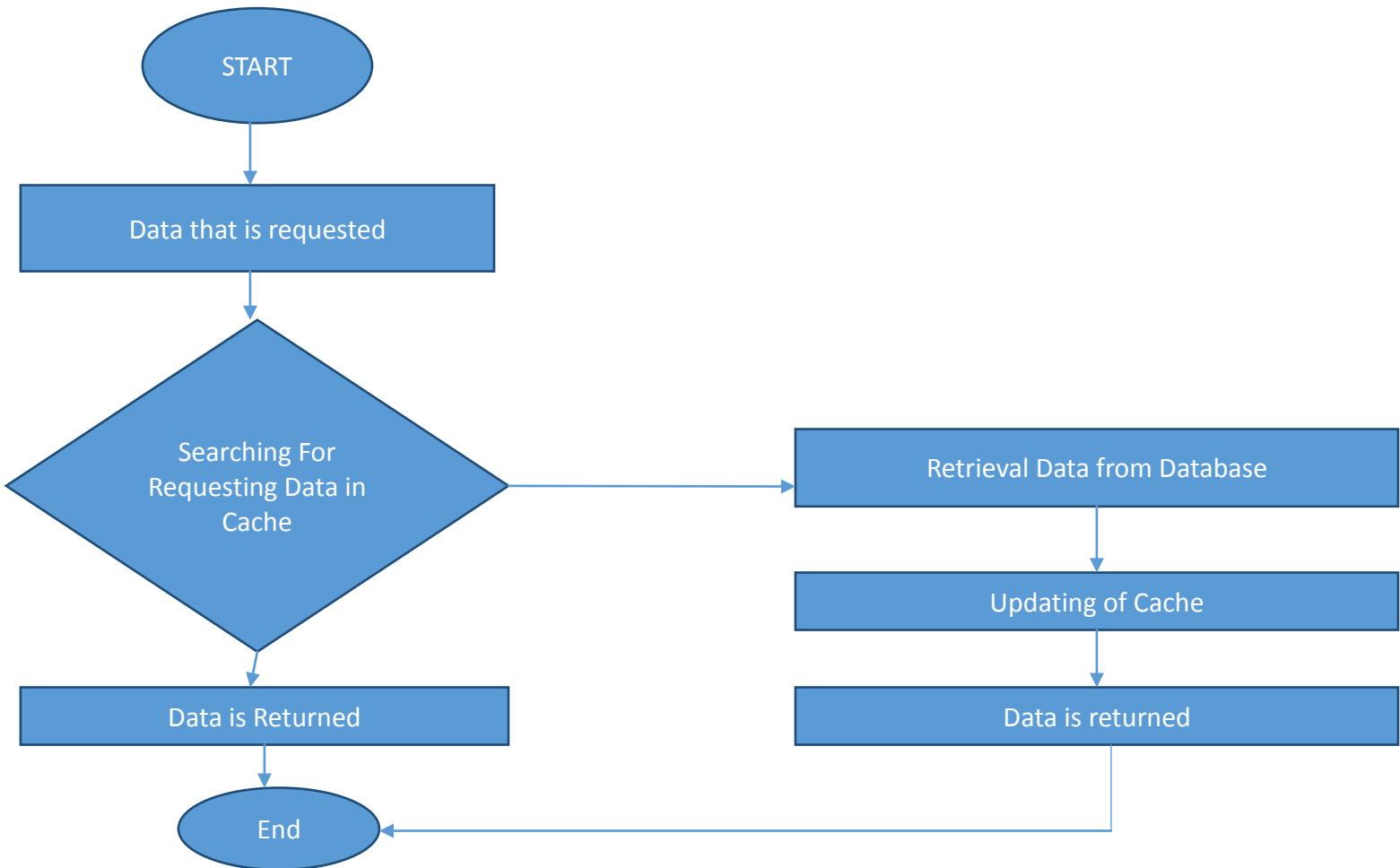


Figure 4.2.1: Flow Diagram

4.3 Concept

Once log in is a hit, the records owner will pick the call of the sport photograph and keep it on the cloud server. The thriller picture selected thru the proprietor may be encrypted the use of the AES set of rules. Then, the encrypted image can be embedded into the duvet picture using the hybrid steganography scheme DWT-SVD to get the stego image. Thereafter, SHA-2 is used to generate the hash price of the stego picture in advance than its miles stored inside the cloud to maintain facts integrity. The hash rate of the photograph is likewise generated the usage of SHA-2 after the photograph is retrieved from the cloud. Both hash values are as compared the usage of the verification manner to validate whether the statistics stored in the cloud are altered; then, the name of the game picture is obtained. The proposed device is illustrated in both Figures.

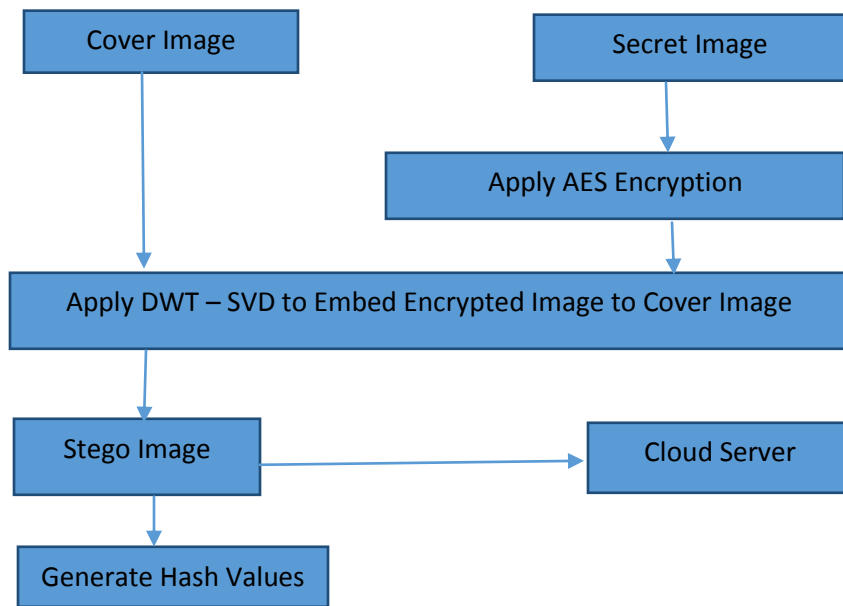


Figure 4.3.1: Process of The Encrypting And Embedding Algorithm

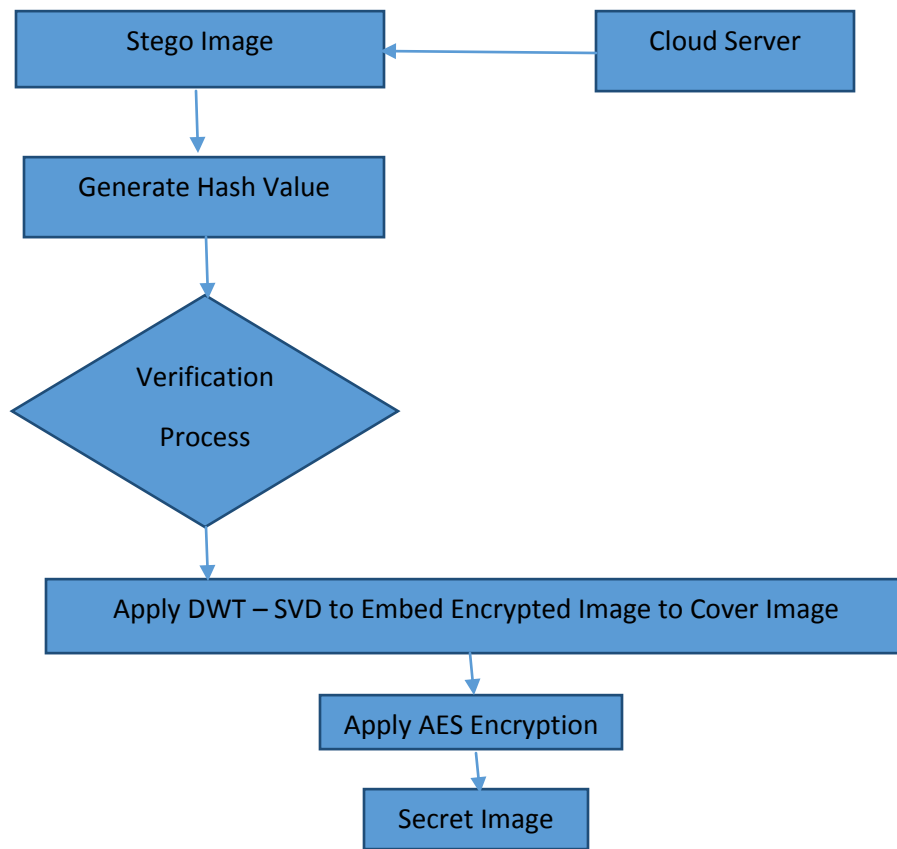


Figure 4.3.2: Process of Retrieving the Secret Image Algorithm

4.4 Secret Image Encryption

The shade photograph comprises a fixed of pixels. Each pixel has three essential components: purple (R), green (G) and blue (B). Each component is represented by way of eight bits. The color components of the secret photo are for my part encrypted. All the RGB components are mixed to provide the colour picture.

The encryption and decryption algorithms of the secret picture are offered as in

Algorithms 1

Encryption method 1: The shade additives (R, G and B) of the name of the game photograph are extracted. 2: The AES set of rules and unique keys are used to encrypt every colour thing. 3: All the additives are mixed to attain the final encrypted picture.

Algorithm 2

Decryption process 1: To extract the encrypted photograph, the stego image is retrieved from the cloud and further decomposed into one-of-a-kind shade additives. 2: The AES set of rules and the respective keys are used to decrypt the shade components. Three: All the additives are combined to reap the decrypted photograph.

4.4 DWT-SVD-based Image Steganography

The algorithms used for the DWT-SVD-primarily based photo steganography scheme are supplied as in Algorithms 3 and 4.

Algorithm 3

Embedding Algorithm 1: The cowl and encrypted snap shots are decomposed into sub-bands the use of DWT. 2: SVD is achieved on the HL sub-band to transform the cover and encrypted photos. 3: The encrypted photograph is embedded into the host image. four: Inverse SVD is completed at the embedded image. five: Finally, inverse DWT is implemented to get the stego photograph.

Algorithm 4

Extraction Algorithm 1: The stego photograph the use of DWT is decomposed into sub bands. 2: SVD is accomplished at the HL sub-band of the decomposed stego image. three: Extraction is carried out to the resultant SVD image. four: Inverse SVD is completed on the resultant image. 5: Finally, inverse DWT is completed to get the encrypted photo.

4.5 Integrity Check Using the SHA-512 Hash Function

The SHA-512 hash function is used to cast off the clash among hash values to reap facts integrity. Firstly, the hash rate of the stego photo is precompiled. Subsequently, the stego photo is dispatched to the cloud and the computed hash price is stored within the community repository. When the customers want to verify statistics integrity, the file is retrieved from the cloud and the hash fee of this file is recomputed. Then, the values are matched. The record is undamaged if the precompiled and recomputed hash values healthy. If those values do now not healthy, then the report has been tampered with and its integrity has been compromised. The set of rules of information integrity is defined as in

Algorithm 5

Data Integrity Algorithm 1: The stego photograph is sent to the cloud after computing its hash fee. 2: The computed hash cost of the stego image is saved within the secured close by repository. 3: After the stego picture is downloaded from the cloud, its hash price is recomputed. 4: The hash values are matched to attain statistics integrity.

Chapter - 5

EXPERIMENTATION AND RESULT

5.1 Experimental Results

The photos used on this experiment are provided in Section 4.2. The outcomes of the encryption-primarily based AES set of rules are discussed in Section 4.three. Finally, the robustness take a look at for the proposed scheme is defined in Section four.4.

5.2 Cover and Secret Images

The sizes of the duvet and thriller snap shots used in the experiments are 512×512 and 256×256 , respectively.



Figure 5.2.1: Cover and secret images

The genuine and mystery photos are tested in Figures 6(a) and three(b), respectively. Several best measures, collectively with top sign-to-noise ratio (PSNR), imply square errors (MSE) and normalized correlation (NC), are used to evaluate the overall performance of the stego and extracted photos. PSNR is a metric used to check the perceptual similarity between the original and stego pictures. It may be defined as follows:

$$PSNR = 10 \log \frac{(255)^2}{MSE}$$

(2) Where MSE is calculated among the host image A and the stego photo as follows:

$$MSE = \frac{1}{MM} \sum_{i=1}^M \sum_{j=1}^M (A - A_s)^2.$$

The stego photograph appears almost same to the host photograph while accurate imperceptibility is completed. That is, the host photograph is unaffected by using the embedding approach. A PSNR above forty dB shows exact perceptual constancy. In the check, PSNR is above 40 dB, thereby indicating the effectiveness of the proposed scheme. NC is used to evaluate the feasibility of the extracted thriller photograph. The similarity among mystery photographs is represented thru the quantity of mismatched facts some of the inserted and extracted secret pictures.

$$corr(d, d^*) = \frac{\sum_{i=1}^N (d_i - \bar{d})(d_i^* - \bar{d})}{\sqrt{\sum_{i=1}^N (d_i - \bar{d})^2} \sqrt{\sum_{i=1}^N (d_i^* - \bar{d})^2}},$$

NC for legitimate mystery pix, which represents the traits of the extracted mystery image, is described as Where (d_i) , (d_i^*) are the specific and modified data, at the same time as \bar{d} is the imply of the real records.

5.3 Results of the Encryption-based AES Algorithm

The photo encryption manner the usage of the AES of the name of the game photo acquired as a color picture is offered in Figure 7(a). The encrypted photo is produced by combining all the coloration additives, as proven in Figure 7(b). In Figure 7(c),

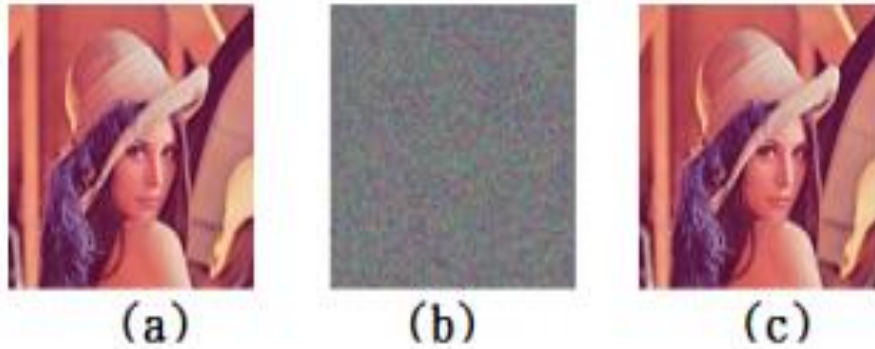


Figure 5.3.1: Encrypted and decrypted secret image

the decrypted photograph based totally on the AES set of regulations is shown. The response time of the cryptographic normal performance in terms of encryption and decryption is highlighted in Table 1.

Table 1: Cryptographic Performance

Size (KB)	Response Time (s)	
	Encryption	Decryption
256	0.4375	0.5227

The previous test showed that the fee of the cryptographic standard overall performance relies upon at the reaction time of the encryption and decryption approaches. In addition, the consequences screen that the decrypted photograph is much like the name of the sport photo, and consequently, the AES algorithm plays efficaciously. This set of guidelines moreover exhibits well maneuverability for picture encryption based totally completely on this locating.

5.4 Robustness Test of the Proposed Method

The stego and extracted snap shots are proven in Figures eight(a) and 8(b), respectively. The NC of the extracted picture is zero.9968.



Figure 5.4.1: StegoAnd Extracted Images

The reliability take a look at for the proposed method is illustrated in Figure 6. The extracted mystery image is proven in Figure nine(b) if the fruit photograph shown in Figure nine(a) is used for detection.



Figure 5.4.2: Reliability Test

Gaussian noise $m = \text{zero}$, $v = 0.001$; speckle; compression QF 60%; rotation with the aid of 10 Performance and higher stability than natural SVD whilst going via diverse malicious attacks. Efficiency in phrases of computation time for embedding and extraction (in seconds) is obtainable.

Table 2: Embedding and Extraction Time

Size	Embedding Time (s)	Extraction Time (s)
256 KB	1.123821	1.456813

Chapter 6

Conclusion

6.1 Conclusion

The security of records stored in the cloud is a big problem. Cryptography strategies were applied in cloud computing to assure the confidentiality of private records. However, attackers have numerous chances to interrupt through the safety provided by using cryptography strategies. In this artwork, a information safety device that mixes cryptography and steganography strategies is supplied to benefit multi-layer protection. Firstly, the AES encryption method is used to encrypt the name of the game picture. Secondly, the hybrid steganography scheme SVD-DWT is done to cover the encrypted thriller picture inside the cowl picture to make sure the confidentiality of the statistics. Thirdly, a hash algorithm is used for the hidden report earlier than and after it is downloaded from the cloud to confirm records integrity. As proven inside the simulation effects, the proposed machine offers extremely good photograph in phrases of PSNR. In addition, the gadget reduces suspicion over the presence of hidden statistics in an photo.

6.2 Future Scope

Cloud Computing but suffers from numerous safety problems as facts proprietors store their data on outside servers, there have been growing name for and worries for information confidentiality, authentication and access manipulate. Cloud protection is becoming a key differentiator and competitive element among cloud providers. In spite of severa blessings which can be furnished by means of way of the cloud computing offerings, cloud computing provider customers are very lots afraid approximately the security in their facts as soon as it is over the cloud beneath the manipulate of one/three party carriers. With the boom inside the increase of cloud computing, safety wants to be analyzed regularly. The Users need to be aware of the risks and vulnerabilities present in the modern-day cloud computing environment earlier than being a part of the surroundings.

References

- [1] A. Bhandari, A. Gupta, and Debasis Das, "Secure algorithm for cloud computing and its applications," in 6th International Conference Cloud System and Big Data Engineering (Confluence'16), IEEE, 2016.
- [2] S. CherillathSukumaran, M. Mohammed, "DNA cryptography for secure data storage in cloud," *International Journal of Network Security*, vol. 20, no. 3, pp. 447-454, 2018.
- [3] E. F. Coutinho, F. R. de C. Sousa, P. A. L. Rego, D. G. Gomes, J. N. de Souza, "Elasticity in cloud computing: A survey," *Annals of Telecommunications*, vol. 70, no. 7-8, pp. 289-309, 2015.
- [4] S. A. El-Booz, G. Attiya, and N. El-Fishawy, "A secure cloud storage system combining time-based one-time password and automatic blocker protocol," *EURASIP Journal on Information Security*, 2016.
- [5] K. El-Makkaoui, A. Ezzati, and A. Beni-Hssane, "Cloud-RSA: An enhanced homomorphic encryption scheme," in *Europe and MENA Cooperation Advances in Information and Communication Technologies*, pp. 471-480, Springer, 2017.
- [6] S. E. Elgazzar, A. A. Saleh, H. M. El-Bakry, "Overview of using private cloud model with GIS," *International Journal of Electronics and Information Engineering*, vol. 7, no. 2, pp. 68-78, Dec. 2017.
- [7] B. L. Gunjal, S. Mali, "MEO based secured, robust, high capacity and perceptual quality image watermarking in DWT-SVD domain," *SpringerPlus*, vol. 4, no. 1, Dec. 2015.
- [8] L. C. Huang, L. Y. Tseng, M. S. Hwang, "A reversible data hiding method by histogram shifting in high quality medical images", *Journal of Systems and Software*, vol. 86, no. 3, pp. 716–727, Mar. 2013.
- [9] S. F. Lu, H. Ali, and O. Farooq, "Proposed approach of digital signature technology for building a web security system based on SHA-2, MRC6 and ECDSA," in 2nd International Conference on Information Technology and Industrial Automation (ICITIA'17), pp. 254-261, 2017.

Management (CAMAN), 2011

Publication

9	Submitted to TAFE NSW Higher Education Student Paper	1%
10	Submitted to KDU College Sdn Bhd Student Paper	1%
11	Submitted to Arab Open University Student Paper	1%
12	Submitted to Higher Education Commission Pakistan Student Paper	<1%
13	Submitted to University of Wolverhampton Student Paper	<1%
14	link.springer.com Internet Source	<1%
15	www.facultateonline.ro Internet Source	<1%
16	iiespace.iie.ac.za Internet Source	<1%
17	Lecture Notes in Computer Science, 2004. Publication	<1%

Exclude quotes

Off

Exclude matches

Off

Management (CAMAN), 2011

Publication

9	Submitted to TAFE NSW Higher Education Student Paper	1%
10	Submitted to KDU College Sdn Bhd Student Paper	1%
11	Submitted to Arab Open University Student Paper	1%
12	Submitted to Higher Education Commission Pakistan Student Paper	<1%
13	Submitted to University of Wolverhampton Student Paper	<1%
14	link.springer.com Internet Source	<1%
15	www.facultateonline.ro Internet Source	<1%
16	iiespace.iie.ac.za Internet Source	<1%
17	Lecture Notes in Computer Science, 2004. Publication	<1%

Exclude quotes

Off

Exclude matches

Off