SECURE FILE STORAGE AND SHARING ON CLOUD USING AES ALGORITHM

Mr. Jadhav Swapnil A , Mr. Abhang Amol S, Mr. Patil Rahul A

[1] student, computer engineering, pune vidyarthi griha's coe, maharashtra, india
[2] student, computer engineering, pune vidyarthi griha's coe, maharashtra, india
[3] student, computer engineering, pune vidyarthi griha's coe, maharashtra, india
[4]professor, computer engineering, pune vidyarthi griha's coe, maharashtra, india

ABSTRACT

Secure file storage and sharing on cloud using aes algorithm along implementation is presented this report.The auto generated token based certification activation approach with SSL (Secure Socket layer) provides the appropriate collaboration between the cloud client and the cloud services provider, then using n layer the all token in crypto-graphy format so that user may become confident during data transfer by utilizing various cloud application and services. The chances of attacks may be reduced by implementing this AES with N layer approach. this designed algorithm takes less time to execute and increases the performance of the system.

Keyword:- *Cloud Computing, Cloud Security, AES, DES ,Encryption, Decryption.*

1. INTRODUCTION

Cloud computing, is nothing on-the-line computing, Its a kind of Internet-based computing which provides shared processing resources and data to computers and other devices on demand. It is special model for enabling on-demand access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services), which can be fastly provisioned and released with minimal management effort. Its storage solutions provide users and enterprises with various capabilities to store and process their data in third-party data centers. It depends on sharing of resources to achieve coherence and economy of scale, similar to a utility (like the electricity grid) over a network.

Now days availability of high-capacity networks and , storage devices , low-cost computers as well as the widespread adoption of hardware virtualization, and autonomic and utility computing have led to a growth in cloud computing. Companies can scale up as computing needs increase and then scale down again as demands decrease.

1.1 Cloud Computing

CLOUD stands for common location independent only utility o demand. It is an umbrella term used for internet based development and services. The Functioning these services depends on deployment and delivery models that help to dynamically deliver a variety of things as a services over the internet based on demand of the consumer as example network, storage, hardware as well as software. Currently crimes on internet are increasing ways to steal information. Therefore, the security becomes a mandatory issue.

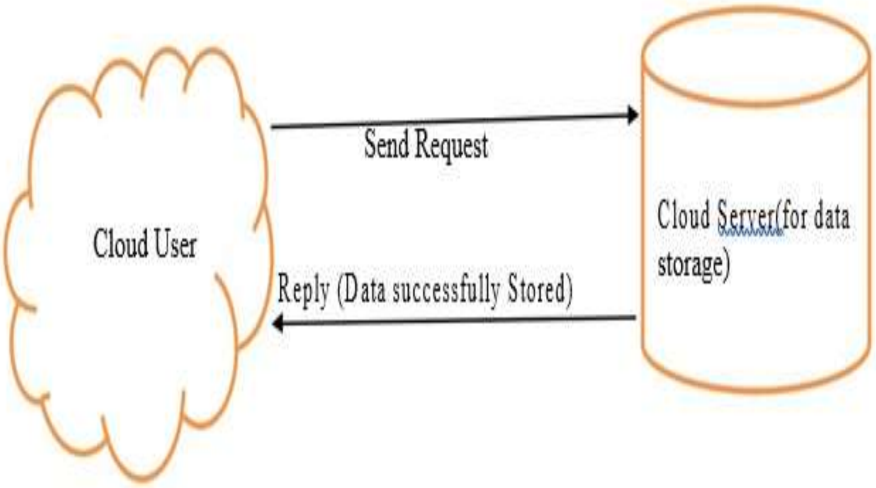
Cloud User
Send Request
Reply (Data successfully Stored)
Cloud Server(for data storage)

Figure 1.1: Cloud Computing

1.2 Aim

Main focus of this project saved and secure data over cloud using N-layer Architecture

1.3 Objective

While making a cloud secure, the following objectives are to be met:

1. Find out possible solution.
2. Create application
3. Apply Encryption.
4. Testing.
5. Execute that application

1.4 Necessity

Now a Days cloud is very essential for data storage and for this we have to secure our data. So, find out the well possible solution for this. in my project I found no of solution as I discuss in Analysis Of Possible Solution.

The reason for this work is to overview the late research on security calculations for mists to address the security dangers and arrangements. We have found that much research has been done to guarantee the security of data. We save the data on cloud using token and that token are we are encrypted using N-Layer Architecture.in this encryption algorithm we use AES, RSA, DES, Caser Cipher etc.

2. SYSTEM ANALYSIS

The act, process, or profession of studying an activity as a procedure, a business, function typically by mathematical means in order to define its goals or purposes and to discover operations and procedures for accomplishing them most efficiently.

2.1 Existing Work

There are a various security issues concerns associated with cloud computing but these issues depict into two broad categories: security issues faced by cloud providers organizations providing software- platform-, or infrastructure-as-a-service via the cloud) and security issues faced by their customers (companies or organizations who host applications or store data on the cloud).There are several types of attacks performed by the attackers on cloud and the most popular attacks are listed below:

1. Social Engineering
2. Malware Injection
3. XML
4. Signature Wrapping
5. Account Hijacking
6. Traffic Flooding
7. Wireless LAN attack pose Is a greater risk to cloud computing system

For preventing confidential data from the attackers, the cloud service providers have duty top provide security at separate levels.as an examples how to provides security on data and files in individual manner that sometimes becomes more difficult. Therefore, they suggest cloud to their customers who are cloud clients to use secure cloud services. The benefit to use such type of secure cloud services is to give secure treatments and calculations for data storage in the database. generally, whenever any cloud client send request to cloud service providers for accessing specific cloud service.

For analyzing cloud data security in depth, there us a need it study various different parameters related to data security like data security risk, data security requirements, deployment if security functions and some processes through digital signature etc. Besides there are number of positive and negative impacts of data security as given by cloud services provides where the positive impact is to provide the security if data on the server which is also a type of critical risk. Therefore, risk management and risk assessment becomes crucial factor for any cloud service provider to handle. They also concentrate to provides security at exact location of data, access of data. SLA (Service level Agreement), Authentication and authorization. The Network and system administration helps, to implement various security policies in different cloud application.

2.2. Similar Cloud security Algorithm

In computer Networking, cloud computing is a word is describing different computing concept which contain huge number of computers attached through a real-time communication like internet.Lots of solution are available. I describe some of them. Cloud computing is growing fast with time. Cloud computing illustrate Information Technology as a fundamentally diverse operating model that take advantages.

2.2.1. Tiny Encryption Algorithm

In cryptography, the Tiny Encryption Algorithm (TEA) is a block cipher notable for its simplicity of description and implementation, typically a few lines of code. It was designed by David Wheeler and Roger Needham of the Cambridge Computer Laboratory; it was first presented at the Fast Software Encryption workshop in Leuven in 1994, and first published in the proceedings of that workshop.

TEA operates on two 32-bit unsigned integers (could be derived from a 64-bit data block) and uses a 128-bit key. It has a Feistily structure with a suggested 64 rounds, typically implemented in pairs termed cycles. It has an extremely simple key schedule, mixing all of the key material in exactly the same way for each cycle. Different multiples of a magic constant are used to prevent simple attacks based on the symmetry of the rounds. The magic constant,2654435769 or 9E3779B916 is chosen to be 232/, where is the golden ratio.

TEA has a few weaknesses. Most notably, it suffers from equivalent key search key is equivalent to three others, which means that the effective key size is only 126 bits. As a result, TEA is especially bad as cryptographic. This weakness led to a method for hacking Microsoft's Xbox game console, where the cipher was used as a hash function. TEA is also susceptible to a related-key attack which re- quires 223chosen plaintexts under a related-key pair, with 232 time complexity. Because of these weaknesses, the XTEA cipher was de- signed.

2.2.2 Triple DES

The speed of exhaustive key searches against DES after 1990 began to cause discomfort amongst users of DES. However, users did not want to replace DES as it takes an enormous amount of time and money to change encryption algorithms that are widely adopted and embedded in large security architectures.

The pragmatic approach was not to abandon the DES completely, but to change the manner in which DES is used. This led to the modified schemes of Triple DES (sometimes known as 3DES).

Incidentally, there are two variants of Triple DES known as 3-keyTriple DES (3TDES) and 2-key Triple DES (2TDES).

The encryption-decryption process is as follows :-

- Encrypt the plaintext blocks using single DES with key K1.
- Now decrypt the output of step 1 using single DES with key K2.
- Finally, encrypt the output of step 2 using single DES with key K3.
- The output of step 3 is the cipher text.
- Decryption of a cipher text is a reverse process. User first de- crypt using K3, then encrypt with K2,
- And finally decrypt with K1.

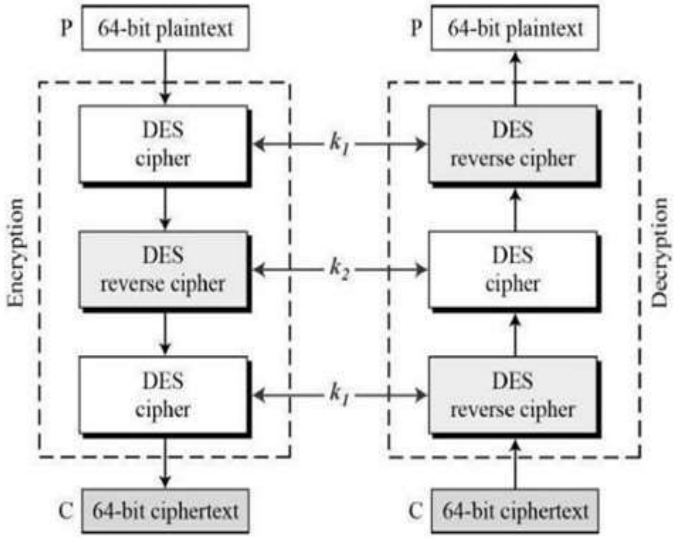

Figure 2.1: Triple DES

Due to this design of Triple DES as an encrypt decrypt encrypt process, it is possible to use a 3TDES (hardware) implementation for single DES by setting K1, K2, and K3 to be the same value. This provides backwards compatibility with DES.

Second variant of Triple DES (2TDES) is identical to 3TDES except that K3is replaced by K1. In other words, user encrypt plaintext blocks with key K1, then decrypt with key K2, and finally encrypt with K1 again. Therefore, 2TDES has a key length of 112 bits. Triple DES systems are significantly more secure than single DES, but these are clearly a much slower process than encryption using single DES.

2.3 Proposed System

As cloud computing services rapidly expand their customer base, it has become import to share cloud resources, so as to provide them economically. In cloud computing services, multiple types of re- sources. such as processing ability, bandwidth and storage, need to allocated simultaneously. We can save the data and this designed algorithm takes less time to execute and increases the performance of the system.

2.3.1 Working of Project

Main objective is to develop proposed system which is platform in- dependent and offer high level data security best of ever provided. Multiple Encryption algorithms will be used in the system with the intention encryption in a single level. Random function generator will be used to generate n digit random number depending upon n number of encryption algorithms to be used. This generated random number will decide the order of encryption algorithms to used.

As the order of algorithms to be used will be random so its to- tally no feasible to predict/crack the order of algorithms applied for encryption.

For Random number generator we will be using scheme to generate random number depending on pass phrase we provide. In this way Random number generator will provide different random number for different pass phrases.

Also the number of encryption algorithms we will use and their order will be kept secret and hence it is very much difficult for at- tacker/intruder to break the system. We use Algorithms like AES, RSA, DES, Caser Cipher etc.

Order of algorithms for decryption process will be in reverse manner, i.e. algorithm n, algorithm n-1 ...algorithm 1.

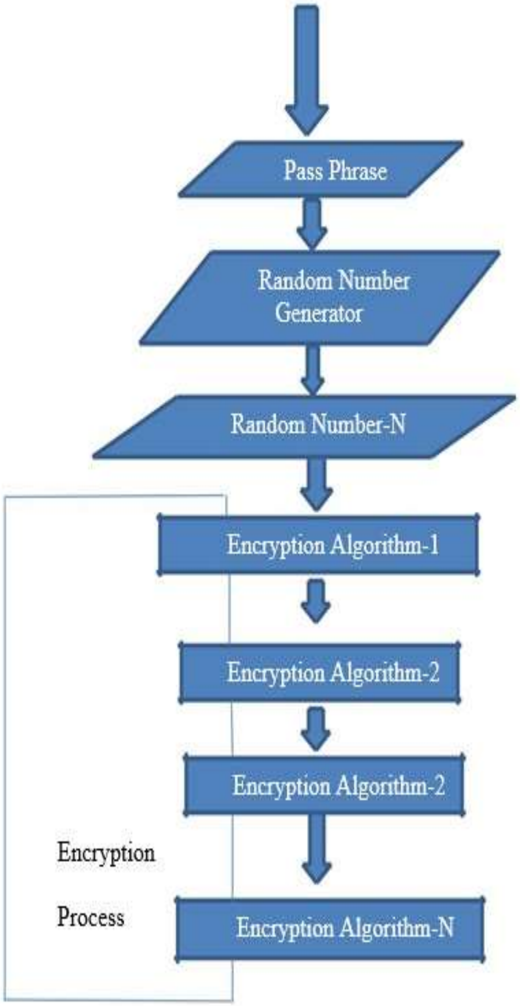

Figure 2.2: Encryption Process

2.3.2 N-Layer Architecture

The calculation depends on a few substitutions, stages and direct changes, each executed on information squares of 32 bytes accordingly the term block cipher. Those operations are rehashed a few times, called ”rounds. The combination AES, RAS and DES show the powerful encryption technique.

2.3.3 Random Number Generator

An Random number generator (RNG) is a computational or physical gadget intended to create a grouping of numbers or images that can’t be sensibly anticipated superior to by an irregular possibility.

Different utilizations of arbitrariness have prompted the improvement of a few unique strategies for creating random information, of which some have existed since antiquated times, among their positions are surely understood ”exemplary” cases, including the moving of shakers, coin flipping, the rearranging of playing cards, the utilization of yarrow stalks (for divination) in the I Ching, and in addition innumerable different systems. Due to the mechanical way of these procedures, creating vast quantities of adequately arbitrary numbers required a great deal of work and/or time. In this way, results would once in a while be gathered and circulated as arbitrary number tables. These days, after the coming of computational irregular number generators, a becoming numb of government-run lotteries and lottery amusements have begun utilizing RNGs rather than more conventional drawing strategies. RNGs are additionally use to decide the chances of present day opening machines.

A few computational strategies for irregular number era exist. Numerous miss the mark regarding the objective of genuine hap- hazardness, in spite of the fact that they may meet, with shifting achievement, a portion of the factual tests for arbitrariness planned to quantify how capricious their outcomes are (that is, to what degree their examples are perceptible). Be that as it may, precisely com- posed cryptographically secure computationally based strategies for producing irregular numbers additionally exist, for example, those in view of the Yarrow calculation, the Fortuna (PRNG), and others.

2.4 Technology used in Project

We are following strong custom Java and SQL for encryption more- over, system is built in Java EE (Enterprise Edition 8.0).

- Java Eclipse Mars
- SQL Database
- Cloud services

2.5 System requirements

- Windows 10 (8u51 and above)
- Windows 7 SP1
- Windows Server 2008 R2 SP1 (64-bit) RAM: 128 MB
- Disk space: 124 MB for JRE; 2 MB for Java Update
- Processor: Minimum Pentium 2 266 MHz processor
- Browsers: Internet Explorer 9 and above, Firefox

2.6 Analysis conclusion

After examination of comparative strategies is conceivable to say that, this algorithm is combination of AES, RAS the Encryption security should be higher. Only the authenticated and authorized user can access the data, user cannot decrypt the data and get back the original data from it. Data security is provided by implementing N- Layer algorithm.

3.SYSTEM DESIGN

System Design outline is the procedure of characterizing the engineering, parts, modules, interfaces, and information for a framework to fulfil determined necessities. Frameworks configuration could be seen as the utilization of frameworks hypothesis to item advancement. There is some cover with the orders of frameworks examination, frameworks design and frameworks building.

3.1 Cloud Storage

Cloud storage is a model of information stockpiling in which the computerized information is put away in sensible pools, the physical stockpiling traverses various servers (and frequently areas), and the physical environment is regularly possessed and oversaw by a facilitating organization. These distributed storage suppliers are in charge of keeping the information accessible and available, and the physical environment ensured and running. Individuals and associations purchase or rent stockpiling limit from the suppliers to store client, association, or application information.

3.1.1 Cloud Storage Architecture

Cloud storage designs are fundamentally about conveyance of capacity on interest in a very versatile and multi-inhabitant way. Blandly, distributed storage designs comprise of a front end that fares an API to get to the capacity. In customary stockpiling frameworks, this API is the SCSI convention; however in the cloud, these conventions are advancing. There, you can discover Web administration front finishes, record based front closures, and much more conventional front closures, (for example, Internet SCSI, or iSCSI). Behind the front end is a layer of middleware that I call the capacity rationale. This layer actualizes an assortment of components, for example, replication and information lessening, over the conventional information position calculations (with thought for geographic arrangement). At last, the back end executes the physical stockpiling for information. This might be an inside convention that executes particular compo- nents or a customary back end to the physical plates.

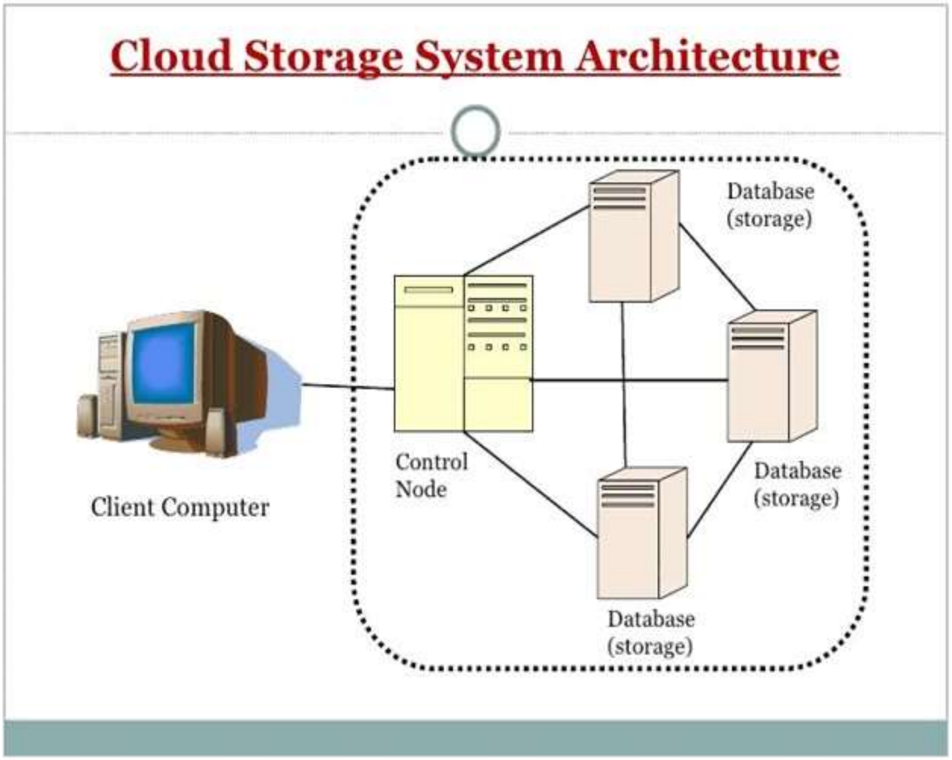

Figure 3.1: cloud storage System Architecture

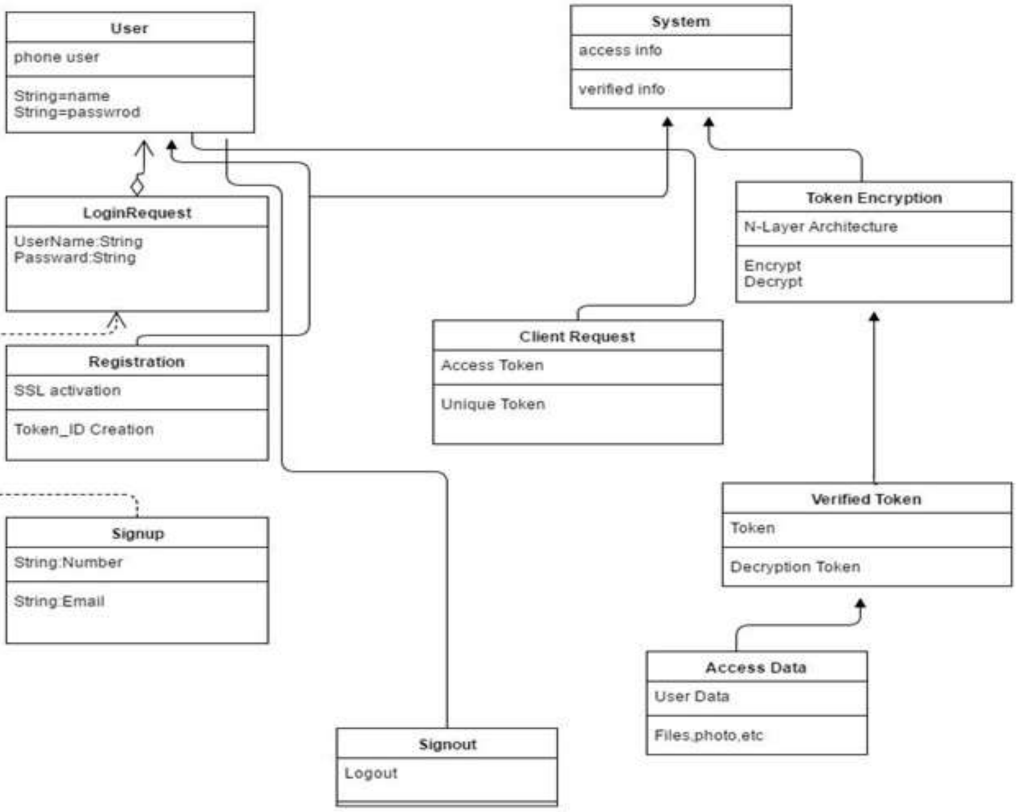

Figure 3.2: Class diagram for working in cloud with token encryption

3.2 UML Diagrams

The Unified Modelling Language (UML) is a broadly useful, formative, displaying dialect in the field of programming building, that is proposed to give a standard approach to envision the configuration of a framework .

3.2.1 Class Diagram

A class Diagram in the Unified Modelling Language (UML) is a kind of static structure graph that depicts the structure of a framework by demonstrating the framework’s classes, their properties, operations (or strategies), and the connections among articles.

3.2.1.1 Diagram Description:

First of all, Signup and Login Request are identified. After the SSL activation user can registered, already exiting user are use signup, new user can get random token by system then this token should be encrypted form then only particular user know that the key for the decryption .

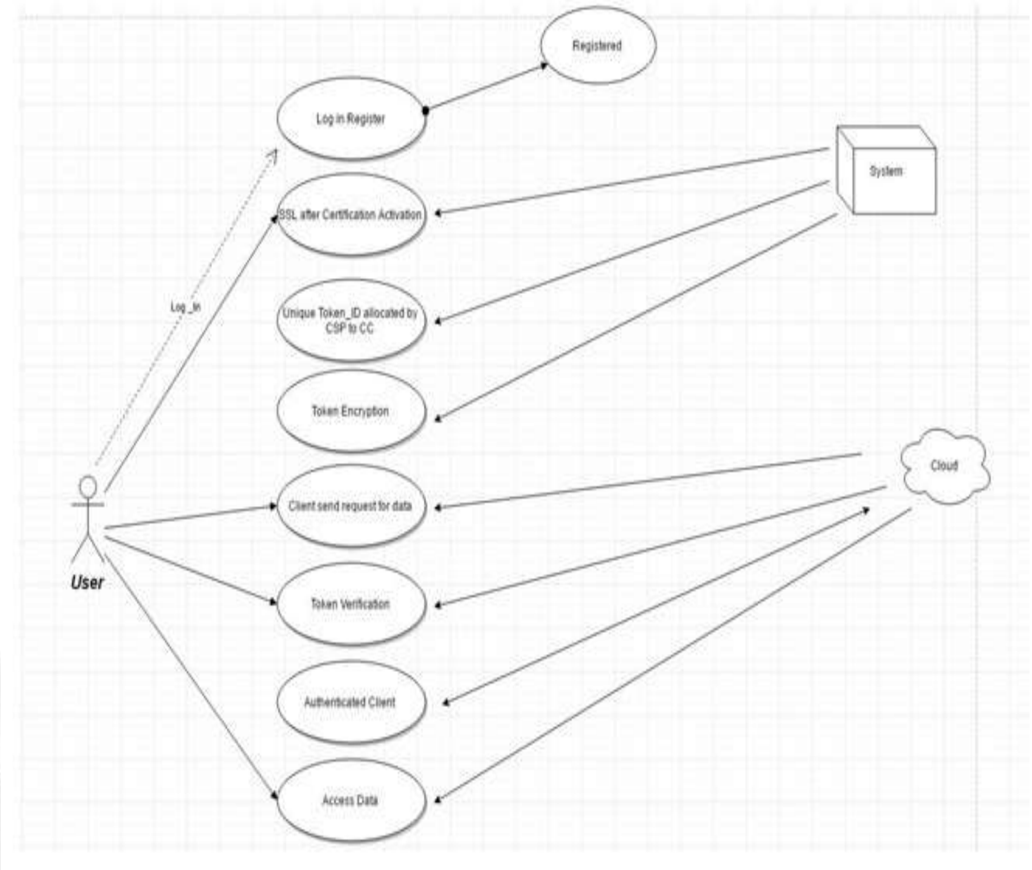

Figure 3.3: use case diagram for working in cloud with token encryption

3.2.2 Use Case Diagram

A use case diagram at its simplest is a representation of a user's interaction with the system that shows the relationship between the user and the different use cases in which the user is involved. A use case diagram can identify the different types of users of a system and the different use cases and will often be accompanied by other types of diagrams as well.

3.2.3 Activity Diagram

Activity diagram are graphical representations of work processes of stepwise exercises and actions with backing for decision, emphasis and simultaneousness. In the Unified Modeling Language, action outlines are planned to demonstrate both computational and hierarchical procedures (i.e. workflows).Activity charts demonstrate the general stream of control.

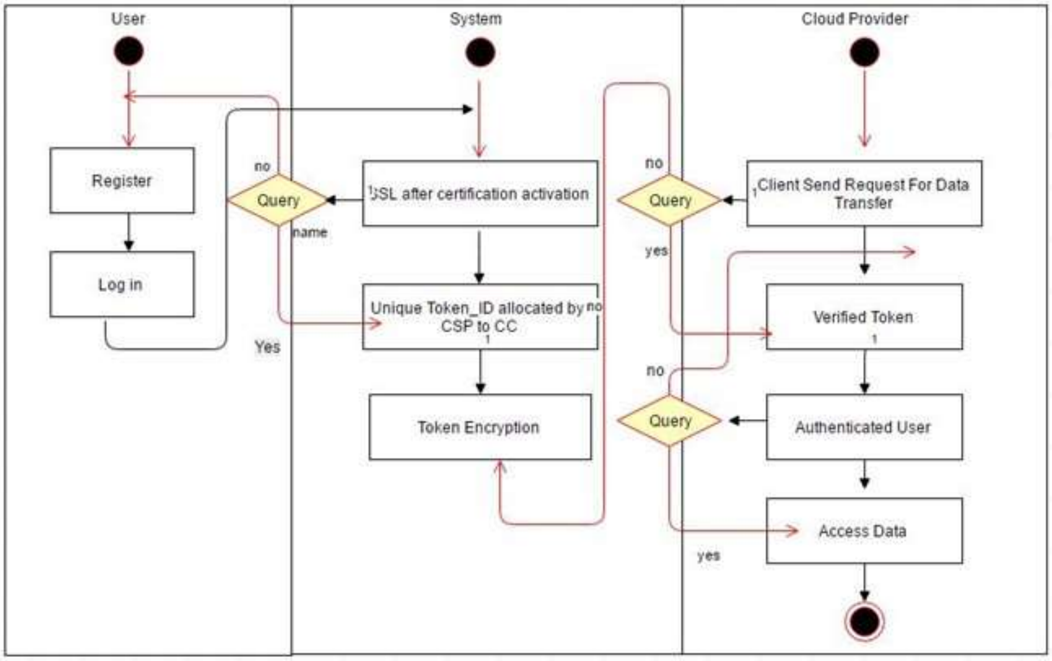

Figure 3.4: Activity diagram for working in cloud with token encryption

3.3 System design Conclusion

By designing UML charts, we can say that, UML (Unified Modelling Language) which permits the formal acceptance of constant inserted frameworks displayed with UML Diagrams. Formalizing the UML is exceptionally testing, not just as a result of the sheer size of the standard, its number of ideas and documentations. Indeed, even the we utilized of UML have communicated the sentiment that there is an excess of cover and repetition in the documentations of UML. UML takes after the item situated ideas and system.

4.EVALUATION

4.1 SSL (Secure Socket Layer)

1. A browser or server attempts to connect to a Website, a.k.a.Web server, secured with SSL. The browser/server requests that the Web server identify itself.

2. The Web server sends the browser/server a copy of its SSL certificate.

3. The browser/server checks to see whether or not it trusts the SSL certificate. If so, it sends a message to the Web server.

4. The Web server sends back a digitally signed acknowledgement to start an SSL encrypted session.

5. Encrypted data is shared between the browser/server and the Web server[10].

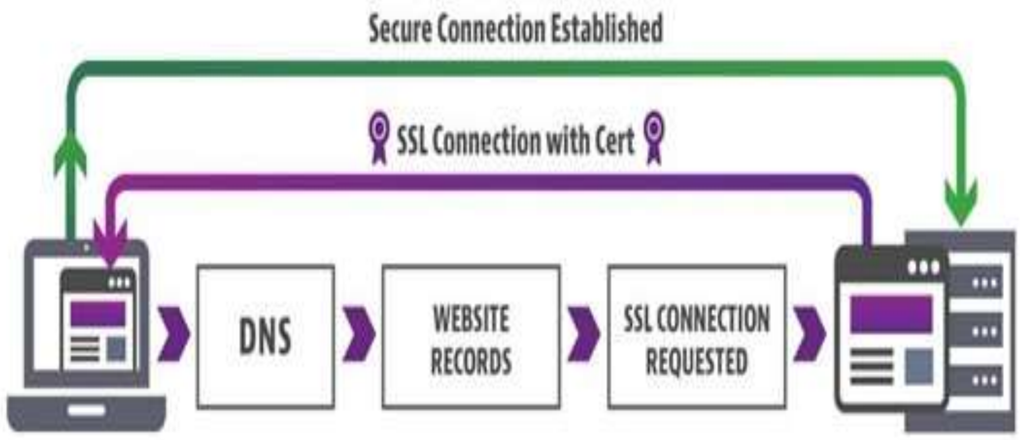

Figure 4.1: SSL (Secure Socket Layer) Working

4.2 N-Layer Architecture

A public-key cryptography algorithm which uses prime factorization as the trapdoor one-way function. Define n == p,q for p and q primes. Also define a private key and a public key such that de =1(mod (n)), (e, mod (n))=1,

where (n) is the totient function, (a,b) denotes the greatest com- mon divisor (so (a,b)=1 means that a and b are relatively prime), and a=b(mod m) is a congruence. Let the message be converted to a number m. The sender then makes n and e public and sends E=Me (mod n).

To decode, the receiver (who knows d) computes

Ed=(Me)d=Me d=MN mod (n)+1=M (mod n)

since n is an integer. In order to crack the code, d of must be found.

But this requires factorization n since mod(n)=(p-1) (q-1)

Both p and q should be picked so that P+1 and q+1 are divisible by large primes, since otherwise the Pollard p-1 factorization method or Williams p+1 factorization method potentially factor n easily. It is also desirable to have ((p q)) large and divisible by large primes.

4.3 Evaluation Conclusion

Security of the Cloud relies on trusted computing and cryptography. Only the authenticated and authorized user can access the data, even any unauthorized user want access the data he cant allow.SSL use for the secure File transmission as well as used the N- Layer encryption algorithm that can give better solution for the data security.

5.Conclusion

So, no of references and gaining of data no of security algorithm are available for secure data. but todays date hacker or cracker and are also powerful. The security most important task so, I conclude that The results of this algorithm prove that TBDSA with cryptography provide a high level security during data transmission. And I hope that is the best solution for saving data on cloud in proper as well as secure manner.

6.Bibliography

1. Rashminigoti and Dr. Shailendra singh, 2013. A survey of cryp- tographic algorithm for cloud computing, International journal of emerging trends and computer application systems.

2. R.K Seth and Rimmy Chuchra March-April-2014.TBDSA- A new data security algorithm in cloud computing, International journal of computer science and information technology.

3. en.wikipedia.org/wiki/TinyEncryptionAlgorithm

4. T.Sivasakthi and Dr.Prabakarn Feb-2014.Applying digital sig- nature with encryption algorithm of user authentication for data security in cloud computing, International journal of innovative research in computer and communication engg.

5. M.Vijayapriya Sept-2013, Security algorithm in cloud comput- ing: Overview, International journal of computer science and emerging technology.

6. http://ijaiem.org/volume3issue3/IJAIEM-2014-03-17-048.pdf

7. https://en.wikipedia.org/wiki/Cloudcomputingarchitecture

8. https://www.researchgate.net/publication/239732057CloudStorageArchite

9. https://www.draw.io

10. https://www.entrust.com/wp-content/uploads/2015/08/HowSSLWorksCh

11. http://mathworld.wolfram.com/RSAEncryption.html

12. http://www.tutorialspoint.com/cryptography/tripledes.htm

13. https://en.wikipedia.org/wiki/Randomnumbergeneration