Implementation of a Mechanism to Enhance Data Security and User Authorization in Cloud

Zeenat Qamar Ansari[*1], Dr. Tulika Pandey[*2]

1. M.Tech(CSE), Research Scholar
2. Assistant Professor

Dept. Of Computer Science and IT, SHUATS, Allahabad, India

[1]zeenatansari61@gmail.com

[2]tulika.tulika@shuats.edu.in

***Abstract*— Now a day's cloud computing has become one of the main topic of IT and cloud data storage security is major concern. Cloud is the fastest growing technology. This technology provides access to many different applications. Cloud computing is used as data storage so data security and privacy issues such as confidentiality, availability and integrity are important factor associated with it. Cloud storage provides user to access remotely store their data so it becomes necessary to protect data from unauthorized access, hackers or any type of modification and malicious behaviour. Security is an important concern. The meaning of data storage security is to secure data on storage media. Cloud storage does not require any hardware and software management. It provides high quality applications. As we proposed the concept of cloud data storage security strategy capable to overcome the shortcomings of traditional data protection algorithms and improving security using steganography, encryption decryption techniques, compression and splitting technique adoptable to better security for the cloud. We have developed a desktop application through which user can share data. This thesis enhanced advance security goal for cloud data storage.**

***Keywords*— Cloud data, Security, encryption, decryption, privacy.**

I. INTRODUCTION

The National Institute of Standards and Technology (NIST) define cloud computing as "a model for user convenience, on-demand network access contributes the computing resources (e.g. network, storage, application, servers and services) that can be rapidly implemented with minimal management effort or service provider interference" [5]. The users can access the cloud data and application at anytime and anywhere. The cloud contains large number of servers required to deliver scalable and reliable on-demand services [5]. Cloud Computing is an emerging information technology that change the way of IT architectural solution. It is a new pattern of business computing. Computing refers to manipulating Cloud, Configuring and Accessing the Applications online [2]. It offers the online data storage, Infrastructure and applications. It overcomes the Platform dependency issues because it do not need to install the software on our local PC. Cloud computing provides information resources for users in "CLOUD" through the Internet [1][2]. As we proposed the concept of cloud data storage security strategy capable to overcome the shortcomings of traditional data protection algorithms and improving security using encryption decryption techniques DDES (Double Data Encryption standard) and RNS (Residue Number System) are adoptable to better security for the cloud. We have developed a desktop application through which user can share data. This paper enhanced advance data security and user authorization in cloud.

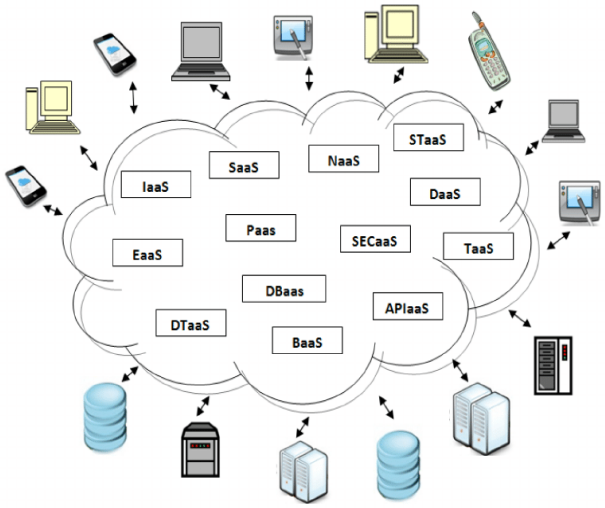

Figure 1. Cloud Computing Diagram

.

Cloud computing is a general term for anything that involves hosted services over the Internet. These services are broadly divided into three categories: [6]

Infrastructure as a Service (IaaS): In IaaS model computer resources such as storage, computing capabilities are made available to the customer on demand. It's cost saving model. In this model customer only pay to use IT infrastructure as needed.[14]

E.g: Amazon Web Services, Virtual machines, servers, storage, load balancers, network.

Platform as a Service (PaaS): In the PaaS model a development environment is offered to the customer which is managed by the provider. On which customer can develop and run their applications without building and managing complex infrastructure.[14]
E.g: Google Application Engine, Execution runtime, database, Web server, Development tools.

Software as a Service (SaaS): In the SaaS model an application is offered to the customer by the cloud service provider. In which application is hosted by the provider at their infrastructure and distributed over the network as a service on demand.[14]
E.g: Online word processing and spreadsheet tools, Microsoft office, Email, communication, Games.
Cloud computing is typically classified in four types.

Public cloud: Public cloud is publicly accessible cloud which is managed by third parties. All customers share a common infrastructure pool with limited configuration. The cloud provider is responsible for creation and ongoing maintenance of the public cloud.[6][14]

Private Cloud: Private cloud is accessible only by an organization and also managed by the organization. Private cloud enables an organization to use cloud computing by means centralizing access to IT resources from different geographical location. .[6][14]

Hybrid cloud: Hybrid cloud combines both public and private cloud models. With Hybrid cloud organization can utilize third party cloud provider service in a full or partial manner. Thus, Hybrid cloud increases flexibility of computing.[6][14]

Community Cloud: Community cloud is a multi-tenant infrastructure which is shared among several organizations. And it is managed, governed and secured by all the participating organization. These organizations have similar cloud requirements and their ultimate goal is to achieve business objective. It is beneficial in order to cost saving.
Cloud based environment there are many security issues such as authentication, integrity, privacy, virtualization, confidentiality, large amount data processing, scalability, access control etc.[8] Traditional security approaches are no longer suitable for data and application in cloud. [1][2][3][4].

The following section highlights, Section one introduction of cloud security and privacy. Section two a review of literature on security issues in cloud computing and the remaining sections are organized as follows. Section three discusses overview of cloud computing in cloud computing laying emphasis on SaaS, PaaS and IaaS; and cloud computing deployment methods. Section four deployment models of cloud. Section five discusses modules description. Section six discusses security algorithms. Section seven presents the result discussion. Section eight present the conclusion.

II. LITERATURE SURVEY

Subhashini et al.[2011][2] have depicted all security related issues present in the distributed computing. The different organizations of the cloud and every one of the issues present in every sending are been characterized in the paper. They have characterized in regard to the administration conveyance where in each kind of SaaS, PaaS, and IaaS. They specifically characterized all the security issues in the product as an administration of distributed computing. In Issues of SaaS, there are classifications dependent on information, arrange, web applications and virtualization vulnerabilities.
Balachandra reddy et al.[2010][4] have talked about administration level understandings that are been issued by client to supplier before getting into cloud. This is the main trust a supplier will see from client, yet it insufficient to give security as it doesn't answers the issues to the misfortunes of the client, there ought to be sure changes as per the sort of administration a client is working and should be institutionalized with favored client get to, information isolation, area of information and so on.
Kresimer Popovic et al.[2010][7] have talked about various security concerns present in the cloud display which is losing privacy and uprightness of the information while exchange, stockpiling and recovery. They additionally examined on the things that will be think about where the dangers are available in distributed computing like from client to kind of administrations. With the above issues they reasoned that we have to take security and protection in giving cloud administrations.
Patrick Mc. Daniel et al.[2010][10] portrayed about difficulties of security and upgrades that are to be made over cloud for secure information over cloud. They focused chiefly on security issues over cloud occurrences. The occurrences over cloud will keep running on some base framework which may trade off and causes a security issue. There are additionally outside foes over cloud which may need security of occasions from outsiders. They talked about specific open doors which are to the extraordinary difficulties for analysts. The distributed computing security concerns were examined in detail in [13] the primary issues talked about were protection worries because of outsider clients. As the security because of programmer's increment over web and the distributed computing is absolutely on web, there are diverse issues like assaults are examined on it.
Sameera Abdulrahman Almulla et al.[2010][11] have examined about administration in distributed computing ,the difficulties with respect to the data security worries in regards to classification, integrity and accessibility. They talk about security difficulties of distributed computing in regards to character and access the executives.
Steve Mansfield et al.[2008][12] has talked about with respect to the upsides of having the cloud in the meantime the issues present in cloud. When we use in our edge territory we

utilize numerous security sides like firewalls DMZ'z and so on., where as in cloud all are on a remote framework with no security. Creator predominantly indicates out that we require have a lot of trust in the plan of framework with great validation and approval capacities.

1.1 MOTIVATION

Cloud security is important for both business and personal users. Everyone wants to know that their information is safe and secure. Some methods of securing customer data from cloud providers are based on Trusted Computing (TC) Technologies such as Trusted Platform Module (TPM). But the protection of data is controlled by third party and does not give data publisher full control. Data Centric Security (DCS) is another approach where the data is protected before outsourcing it to cloud. The cryptography technologies are the main security tools for the DCS approach. In general, a new security is required to enable cloud resources to be utilized efficiently by customer without exposing their sensitive data and private information to unauthorized entities including the cloud providers. In addition, the data publishers are able to control their outsourced data security and privacy and verify security conditions, such as integrity of data at anytime.

III. OVERVIEW OF CLOUD COMPUTING

In Cloud Computing, we talk about a disseminated design that brings together server assets on a versatile stage, so that accommodate cloud administrations and on-request figuring assets. Cloud specialist co-ops (CSP‟s) propose cloud stages for their customer's fulfillment by using and making their web administrations. Web access suppliers (ISP‟s) offer customers to enhance the fast broadband to get to the web. CSPs and ISPs (Internet Service Providers) together offer administrations. Distributed computing is an imperative model that permits increasingly advantageous to access, on-request organize access to a mutual pool of configurable figuring assets like systems, servers, stockpiling, applications that can be immediately provisioned and discharged with administration provider's communication or negligible administration exertion. By and large, cloud providers offer three sorts of administrations, i.e. programming as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). There are a few explanations behind associations to move towards IT arrangements that incorporate distributed computing as they are basically required to pay for the assets on utilization premise. Mists are the development of the dispersed frameworks in the creative pattern, the ancestor of cloud being the matrix. The client does not ready to require skill or colleague to control the framework of mists; it gives just deliberation idea. It tends to be produced as an administration of an Internet with increment adaptability, higher throughput, enhances nature of administration and registering power. Distributed computing suppliers convey visit online business applications, which are gotten to through an internet browser from servers [1].

A. Characteristics of Cloud Computing

- **Ultra large-scale:** In ultra vast scale processing, the size of cloud is extensive union. The billow of Google has possessed more than one million servers get to. For instance, IBM, Microsoft, Yahoo, Rediff, Amazon they have more than several thousand servers. There are many servers in a venture control get to.
- **Virtualization:** Distributed computing makes client to get to benefit all over, through a terminal. All that you can finish the procedure through a web access by utilizing a note pad PC or an advanced cell or a Tablet or a Laptop. Clients can accomplish or share it safely through a straightforward way, whenever, anyplace. Clients can finish an assignment that can't be finished in a solitary PC.
- **High reliability:** Cloud applies information multi transcript blame tolerant, the calculation hub isomorphism interchangeable thus as to enhance and guarantee the high unwavering quality of the cloud benefit. By utilizing distributed computing is profoundly dependable than neighborhood PC process connection.
- **Versatility:** Distributed computing can create a few sorts of uses upheld by cloud administration, and single cloud can keep up various applications running in the meantime.
- **High extendibility:** The size of cloud can exceptionally stretch out or progressively want to meet the expanding necessity of cloud administrations.
- **On demand service:** Cloud is a huge asset pool, which will you can pay as per your prerequisite; cloud is much the same as that running water, electric, and gas that can be charged by the sum that you utilized.
- **Extremely inexpensive**: The focused on the board of cloud makes the endeavor needn't embrace the administration cost of the server farm that expansion speed of the administration. The flexibility can enhance the usage rate of the available assets contrasted and conventional frameworks, accordingly clients can thoroughly appreciate the cloud administration and minimal effort as favorable position or to a great degree modest.

IV. DEPLOYMENT MODELS OF CLOUD

The cloud can be deployed in three models. They are described in different ways. In generalized it is described as below:

A. Public Cloud: Open cloud depicts distributed computing in the customary standard sense, whereby

assets are progressively provisioned on a fine-grained, self-benefit premise over the Internet, through web applications/web administrations, from an off-website outsider supplier who charges on a fine-grained utility registering premise. This is a general cloud accessible to open over Internet.

B. Private Cloud: A private cloud is one in which the administrations and foundation are kept up on a private system. These mists offer the best dimension of security and control, however they require the organization to at present buy and keep up all the product and framework, which lessens the cost funds.

C. Hybrid Cloud: A half and half cloud condition comprising of different inward as well as outer suppliers "will be normal for generally ventures". By incorporating numerous cloud administrations clients might have the capacity to facilitate the change to open cloud administrations while staying away from issues, for example, PCI consistence.

V. MODULES DESCRIPTION IN PROPOSED SYSTEM

A. Admin

Domain Authority is a super user who creates the Data Owner user and maintains the Proxy servers' configurations. He has the writes to Add, Edit or Delete any number of Data owners.
Once the Domain Authority logged in he has following functions.
Step 1. Admin can add , edit, delete server.
Step 2. Admin can add new data owner, edit and delete data owner details.
Step 3. Admin can view Domain (View Only)
Step 4. Admin can view Sub-Domain (View Only)

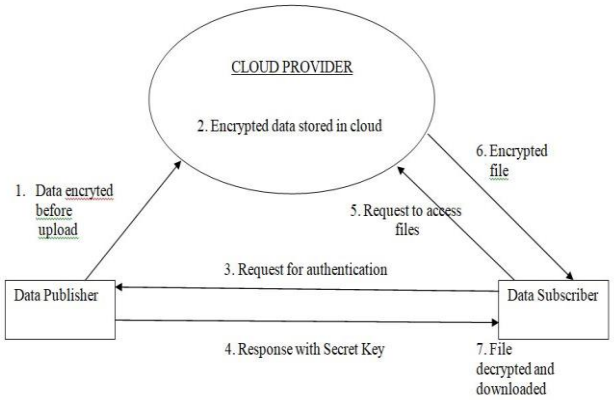

Figure 2. Proposed system architecture

B. Data Publisher

Data Publisher is a person who will store the files in Proxy which in turn accessed by the authorized subscriber. Data Publisher is like a Librarian who will upload all files in the system. Whenever the file is uploaded it will be encrypted by the system using Data Publisher Encryption Key. Data Publisher has to specify the Access Policy for each and every file. Access policies are set using Domain Attribute and Sub-Domain Attribute.

Once the Data Owner logged in he has following functions.

Step 1. View/delete User Details
Step 2.View User Request & Send Secret File
Step 3. Verify Identity Token
Step 4. Send Secret Key to requested subscriber
Step 5. File Upload
Step 6. View/delete Uploaded File Details
Step 7. Setting of File Access Control
Step 8. View/delete File Access Control Details
Step 9. Manage Transaction Details
Step 10. Change Password

File Upload Process

Data publisher uploads the encrypted file. Encryption is done using RNS and DES for more security. The Uploaded file is saved to a cloud selected by the system randomly. Data publisher does not know about the cloud on which the selected file is stored. File upload process is presented below.

1. Select file
2. Generate DES key
3. Encrypt selected File using DES
4. Generate RNS key
5. Encrypt previous encrypted file using RNS
6. Select cloud randomly

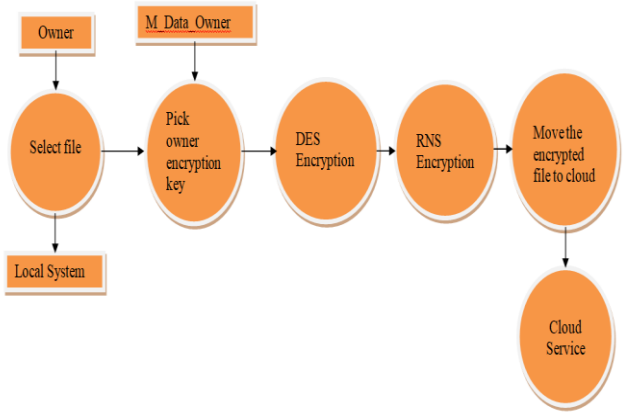

Figure 3. DFD Upload Service

C. Data Subscriber

Data Subscriber is a person who will access (download/view) data, suppose publisher is a college Liberian and subscribers are students, lectures and admin staff in a college. Data Subscriber will register and then demand for desired file. He will receive the Identity Token through email. User will receive their access key (Attributed based Decryption Key) from respective publisher through email. With the help of the

access key data subscriber will be able to download the files for which he has access.
Suppose the subscriber wants to download any file, first he has to select the file from the list and the system ask for the access key, After system getting the access key it will separate the Attribute Set from the key and check for the access rights, if the user has the access he can download the encrypted file which in turn decrypted using the decryption key and download to the subscriber local system.

Data Subscriber will be an authorized user after the following process
Step 1. Subscriber Registration – (User)
Step 2. Fill the user details
Step 3. Provide Domain and Sub Domain Details
Step 4. An Identity Token key will be generated
Step 5. Identity Token key will be send to the Subscriber on his registered email Id
Step 6. Now Data Subscriber will Login with two step verification
Step 7. Fill registered email Id and password
Step 8. Upload the identity token key send on email
Step 9.After Identity Token key Verification Data Subscriber will be logged in

Once the User logged in he has following functions.

Step 1. View the uploaded file details
Step 2. Request for Data Publisher's secret key
Step 3. Using the secret key of Data Subscriber, file will be downloaded
Step 4. View the transaction
Step 5. Change password.

File Download Process
Data Subscriber will login by using his identity key which was downloaded from his email and located on its local system. After login he will select for required file to download, a request will be send for that required file If the person is registered to view that file, he will be verified by checking the secret key Access control will be verified, if he is the legitimate user then, a two layer encrypted file form the cloud will be downloaded and saved on its local system
File download process is presented below.

1. Select file
2. Upload data publisher's Secret key
3. Verify the key
4. Generate DES key
5. Decrypt selected File using DES
6. Generate RNS key
7. Decrypt previous decrypted file using RNS
8. File will be downloaded to data subscriber local machine

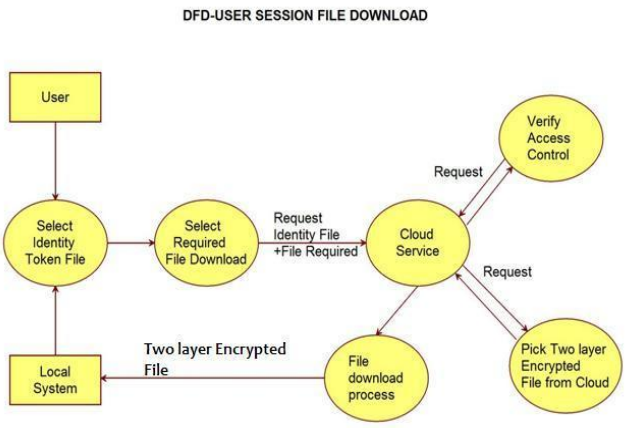

Figure 3 DFD User Session File Download

VI. SECURITY ALGORITHMS

In Cloud Storage, any person's or association's information is depicting about open and keep up from various associated and conveyed assets that give to a cloud. Encryption calculation [25] assumes a critical job to give secure correspondence over associated and appropriated assets by utilizing the key device for ensuring the information. Encryption calculation has fundamentally changed over the information into mixed kind to ensure by utilizing "the key" and transmitter client just have the way to unscramble the information. There are two kinds of key encryption systems utilized in security calculations; they are symmetric key encryption and awry key encryption. In symmetric key encryption, single key is utilized to scramble and decode the information. Two keys are principally utilized in uneven key encryption. They are private key and open key. In Public key process, it is utilized for encryption. Another private key is utilized for unscrambling [26]. There are various existing procedures used to acknowledge security in distributed storage. The principle center is about cryptography to make information secure while transmitted over the system. Cryptography idea is that the reconsider and practice of procedures for anchoring correspondence and information inside the nearness of foes. In cryptography idea, encryption and unscrambling strategies are utilized. An encryption procedure changes over message or plaintext into figure content and decoding strategy separates the first message or plaintext into similar figure content. At first, the data must be encoded and transmitted by utilizing the encryption calculation in cryptography. Besides, the data ought to be unscrambled by utilizing the decoding strategy the collector side can peruse the first data.

- **Data Encryption Standard (DES) Algorithm:** The Data cryptography standard (DES) [29] is a symmetric-key square figure found as FIPS-46 inside the Federal Register in January 1977 by the National Institute of Standards and Technology (NIST). In encryption site, DES takes a 64-bit plaintext and makes a 64-bit figure content, after that the unscrambling site, it takes a 64-bit figure message

and makes a 64-bit plaintext. Every encryption and unscrambling methods are utilized for same 56 bit figure key. The encryption procedure is made of two changes (P-boxes), that we tend to call introductory and last stage, and sixteen Feistel rounds [30]. Each round transmits an alternate 48-bit round key produced from the figure key encryption.

- **Residue Number System (RNS) Algorithm:** The residue number system (RNS) is a method for representing an integer as an *n*-tuple of its residues with respect to a given base. Since RNS has inherent parallelism, it is actively researched to implement a faster processing system for public-key cryptography. The residue number system (RNS) is a method for representing an integer in which a given integer *x* is represented by its residues divided by a base of integers, which are pairwise co-prime. If we denote the base by B={m1,m2,…,mn}B={m1,m2,…,mn} and the RNS representation of *x* as [x1,x2,…,xn][x1,x2,…,xn], it holds that xi=xmodmixi=xmodmi. The main feature of RNS is that addition, subtraction, and multiplication are carried out by independent addition, subtraction, and multiplication with respect to each base element. The operation flow at each base element is called a channel. If each channel has a processing unit, an *n*-fold speed increase can be achieved, as compared with the case with a single processing unit. This parallelism seems attractive in pursuing efficient computation of public-key cryptography, which is constructed by integer operations of several hundred or several thousand bits with a modular reduction.

- **MD5-**(Message-Digest calculation 5): Generally, the cryptographic hash work calculation is utilized with a 128-piece hash esteem and procedures a variable length message into a settled size yield of 128 bits. At first, the information message is separated into lumps of 512-piece squares a short time later the message is secured so its aggregate length is distinct by 512. In this procedure, the transmitter of the information uses the general population key to encode the message and the collector utilizes its private key to decode the message.

Pseudo codes for Encryption are follows:

```
publicclassDES_Algorithm
{
static//byte[] buf = new byte[1024];
byte[] buf = newbyte[2048];
static Cipher ecipher;
static Cipher dcipher;
publicstatic String DESKeyGeneration()
{
RandomValuerv=newRandomValue();
String key=rv.DESKeyValue();
return key;
}
publicDES_Algorithm(SecretKey key) throws Exception
{
byte[] iv = newbyte[] { (byte) 0x8E, 0x12, 0x39, (byte) 0x9C,
0x07, 0x72, 0x6F, 0x5A };
AlgorithmParameterSpecparamSpec =
newIvParameterSpec(iv);
ecipher = Cipher.getInstance("DES/CBC/PKCS5Padding");
dcipher = Cipher.getInstance("DES/CBC/PKCS5Padding");
ecipher.init(Cipher.ENCRYPT_MODE, key, paramSpec);
dcipher.init(Cipher.DECRYPT_MODE, key, paramSpec);
}
publicclassHashingTechnique
{
publicstatic String MD5(String data)
{
String output="";
try
{
MessageDigest digest = MessageDigest.getInstance("MD5");
byte[] buffer = newbyte[8192];
buffer = data.getBytes();
digest.update(buffer);
byte[] md5sum = digest.digest();
BigIntegerbigInt = newBigInteger(1, md5sum);
output = bigInt.toString(16);
System.out.println("MD5: " + output);
}
catch (Exception e)
{
System.out.println("Opps,Exception In MD5 Algorithm.");
}
return output;
}
}
```

VII. RESULTS

In this proposed work a Web application is developed. The application can be accessed through Web Page from where below actions can be performed; User registration for following roles – Data Publisher and Data Subscriber. In this application a method is developed through which a user can share files with other users. The page is user friendly which simplifies the steps for user to access it by simply Signing In and select the available options to access or upload the files available with specific roles. When Data Publisher upload the files, name of the files get saved to MYSQL database table. To download the file, Data Subscriber must send a request to Data Owner who may give permission to download by sending a key mail to requested user's registered email. RNS and DES algorithm is used for Encryption.

Comparison of Existing and Proposed System

- Proposed system provides high security for data since it is in un-understandable format in cloud whereas existing system stores the data in original form
- Proposed system provides two layer encryption, first DES and second RNS encryption before uploading to cloud whereas existing system uses single layer encryption.
- Proposed system provides distributed storage in cloud. Data get stored in different folder / place / file where as in existing system all get stored in single place / file / folder.
- Data Integrity is preserved, since there is no assurance for data trustworthiness by different cloud provider, when data service is outsourced to the cloud, at that point ensuring its storage correctness and integrity emerges, since in proposed model, data is encrypted on local machine before outsourcing it to cloud.
- Data Confidentiality is preserved as the data are self-protected and the protection cannot be undone in the cloud or anywhere else by any authorized entity. For e.g, by keeping the data encrypted all the time at the cloud, even the cloud provider cannot decrypt. The data confidentiality is protected even if there are security breaches in the cloud.
- Privacy of data access policies is preserved as the access to data is enforced under the secure policies hidden inside the data. Access is performed without the necessity of exposing these policies or any sensitive information to a cloud provider.
- Data privacy and integrity rely on the strength of the cryptographic methods used. Since the proposed model is using DES and RNS so it provide security strength to the data because it requires secret key and RNS modulii hence it is Impossible to decrypt without knowing secret key and RNS modulii ,so it is strong.
- Scalability can be measured in several aspects. Because in the DCS approach, each set of data has its own access control enforcement, the data set can be moved within the cloud environment without restriction related to access control enforcement. Furthermore, self-protected data allow the cloud to distribute information resources efficiently with less worry about trust requirements.
- Virtual machine (VM) data leakage possibility will not expose sensitive data for unauthorized entities because the data in the cloud are encrypted and can only be decrypted outside a cloud environment. Although a data set including its security parameters can be leaked, an unauthorized entity cannot access the data contents without breaking its encryption.

Enhancement in User Authentication

- In Proposed system, for authentication part it uses id, password and user identity key which is send on user mail and saved on its local system, where as in existing system we need Id and password for authentication.

VIII. CONCLUSION AND FUTURE SCOPE

Cloud computing is growing as a new thing and it is the new trend indeed and many of the organizations and big companies are moving toward the cloud but lagging behind because of some security problems[7]. Cloud security is an ultimate concept which will crush the drawbacks the acceptance of the cloud by the big MNCs, companies and organizations. There are a lot of security algorithms which may be implemented to the cloud. DES, RSA, ECC, Triple-DES, AES, and Blowfish etc are some symmetric and asymmetric algorithms.[7] DES and AES are mostly used symmetric algorithms as they are relatively more secure. DES is quite simple to implement than AES. In proposed system we discussed about cloud storage security issues and challenges. In future we will try to deploy this in other cloud based environment and the best can be chosen. In future standard can be developed for cloud storage security. We will try to find out problems related to existing security algorithms and implement better version of existing security algorithms.

REFERENCES

[1] Lombardi F, Di Pietro R. Secure virtualization for cloud computing. Journal of Network Computer Applications (2010), doi:10.1016/j.jnca.2010.06.008.

[2] Subashini S, Kavitha V., “A survey on security issues in service delivery models of cloud computing,” Journal of Network and Computer Applications (2011) vol. 34 Issue 1, January 2011 pp. 1-11.

[3] Sudha.M, Bandaru Rama Krishna rao, M.Monica, “A Comprehensive approach to ensure secure data communication in cloud environment” International Jornal Of computer Applications, vol. 12. Issue 8, pp. 19-23.

[4] Balachander R.K, Ramakrishna P, A. Rakshit, “Cloud Security Issues, IEEE International Conference on Services Computing (2010),” pp. 517-520.

[5] Cong Wang, Qian Wang, KuiRen, and Wenjing Lou, “Ensuring Data Storage Security in Cloud Computing” proceeding of International workshop on Quality of service 2009”, pp.1-9.

[6] Gary Anthes, “Security in the cloud,” In ACM Communications (2010), vol.53, Issue11, pp. 16-18.

[7] KresimirPopovic, ŽeljkoHocenski, “Cloud computing security issues and challenges,” MIPRO 2010, pp. 344-349.

[8] KikukoKamiasaka, Saneyasu Yamaguchi, Masato Oguchi, “Implementation and Evaluation of secure and optimized IP-SAN Mechanism,” Proceedings of the IEEE International Conference on Telecommunications, May 2007, pp. 272-277.

[9] Luis M. Vaquero, Luis Rodero-Merino, Juan Caceres1, Maik Lindner, “A Break in Clouds: Towards a cloud Definition,” ACM SIGCOMM Computer Communication Review, vol. 39, Number 1, January 2009, pp. 50-55.

[10] Patrick McDaniel, Sean W. Smith, “Outlook: Cloudy with a chance of security challenges and improvements,” IEEE Computer and reliability societies (2010), pp. 77-80.

[11] SameeraAbdulrahmanAlmulla, Chan YeobYeun, “Cloud Computing Security Management,” Engineering systems management and its applications (2010), pp. 1-7.

[12] Steve Mansfield-Devine, “Danger in Clouds”, Network Security (2008), 12, pp. 9-11.

[13] Anthony T. Velte, Toby J.Velte, Robert Elsenpeter, Cloud Computing: A Practical Approach, Tata McGrawHill 2010.

[14] Lizhe Wang, Jie Tao, Kunze M., Castellanos A.C., Kramer D., Karl W., "Scientific Cloud Computing: Early Definition and Experience," 10th IEEE Int. Conference on High Performance Computing and Communications, pp. 825-830, Dalian, China, Sep. 2008, ISBN: 978-0-7695-3352-0.

[15] Pring et al., "Forecast: Sizing the cloud; understanding the opportunities in cloud services," Gartner Inc., Tech. Rep. G00166525, March 2009.

[16] AmanBakshi, Yogesh B. Dujodwala, "Securing cloud from DDoS Attacks using Intrusion Detection System in Virtual Machine," ICCSN ‟10 Proceeding of the 2010 Second International Conference on Communication Software and networks, pp. 260-264, 2010, IEEE Computer Society, USA, 2010. ISBN: 978-0-7695-3961-4.

[17] H. KAMAL IDRISSI, A. KARTIT, M. EL MARRAKI FOREMOST SECURITY APPREHENSIONS IN CLOUD COMPUTINGJournal of Theoretical and Applied Information Technology 31 st January 2014. Vol. 59 No.3

[18] Kuyoro S. O, Ibikunle F. &Awodele O Cloud Computing Security Issues and ChallengesInternational Journal of Computer Networks (IJCN), Volume (3) : Issue (5) : 2011

[19] Chunye Gong, Jie Liu, Qiang Zhang, Haitao Chen and ZhenghuGongngThe Characteristics of Cloud Computing2010 39th International Conference on Parallel Processing Workshopse Brazilian Computer Society 2010

[20] SO, Kuyoro. Cloud computing security issues andchallenges. International Journal of Computer Networks, 2011, vol. 3, no 5.

[21] D. H. Rakesh, R. R. Bhavsar, and A. S. Thorve, "Data security over cloud," International Journal of Computer Applications, no. 5, pp. 11-14, 2012.

[22] J. Krumm, "A survey of computational location privacy," Personal and Ubiquitous Computing, vol. 13, no. 6, pp. 391-399, 2009.

[23] K. Hwang, S Kulkarni and Y. Hu, "Cloud security with virtualized defence and Reputation-based Trust management," Proceedings of 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing (security in cloud computing), pp. 621-628, Chengdu, China, December, 2009. ISBN: 978-0-7695- 3929 -4.

[24] Marios D. Dikaiakos, DimitriosKatsaros, PankajMehra, George Pallis, Athena Vakali, "Cloud Computing: Distributed Internet Computing for IT and Scientific Research," IEEE Internet Computing Journal, vol. 13, issue. 5, pp. 10-13, September 2009. DOI: 10.1109/MIC.2009.103.

[25] AL.Jeeva, Dr.V.PalanisamyAndK.Kanagaram "Comparative Analysis Of Performance Efficiency And Security Measures Of Some Encryption Algorithms" International Journal Of Engineering Research And Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue 3, pp.3033- 3037, May-Jun 2012.

[26] Maha TEBAA, Saïd EL HAJJI, Abdellatif EL GHAZI, "Homomorphic Encryption Applied to the Cloud Computing Security", World Congress on Engineering, Volume I, ISBN: 978-988-19251-3-8; ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online) , 2012.

[27] Pratap Chandra Mandal, „Superiority of Blowfish Algorithm‟, International Journal of Advanced Research in Computer Science and Software Engineering. September (2012) ISSN: 2277-128X Vol. 2, Issue 7.

[28] G. Devi and M. Pramod Kumar, „Cloud Computing: A CRM Service Based on a Separate Encryption and Decryption using Blowfish Algorithm‟, International Journal of Computer Trends and Technology. (2012) Vol. 3 Issue 4, ISSN: 2231-2803, pp.592-596.

[29] Neha Jain and GurpreetKaur „Implementing DES Algorithm in Cloud for Data Security" VSRD International Journal of CS & IT Vol. 2 Issue 4, pp. 316-321, 2012.

[30] G. Devi , M. Pramod Kumar, "Cloud Computing: A CRM Service Based on a Separate Encryption and Decryption using Blowfish algorithm" International Journal Of Computer Trends And Technology Volume 3 Issue 4, ISSN: 2231-2803, pp. 592-596,2012.

[31] D. S. Abdul. Elminaam, H. M. Abdul Kader and M. M. Hadhoud ,"Performance Evaluation of Symmetric Encryption Algorithms", Communications of the IBIMA Volume 8, 2009.

[32] Gurpreet Singh, SupriyaKinger "Integrating AES, DES, and 3-DES Encryption Algorithms for Enhanced Data Security" International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013.

[33] Mr. Gurjeevan Singh, , Mr. AshwaniSingla and Mr. K S Sandha " Cryptography Algorithm Compaison For Security Enhancement In Wireless Intrusion Detection

System" International Journal of Multidisciplinary Research Vol.1 Issue 4, August 2011.

[34] Gurpreet Singh, SupriyaKinger"Integrating AES, DES, and 3-DES Encryption Algorithms for Enhanced Data Security "International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013.