A Mechanism to Enhance the Data Security and User Authorization in Cloud

Shikha Singh[#], Er. Ashish Pandey[*]

[#]Computer Science & Engineering, I.E.T, Dr. Rammanohar Lohia Avadh University, Faizabad, Uttar Pradesh, India.

*Assistant Professor, Dept. of Computer Science & Engineering, I.E.T, Dr. R M L Avadh University Faizabad, Uttar Pradesh, India

Abstract— **Now days cloud computing become one of the main topic of IT and main point is cloud data storage security. 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 provide 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 Double Data Encryption Standard (DDES) encryption and decryption technique and Randam Number System technique adoptable to better security for the cloud. We have developed a web 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 It is a new pattern of business computing. Computing is 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 need not 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(Random 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.

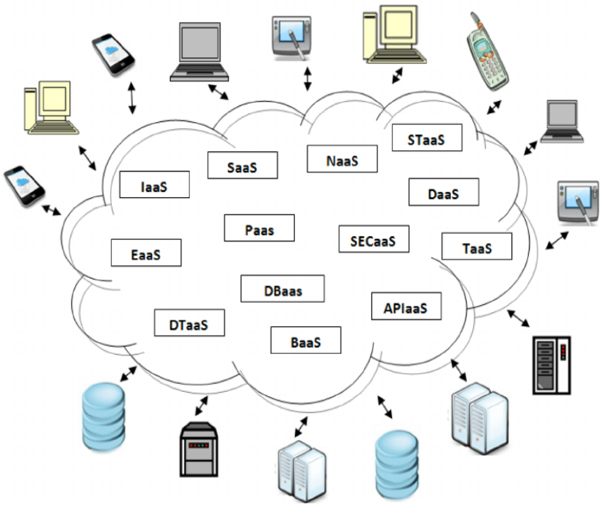

Figure 1. Cloud Computing Diagram

.

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 computingin cloud computing laying emphasis on SaaS, PaaS and IaaS; and cloud computing deployment methods. Section fourdeployment models of cloud. Section five discussesmodules description.Section six discusses security algorithms. Section seven presents the result discussion. Section eight present the conclusion.

II. LITERATURE SURVEY

S.MahdiShariatiet.al[2015][2] investigated the security challenges and issues based on two perspectives that are –Data security, Privacy and protection. Authors also discussed about cloud computing, their services and related challenges such as availability, data location, data isolation and recovery , and also mention risks such as -insecure interface, data loss or leakage malware etc. And also analyzed protection & privacy related issues that are- loss of control, invalid storage etc. and also analysis of data storage issues like–service provider, data integrity recovery & backup with principles such as-transparency, integrity, minimization etc.

DiaoZheet.al[2017][4] to achieve data security of Cloud storage and to formulating corresponding security policy and analyzing the security risks and relate them with the previous research results. And also focus on the relevant security technology which is based on the structural characteristics of cloud storage system.

M. Subhashniet. al [2018][7] discussed about the cloud computing and their characteristics, entites and service models and discuss about the security to the data to maintain confidentiality, integrity availability and privacy. The security issues related to data transmission, privacy, confidentiality, integrity, storage, backup& recovery. Also discuss security algorithms are known as ENCRYPTION ALGORITHM. At last author also discuss various algorithms. such as- RSA, AES, Blowfish, Elliptic Curve Cryptography, Difie-Hellman key exchange.SameeraAbdulrahmanAlmullaet.al[2010][11]have examined about administration in distributed computing ,the difficuManpreetKaur et. al[2016][10] reviewed the comparative analysis of various encryption algorithms. Cloud computing ,data security challenges related with their deployment, service and network related models are described. And also discussed about the encryption algorithms .

PalkeshSoniet. al[2016][11] proposed a survey paper in which deep analysis of security issues are described and also focus on the challenges in Cloud computing.lties 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.

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][2].

A. Characteristics of Cloud Computing

- **Ultra large-scale:** In ultra vast scale processing, the size of cloud is extensive union[5]. 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)

B. Data Owner

Data Owner is a person who will store the files in Proxy which in turn accessed by the authorized subscriber. Data Owner are like Liberian who will upload all the files in the system. Whenever the file is uploaded it will be encrypted by the system using Data Owner Encryption Key.

Data Owner 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. Data owner can view User Details (View, Delete)
Step 2. View User Request & Send Secret File
Step 3. View All Request
Step 4. Send Secret Key to requested user
Step 5. Get RNS Key
Step 6. Get user Domain & Sub Domain Details
Step 7. RNS Keys + Domain Details + Expiry Date
Step 8. Encrypt the above string using DES algorithm
Step 9. Send the Secret file to Requested User Email ID
Step 10. File Upload
Step 11. File Selection
Step 12. Encrypting using RNS
Step 13. Proxy server Selection
Step 14. Move to Proxy
Step 15. Transfer the Encrypted file to selected Proxy
Step 16. Encrypting RNS output using DES in Proxy
Step 17. Uploaded File Details (View, Delete)
Step 18. File Access Control Setting
Step 19. File Access Control Details (View, Delete)
Step 20. Transaction Details
Step 21. Change Password

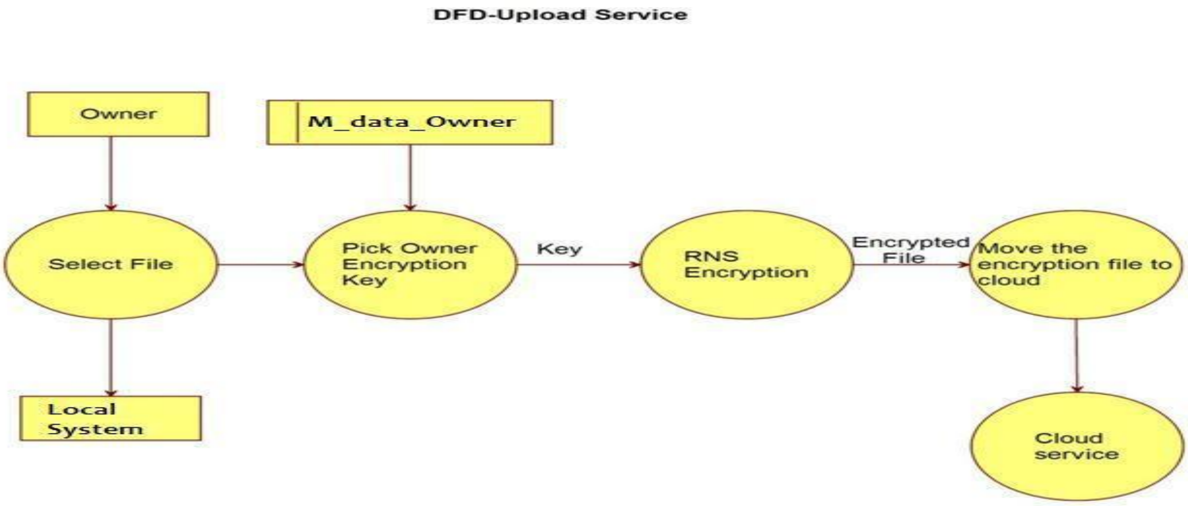

Figure 2. DFD Upload Service

C. **User:**

User are the data access users, suppose publisher is a college Liberian then subscriber are like students, lectures and admin staff in a college.

User can able to register them and 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 they can able to download the files for which they have access, remember access control is set by data owner.

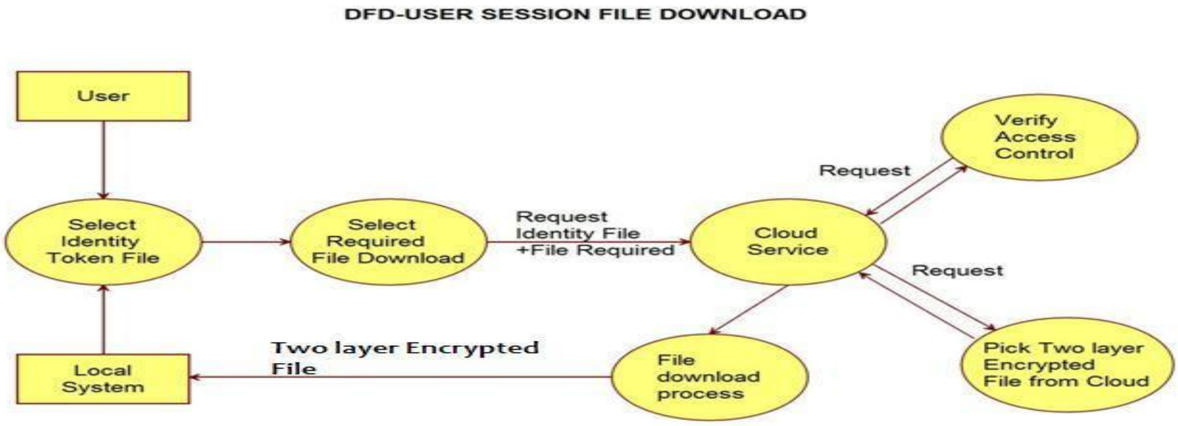
DFD-USER SESSION FILE DOWNLOAD
User
Verify Access Control
Request
Select Identity Token File
Select Required File Download
Request Identity File +File Required
Cloud Service
Request
Two layer Encrypted File
File download process
Pick Two layer Encrypted File from Cloud
Local System

Figure 3 DFD User Session File Download

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.

Once the User *logged in he has following functions.*
Step 1. User Registration – (User)
Step 2. Fill the user details
Step 3. Provide Domain and Sub Domain Details
Step 4. Generate a Identity Token
Step 5. Email Identity Token to the User
Step 6. Login
Step 7. Identity Token Verification

Step 8. Request for Secret Key
Step 9. Upload Identity Token
Step 10. File Details (View)
Step 11. File Download
Step 12. Select the file from the list
Step 13. Select the Secret Identity file from the local system
Step 14. Send secret Identity file and selected file to user
Step 15. Decrypt the Secret identity file
Step 16. Get the Domain Values
Step 17. Check the Access Control using Domain values
Step 18. If Access Control pass fetch the file, Decrypt the file using DES Key or deny the file access
Step 19. Enter the transaction record in the table
Step 20. Send the file to user system
Step 21. Transaction
Step 22. View the transaction of logged user
Step 23. Change password.

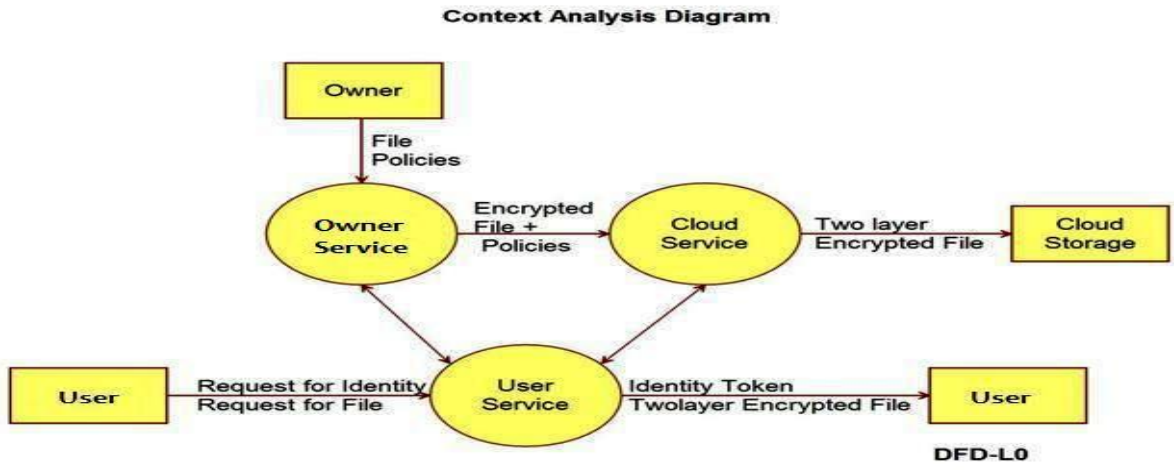

Figure 4 Context Analysis Diagram

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) [27] 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[14]. The encryption procedure is made of two changes (P-boxes), that we tend to call introductory and last stage, and sixteen Feistel rounds [20]. Each round transmits an alternate 48-bit round key produced from the figure key encryption.

- **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[6][3]. 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[16]. 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.

VII. RESULTS

In this proposed work we have developed Web application.For implemented we developed a web page to register the user, data owner and admin. We created a method where user canshare files to other users. We have designed a page in whichuser can simply enter the id of person whom to transfer thefiles and file gets uploaded to cloud server and name of thefiles get saved to MYSQL database table. When user want to download the file he must send a request to data owner and then data owner may give permission to download by sending a key mail to the requested user. RNS and DESalgorithm is used for Encryption.

Table 1.Data Security Enhancement

SN	Existing System	Proposed System
1	No Encryption techniques is used	Proposed system provides high security for data.
2	Directly uploading data to cloud storage. For example Google drive	Before uploading data to cloud, two times data get encrypted, first RNS encryption and DES encryption.
3	In cloud storage all get stored in single place / file / folder	Proposed system provides distributed storage in cloud. Data get stored in different folder / place / file

Table 2. Enhancement in User Authentication

SN	Existing System	Proposed System
1	For user authentication id and password is used.	In Proposed system for authentication apart from id, password it need user identity key.

VIII. CONCLUSIONAND 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] S.MahdiShariati, Abouzarjomehri, M. HosseinAhmadzadegan “Challenges and Security issues in Cloud Computing from two perspectives: Data Security and Privacy Protection,” 2015 IEEE International Conference on Knowledge-Based Engineering and Innovation(KBEI).].

[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] DIAO Zhe, WANG Qinghong, SU Naizheng, ZHANG Yuhan “Study on Data Security Policy Based On Cloud Storage” 2017 IEEE 3rd International Conference on Big Data Security on Cloud.

[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] M.Subhashini, Dr. P. Srivaramangai“ A Study on Cloud Computing Securities and Algorithms,” 2018 |IJSRCSEIT | Volume 3 | Issue3.

[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] ManpreetKaur, KiranbirKaur “A Comparative Review on Data Security Challenges in Cloud Computing,” International Research Journal of Engineering and Technology(IRJET) Volume:03 Issue:01|jan-2016.

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

[12] Subhash Chandra Patel, Ravi Shankar Sing, SumitJaiswal “Secure and Privacy Enhanced Authentication Framework for Cloud Computing” 2015 IEEE SPONSORED SECOND INTERNATIONAL CONFRENCE ON ELECTRONICS AND COMMUNICATION SYSTEM

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

[14] PalkeshSoni, AnkitUpadhyayArvindMaheshwari, PrashantLakkadwala“ Security Related Issues in Cloud Computing : A Survey”IJIRST| Volume 2 |Issue 11 |April 2016. [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.