GALGOTIAS UNIVERSITY

(Established under Galgotias University Uttar Pradesh Act No. 14 of 2011)

SECURE FILE STORAGE ON CLOUD USING CRYPTOGRAPHY

A Report for the Evaluation 3 of Project 2

Submitted by

ANSHIKA KUMAR

(1613105016)

in partial fulfilment for the award of the degree

of

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING WITH SPECIALIZATION OF CLOUD COMPUTING AND VIRTUALIZATION

SCHOOL OF COMPUTING SCIENCE AND ENGINEERING

Under the Supervision of
Mr Ajay Kumar, Assistant Professor

APRIL / MAY- 2020

SCHOOL OF COMPUTING AND SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

Certified that this project report "SECURE FILE STORAGE ON CLOUD USING CRYPTOGRAPHY" is the bonafide work of "ANSHIKA KUMAR (1613105016)"who carried out the project works under my supervision

SIGNATURE OF HEAD
Dr. MUNISH SHABARWAL,
PhD (Management), PhD (CS)
PROFESSOR& DEAN,
School of Computing Science & Engineering

SIGNATURE OF SUPERVISOR
Mr Ajay Kumar, Assistant Professor
PROFESSOR& SUPERVISOR
School of Computing Science & Engineering

ACKNOWLEDGEMENT:

This is an excellent opportunity to acknowledge and to thanks, all those persons without whose support and help this project would be impossible. We might prefer to add some heartfelt words for those who were a part of this project in numerous ways.

I would prefer to because of my project guide Ajay Kumar, for his indefatigable guidance, valuable suggestion, moral support, constant encouragement, and contribution of your time for the successful completion of project work. I'm very grateful to him, for providing all the facilities needed during the project development. At the outset, I sincerely thank all faculty members of my institution GALGOTIAS UNIVERSITY for his extra effort to create our session online and inspire all ideas.

I would prefer to thank all those that helped me directly or indirectly. Last but not the smallest amount, I'd prefer to acknowledge the continuing support of my friends, whose patience and encouragement during these long days and nights are paramount in making this project a reality.

THANK YOU.

DECLARATION:

I hereby declare that this submission is my very own work which, to the simplest of my knowledge and belief, it contains no material previously published or written by another person nor material which to a considerable extent has been accepted for the award of the other degree or diploma of the university or other institute of upper learning, except where due acknowledgment has been made within the text.

I inform that every data used in this report if it's taken from any site is clearly referenced under the reference section.

SIGNATURE

Anshika Kumar

16SCSE105125

Date: 03-may-2020

ABSTRACT:

We intend to safely store data into the cloud, by parting information into a few lumps and putting away pieces of it on cloud in a way that jelly information secrecy, trustworthiness and guarantees accessibility. The quickly expanded utilization of distributed computing in the numerous association and IT ventures gives new programming minimal effort. Distributed computing is valuable as far as ease and openness of information. Distributed computing gives part of advantages with minimal effort and of information availability through Internet. Guaranteeing the security of distributed computing is a main consideration in the distributed computing condition, as clients regularly store delicate data with distributed storage suppliers, however these suppliers might be untrusted. So sharing information in secure way while protecting information from an untrusted cloud is as yet a difficult issue. Our methodology guarantees the security and protection of customer touchy data by putting away information across single cloud, utilizing AES, DES and RC2 calculation. Cloud computing, client can remotely store and recover their information dependent on request administration, without the weight of neighbourhood information stockpiling and upkeep. In any case, the assurance of the secret information prepared and created during the calculation is turning into the significant security concern. The principle goal of distributed computing empowers clients with restricted computational assets to redistribute their huge calculation remaining tasks at hand to the cloud, and financially appreciate the huge computational force, data transfer capacity, stockpiling, and even fitting programming that can be partaken in a compensation for each utilization way.

TABLE OF CONTENTS:

LIST OF TABLES:

TABLE TITLE **TABLE NO.**

LISTS OF FIGURES:

FIGURE TITLE **FIGURE NO.**

CHAPTER 1
INTRODUCTION

Cloud computing is begun from before huge scope disseminated figuring innovation. NIST defines Cloud Computing asa model for empowering helpful, on request organize access to a common pool of configurable processing assets (e.g., networks, capacity, applications and administrations) that can be quickly provisioned and discharged with negligible administration exertion or specialist organization collaboration". In Cloud computing, the two documents and programming are not completely contained on the client's computer. File security concerns emerge on the grounds that both client's application and program are living in supplier premises. The cloud supplier can take care of this issue by scrambling the documents by utilizing encryption calculation.

Mechanical headways are coming about in trends and developments that improve the personal satisfaction. In this quick life where each individual uses a cell phone and approaches the web, the significant worry that the individuals face is with respect to the security of their data present on the web. This security concern is additionally about the record that is put away online on a cloud. This can be fathomed with the assistance of cryptography.

Cryptography methods convert unique information into Cipher content. So just real clients with the correct key can get to information from the distributed storage server. The fundamental point of cryptography is to keep the security of the information from programmers, on the web/programming crackers, and any outsider clients. Non-genuine client access to data brings about loss of privacy. Security has the qualities to square or stop this sort of unapproved get to or some other sort of malevolent assaults on the information here by making sure about the clients'

trust. In the Cloud computing condition, security is considered to be an essential viewpoint because of the criticalness of data put away on the cloud and the various administrations gave to the clients. This information can be private and very delicate. Subsequently, the information the board and security ought to be totally dependable. It is essential that the information in the cloud is shielded from vindictive assaults.

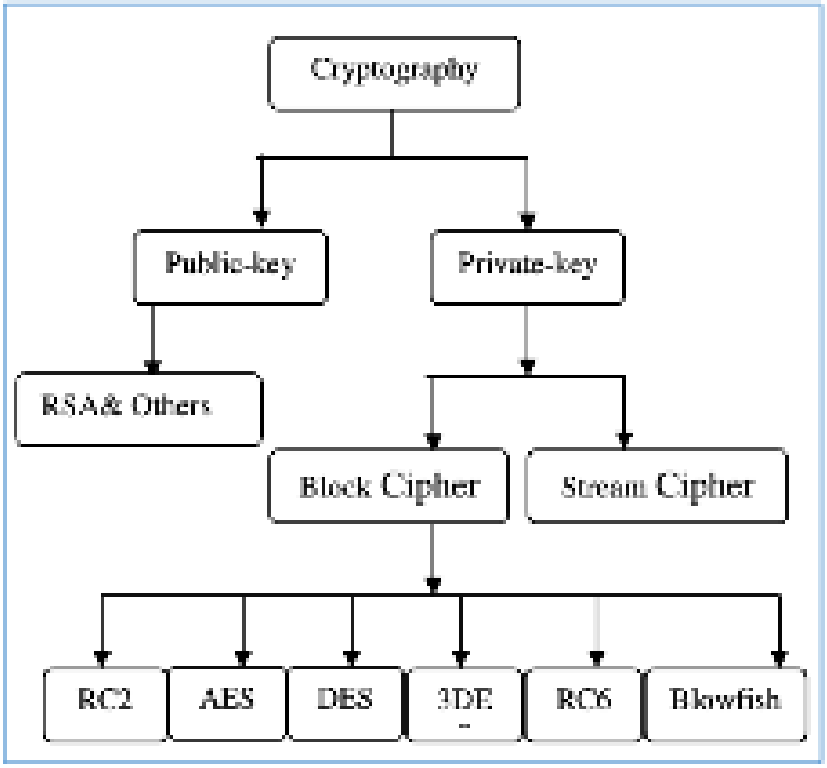

Fig. 1. Cryptographic Technique

1.1 Overall Description

Cryptography is the shielding procedure of information from the unapproved party by changing over into the non-discernible structure. The primary reason for cryptography is keeping up the

security of the information from outsider. There are following two sorts of calculations, for example, (i) symmetric key based calculation, now and again known as ordinary key calculation and (ii) unbalanced key based calculation, otherwise called open key calculation. Symmetric calculation can be additionally separated into two kinds. Data Security Issues Due to responsiveness and multi-tenant characteristics of the cloud, the standard security frameworks are never again fitting for applications and data in cloud. A segment of the issues are as following:

- Due to dynamic adaptability, organization and region straightforwardness features of dispersed processing model, a wide scope of utilization and data of the cloud stage have no settled system and security limits. If there should be an occurrence of security break, it is difficult to isolate a particular resource that has a hazard or has been exchanged off.
- According to profit movement models of Cloud preparing, resources and cloud organizations may be controlled by various providers. As there is a hostile circumstance, it is difficult to pass on a united wellbeing exertion.
- Due to the openness of cloud and sharing virtualized resources by multitenant, customer data may be gotten to by other unapproved customers.

1.2 Purpose

In the distributed computing condition, security is regarded to be a pivotal viewpoint because of the criticalness of data put away in the cloud. The information can be classified and amazingly touchy. Subsequently, the information the executives ought to be totally solid. It is vital that the data in the cloud is shielded from pernicious assaults. Security gets worries for classification, trustworthiness and accessibility of information. Unapproved access to data brings about loss of

information secrecy. Information uprightness and accessibility endures because of disappointment of cloud administrations. Security has the qualities of a supplement to reliability. The utility of this cloud and its administrations are not confined to an area or any premises. All the clients, for example, head, educators and understudies are permitted to utilize this information whenever needed. This task has cloud that is open to every one of the, a database to store school related information and all data, site for clients to login to the cloud.

1.3 Motivation and Scope

The cloud can be gotten to through web from anyplace. The clients need to login to the cloud and give subtleties to get to the information from database. The cloud will likewise give security to all the information put away at our server.

1.4 Hybrid Cryptosystem Phases

The hybrid cryptosystem used to maintain security of the files has two phases:

- Encryption phase
- Decryption phase

1.4.1 Encryption Phase

At the encryption end, On the particular of client, the record being encoded will be cut into n cuts. Every one of the record cuts is scrambled utilizing Blowfish key gave by the client to each cut. The key will be encoded utilizing SRNN open key After encryption, we have scrambled documents cuts and the comparing scrambled keys. Encryption is the best method to accomplish information security. To peruse an encrypted document, you should approach a mystery key or

secret word that empowers you to decode it. Unencrypted data is called plain text and encrypted data is referred to as cipher text. The files are sliced at encryption phase and merged at decryption phase.

1.4.2 Decryption Phase

At the deciphering end, The customer will give n SRNN private keys,

- as demonstrated by the amount of cuts (n) made in the midst of the encryption stage. Blow fish key is decoded at the server end using the SRNN private key specific to the cut. Using the relating unscrambled Blow fish keys,
- record removes put at server are decoded . The unscrambled slices will be combined to create special record.

CHAPTER 2
LITERATURE SURVEY

The Authors has purposed buyers, store their own documents or information on cloud server and customers utilize that information or records at whatever point required. Numerous buyers store or spot their own information on the cloud, so security and protection are significant issue in cloud. These two issues can prompt various security concerns identified with information transmission, honesty control, get to control, character the executives, logging and evaluating, and so on. However, inquire about in the zone of distributed computing accepting incredible consideration from industry, the scholarly community and government. This proposition is worried to defeat the security exchange off and improve the presentation of information transmission and expands the security through Third Party Auditor and Identity Based Encryption. Furnish security in the cloud with the assistance of the Third Party Auditor. This is done to improve the hardness in security by the IBE encryption calculations by including some greater security codes. Encryption is the crucial piece of data sharing .In the Authors has purposed Certain Cloud Service Providers (CSPs) may work unscrupulously with the cloud clients' information, they may sneak the information from cloud and offer it to outsiders so as to procure benefit Thus despite the fact that re-appropriating information on cloud is economical and decreases long span stockpiling and upkeep multifaceted nature, there is least affirmation of information trustworthiness, protection, security and accessibility on cloud servers. Spotlights on the uprightness confirmation technique for redistributed information. The proposed plot consolidates the encoding component alongside honesty check methodology. Distributed storage issues are fathomed utilizing cryptography and steganography procedures. Square savvy Data

security is accomplished utilizing AES, RC6, Blowfish and BRA calculations. Key data security is practiced utilizing LSB procedure. Information respectability is cultivated utilizing SHA1 hash calculation. Low defer parameter is accomplished utilizing multithreading strategy. With the assistance of proposed security system information respectability, high security, low deferral, validation and secrecy parameters are accomplished. The proposed configuration permits clients to review the information with lightweight correspondence and calculation cost. Examination shows that proposed framework is profoundly productive against noxious information alteration assault and server conspiring assault. Execution and broad security examination shows that proposed frameworks are provably secure and profoundly productive. Introduced an encryption conspire which is initially proposed for briefly transmitting huge number of keys in communicate situation. Also, utilizes Symmetric-key encryption with Compact Key. In this paper manufacture an effective framework that permits patients both to share fractional access rights with others, and to perform look over their records. They formalize the necessities of a Patient Controlled Encryption plan, and give a few cases, based one existing cryptographic natives and conventions, each accomplishing an alternate arrangement of properties.

CHAPTER 3
PROBLEM STATEMENT

Client's stores information at cloud specialist co-ops is defenceless against different dangers. In our work, we consider four kinds of risk models. First is the single purpose of disappointment, which will influence the information accessibility that could happen if a server at the cloud specialist co-op fizzled or smashed, which makes it harder for the client to recover his put away information from the server. Accessibility of information is likewise a significant issue which could be influenced, if the cloud specialist organization (CSP) comes up short on administration.

Our subsequent danger is information uprightness. Trustworthiness is a degree certainty that the information in the cloud is what should be there, and is secured against unplanned or purposeful modification without approval. Such concerns are not any more advantageous issues; in this way, a cloud administration client cannot so much depend upon a cloud specialist organization to guarantee the capacity of his fundamental data. Security is an important assistance for wired system just as remote system correspondence to improve what was offered in cloud .Simply putting away the data on mists takes care of the issue isn't about information accessibility, yet about security. The solid purpose of this technique is that the mystery key must be consolidated by reconstructing. Most of the organizations that have kept away from receiving the cloud have done as such in the dread of having their information spilled.

This accomplishment originates from the way that the cloud is a multi-client condition, wherein all the assets are shared. It is moreover an outsider help, which implies that information is

conceivably in danger of being seen or misused by the supplier. It is as it were human instinct to question the capacities of an outsider, which appears to be a considerably greater hazard with regards to organizations and touchy business information. There are additionally a number of outside dangers that can prompt information spillage, counting malevolent hacks of cloud suppliers or bargains of cloud client accounts. The best technique is to rely upon document encryption and more grounded passwords, of the cloud specialist organization themselves.

CHAPTER 4
PROPOSED MODEL

4.1 Symmetric Key Cryptography

Symmetric-key cryptography alludes to encryption strategies in which both the sender and recipient share a similar key (or, less regularly, in which their keys are unique, yet related in an effectively calculable way). This was the main sort of encryption freely known until June 1976. Symmetric key figures are actualized as either block figures or stream figures. A square figure enciphers contribution to squares of plaintext rather than singular characters, the input structure utilized by a stream figure. The Data Encryption Standard (DES) and the

Advanced Encryption Standard(AES) are square figure plans that have been assigned cryptography gauges by the US government (however DES's assignment was at last pulled back after the AES was adopted).

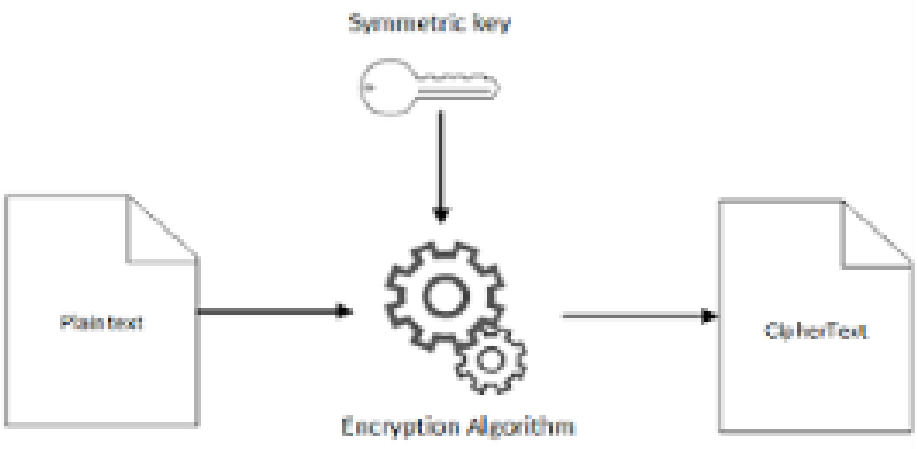

Fig.2. Symmetric Key Cryptography

4.2 Asymmetric Key Cryptography

Public-key calculations are frequently founded on the computational unpredictability of "difficult" issues, regularly from number hypothesis. For instance, the hardness of RSA is identified with the whole number factorization issue, while Diffie–Hellman and DSA are identified with the discrete logarithm issue. All the more as of late, elliptic bend cryptography has created, a framework wherein security is in light of number theoretic issues including elliptic bends. In light of the trouble of the fundamental issues, most open key calculations include tasks, for example, particular increase and exponentiation, which are

substantially more computationally costly than the methods utilized in most square figures, particularly with regular key sizes.

4.3 Data Encryption Standard

DES is the model square figure—a calculation that takes a fixed-length string of plaintext bits and changes it through a progression of entangled tasks into another cipher text bit string of a similar length. On account of DES, the square size is 64 bits. DES additionally utilizes a key to redo the change, with the goal that unscrambling can as far as anyone knows just be performed by the individuals who realize the specific key used to scramble. The key apparently comprises of 64 bits; in any case, just 56 of these are really utilized by the calculation. Eight bits are utilized exclusively for checking equality, and are from that point disposed of. Subsequently the compelling key length is 56 bits. The key is ostensibly put away or transmitted as 8 bytes, each with odd parity. Before the primary adjusts, the square is isolated into two 32-piece parts and prepared on the other hand; this jumbling is known as the Feistal plot. The Feistal structure guarantees that decoding and encryption are fundamentally the same as procedures the main contrast is that sub keys are applied in the converse request when decrypting.

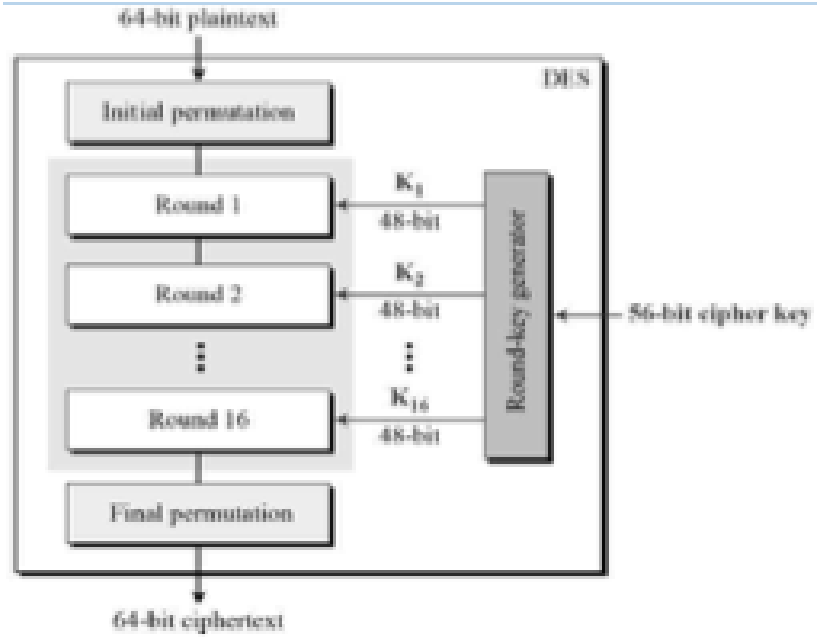

Fig.3. DES Algorithm

4.4 Advanced Encryption Standard

AES is a subset of the Rijndael figure created by Belgian cryptographers, Vincent Rijmen and Joan Daemen, who presented a proposition to NIST during the AES determination process. Rijndael is a group of figures with various key and square sizes. For AES, NIST chose three individuals from the Rijndael family, each with a square size of 128 bits, however three diverse key lengths: 128, 192 and 256 bits.

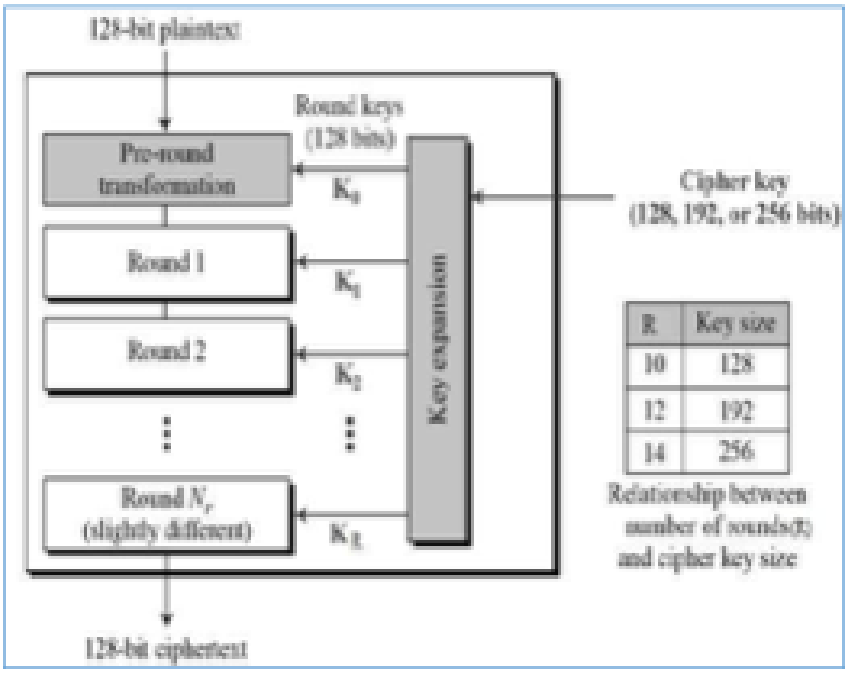

Fig. 4. AES Algorithm

4.4.1 **Byte Substitution (Sub Bytes)**

The 16 info bytes are subbed by looking into a hard and fast table (S-box) given in structure. the result is in an exceedingly lattice of 4 lines and 4 segments.

4.4.2 Shift Rows

Every one of the four columns of the grid is moved to at least one side. Any passages that 'tumble off' are re-embedded on the proper side of column. Move is finished as follows –

- First column isn't moved.
- Second line is moved one (byte) position to at least one side.
- Third line is moved two situations to at least one side.
- Fourth column is moved three situations to at least one side.

- The result is another framework comprising of the same 16 bytes yet moved as for each other.

4.4.3 Mix Columns

Every section of 4 bytes is currently changed utilizing a rare scientific capacity. This capacity takes as info the four bytes of 1 section and yields four totally new bytes, which supplant the primary segment. the result is another new grid comprising of 16 new bytes. It should be noticed that this progression isn't acted within the last round.

4.4.4 Add Round Key

The 16 bytes of the lattice are presently considered as 128 bits and are XORed to the 128 bits of the round key. within the event that this is often the last round, at that time the yield is that the cipher text. Something else, the following 128 bits are deciphered as 16 bytes and that we start another comparative round.

4.4.5 Decoding Process

The procedure of decoding of an AES cipher text is just like the encryption procedure within the converse request. Each round comprises of the four procedures led within the converse order:

- Add round key
- Mix sections
- Shift lines
- Byte substitution

4.5 RC-2 Encryption Algorithm

In cryptography, RC2 (otherwise called ARC2) may be a symmetric-key square figure structured by Ron Rivest in 1987. "RC" means "Ron's Code" or "Rivest Cipher"; different figures structured by Rivest incorporate RC4, RC5, and RC6. The advancement of RC2 was supported by Lotus, who were trying to find a custom figure that, after assessment by the NSA, might be traded as a serious aspect of their Lotus Notes programming. The NSA proposed two or three changes, which Rivest consolidated. After further exchanges, the figure was endorsed for transport in 1989.

	ENCRYPTION	DECRYPTION
MEANING	The process of converting plain text into the cipher text to increase data security is known as encryption of data.	The process of converting cipher text into the plain text to retrieve original data is known as encryption of data.
PROCESS	The data is encrypted with the uniquely generated random number while uploading the file.	The data is decrypted with the uniquely generated random number while downloading the file.
PURPOSE	The cipher text is stored in service provider's database.	The plain text is being downloaded at the user's device.

Table 1: Encryption and Decryption algorithm

CHAPTER 5
FUTURE ENHANCEMENT

The primary point of this framework is to safely store and recover information on the cloud that is just constrained by the proprietor of the information. Distributed storage issues of information security are illuminated utilizing cryptography and steganography procedures. Information security is accomplished utilizing RC6, 3DES and AES calculation. Key data is securely put away utilizing LSB method (Steganography). Less time is utilized for the encryption and decoding process utilizing multi stringing procedure. With the assistance of the proposed security mechanism, we have achieved better information trustworthiness, high security, low deferral, authentication, and confidentiality. In the future we can add open key cryptography to stay away from any assaults during the transmission of the information from the customer to the server.

CHAPTER 6
CONCLUSION

The fundamental objective is to safely store and access information in cloud that isn't constrained by the proprietor of the information. We misuse the strategy of elliptic bend cryptography encryption to ensure information documents in the cloud. Two piece of the cloud server improved the presentation during capacity and getting to of information. The ECC Encryption calculation utilized for encryption is another favourable position to improve the presentation during encryption and unscrambling process. We expect that this way of putting away and getting to information is a lot of make sure about and have superior. Our endeavours are proceeding to take care of the issue of gathering sharing of information in the mutual information segment as right now individual from gathering can get to the information put away over shared information area. One to many, numerous to one, numerous to numerous correspondence is absurd.

CHAPTER 7
REFERENCES

[1]VijayaPinjarkar, Neeraj Raja, KrunalJha,AnkeetDalvi, “Single Cloud Security Enhancement using key Sharing Algorithm, ”Recent and Innovation Trends in Computing and Communication, 2016.

[2] V. Vankireddy, N. Sudheer, R. Lakshmi Tulasi, “Enhancing Security and Privacy in Multi Cloud Computing Environment, ”International Journal of Computer Science and Information Technologies, 2015.

[3] Swapnila S Mirajkar, Santoshkumar Biradar, “Enhance Security in Cloud Computing, ”International Journal of Advanced Research in Computer Science and Software Engineering,2014.

[4] Ashalatha R, “A survey on security as a challenge in cloud computing,”International Journal of Advanced Technology & Engineering Research (IJATER) National Conference on Emerging Trends in Technology,2012.

[5]www.google.com