A Survey Paper On Cloud Computing Using Various Algorithm

Shefali ojha
M.Tech Scholar
Dept. of CSE LNCT Bhopal
sojha03@gmail.com

Vikram Rajpoot
Asst. Professor
Dept. of CSE LNCT Bhopal
rajputvikram022@gmail.com

***Abstract*— The Cloud computing is model that permits useful, on demand network access to mutual pool of configurable resources computing for example storage, servers, and networks, applications that may be rapidly released and provisioned using least managing exertion or service provider's interaction. Cloud Computing is disseminated design that centralizes server assets on a scalable stage so that provide on request services and computing resources.**

Keywords—cloud computing; services; models; security; MD5; AES; RSA ; DES.

I. INTRODUCTION

In the increasingly prevalent cloud computing, datacenters play a fundamental role as the major cloud infrastructure providers, such as Amazon, Google, and Microsoft Azure. Datacenters provide the utility computing service to software service providers who further provide the application service to end users through Internet. The later service has long been called "Software as a Service (SaaS)", and the former service has recently been called "Infrastructure as a Service (IaaS)", where the software service provider is also referred to as cloud service provider. To take advantage of computing and storage resources provided by cloud infrastructure providers, data owners outsource more and more data to the datacenters through cloud service providers, e.g., the online storage service provider, which are not fully trusted by data owners.

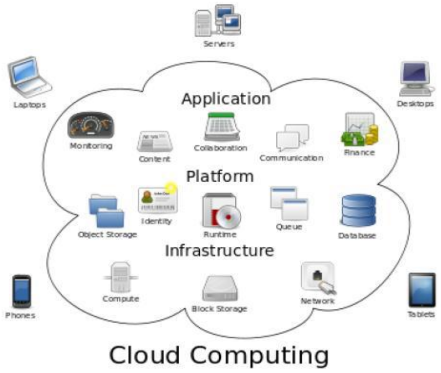

Fig. 1.1 cloud computing

As a general data structure to describe the relation between entities, the graph has been increasingly used to model complicated structures and schema less data, such as the personal social network (the social graph), the relational data base, For the protection of users' privacy, these sensitive data have to be encrypted before outsourcing to the cloud. Moreover, some data are supposed to be shared among trusted partners to all organizations. There have been publicized attacks on cloud computing providers and this paper discusses recommended steps to handle cloud security, issues to clarify before adopting cloud computing, the need for a governance strategy and good governance technology, cloud computing strengths, weaknesses, analyzes the benefits and cloud computing information security management. This paper has discussed some of the services being provided [1].

II. SERVICE PROVIDED BY VCLOUD COMPUTING

Service means different types of applications provided by different servers across the cloud. It is generally given as "as a service". Services in a cloud are of 3 types as given in [2]

A. *Software as a Service (SaaS)*

In SaaS, the user uses different software applications from different servers through the Internet. The user uses the software as it is without any change and do not need to make lots of changes or doesn't require integration to other systems. The provider does all the upgrades and patching while keeping the infrastructure running In SaaS model a software provider license a software application to be used and purchase on demand [3].

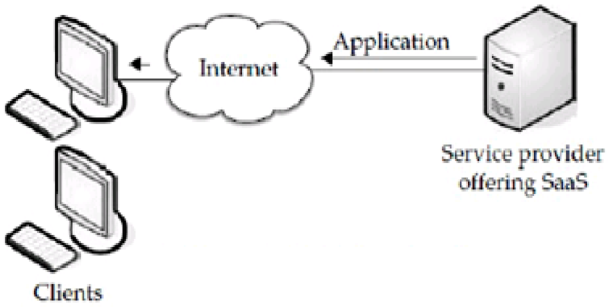

Fig.1.2 SaaS

B. Platform as a Service (PaaS)

PaaS provides all the resources that are required for building applications and services completely from the Internet, without downloading or installing a software. PaaS services are software design, development, testing, deployment, and hosting. Other services can be team collaboration, database integration, web service integration, data security, storage and versioning etc. A PaaS platform developer to write application those run on cloud [4].

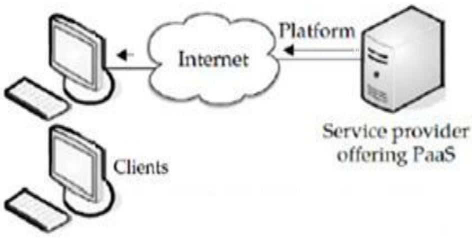

Fig.1.3 PaaS

C. Infrastructure as a service

Infrastructure as a service (IaaS) involve offering hardware related services using the principles of cloud hardware related services using the principles of cloud computing. IaaS provides a virtual-machine, virtual storage, disk image library, virtual infrastructure, raw block storage, and file or object storage, , load balancer, IP addresses, firewalls, virtual local area networks and software providers supply these resources on-demand from their large pools installed in data centers bundles. The IaaS service provider manages all the infrastructure. t offer a service to get a virtual server in few minute and pay only for the resource they use [5].

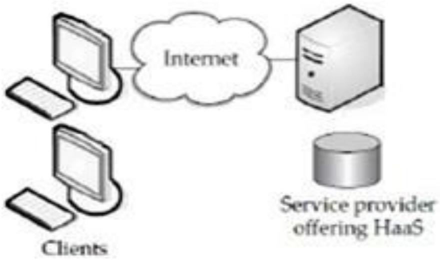

Fig. 1.4 IaaS

III. CLOUD DEPLOYEMNT MODELS

According to [6] there are four cloud deployment models regardless of the service model adopted (Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS)):

A. Public Cloud

This is also called external cloud sometimes and it basically involves an organization that sells readily available cloud services to the general public. Business organizations with sensitive corporate data are reluctant to adopt this model because it increases the threat of exposing confidential data to unauthorized access by third parties and potential cyber criminals. The advantage of using the public cloud is that an organization itself does not have to manage the cloud computing infrastructure nor maintain operational activities. The disadvantage of utilizing the services from a public cloud provider is that it is entirely dependent upon another business entity that is offering resources through public cloud .Public clouds are owned and managed by Providers, and applications from different customers are likely to be mixed together on the cloud's servers, storage systems, and networks. However, this model has a variety of inherent security risks that need to be considered. A well architected private cloud properly managed by a provider provides many of the benefits of a public cloud, but with increased control over security. Public clouds are most often hosted away from customer premises, and they provide a way to reduce customer risk and cost by providing a flexible, even temporary extension to enterprise infrastructure.

B. Private Cloud

Also referred to as internal cloud which means that cloud infrastructure and services are explicitly made available for a single organization. This deployment model can be located on premise or off site as it can also be managed by the organization itself or can be outsourced to a third party. Privately-hosted cloud services tend to be more costly but safer than other deployment models because organizations can retain control of their sensitive data and applications and implement their own security measures. The advantage for maintaining the private cloud is that an organization can retain full control of all the computing resources (e.g. applications, data, and systems) related to a cloud infrastructure. The disadvantage of such a deployment model is that an organization has to invest significantly in computing and storage resources and bear the cost of maintaining all software and computing platforms. Private clouds are client dedicated and are built for the exclusive use of one client, providing the utmost control over data, security, and quality of service. The enterprise owns the infrastructure and has control over how applications are deployed on it. If the private cloud is properly implemented and operated, it has reduced potential security concerns A managed private cloud may enable enterprise customers to more easily negotiate suitable contracts with the provider, instead of being forced to accept the generic contracts designed for the consumer mass market that are offered by some public cloud providers. Private clouds may be deployed in an enterprise datacenter, and they also may be deployed at a co-location facility.

C. Community Cloud

Organizations who share the same concerns and goals (e.g. security controls, privacy concerns, organizational mission, and regulatory compliance requirements) can join this deployment model to share the cloud infrastructure which could exist on-premise or off-premise as it could be managed by a third party as well. Community clouds are tailored to a specific vertical industry, such as government, healthcare or finance, offering a range of services [6], including infrastructure, software or platform as a service. It involves a private cloud that is shared by several organizations with similar security requirements and a need to store or process data of similar sensitivity. This model attempts to obtain most of the security benefits of a private cloud, and most of the economic benefits of a public cloud. An example community cloud is the sharing of a private cloud by several agencies of the same government.

D. Hybrid Cloud

This deployment model can span two or more other deployment models such as private, public, or community. In this model, data and applications are still standardized and enabled by a proprietary technology. The benefit of this model is that it offers a blend of cost effectiveness and scalability without exposing sensitive business data to external threats. This is possible because the hybrid model allows organizations to maintain their mission-critical applications in a private cloud (which provides security and control of in-house computing resource) and migrates their non-critical applications and platforms to the public cloud. Data availability, control, and performance are some of the disadvantages that can arise from adopting the hybrid cloud model. visual model defined by the National Institute of Standards and Technology (NIST) illustrating the three cloud service models and the A Hybrid cloud involves a combination of both public and private cloud models. They can help to provide on-demand, externally provisioned scale. The ability to augment a private cloud with the resources of a public cloud can be used to maintain service levels in the face of rapid workload fluctuations. Enterprise Computing and private cloud extend outward to consume public compute resource for peak need or deliver on Industry cloud. An example is using commodity resources from a public cloud such as web servers to display non-sensitive data [6], which interacts with sensitive data stored or processed in a private cloud. Focus primarily on proprietary data centers, but rely on public cloud resources to provide the computing and storage needed to protect against unexpected or infrequent increases in demand for computing resources.

IV. SECURITY ASPECTS TO FOCUS ON CLOUD COMPUTING

A. Availability

The goal of availability for Cloud Computing systems (including applications and its infrastructures) is to ensure its users can use them at any time, at any place. As its web-native nature, Cloud Computing system enables its users to access the system (e.g., applications, services) from anywhere. This is true for all the Cloud Computing systems.

B. Confidentiality

Confidentiality means keeping users' data secret in the Cloud systems. Cloud Computing system offerings (e.g.,applications and its infrastructures) are essentially public networks Therefore, keeping all confidential data of users'secret in the Cloud is a fundamental requirement which will attract even more users consequently. Traditionally, there secret in the Cloud is a fundamental requirement which will attract even more users consequently. Traditionally, there before placing it in a Cloud may be even more secure than unencrypted data in a local data center; this approach was successfully used by TC3.

C. Privacy

Privacy is an important issue for cloud computing, both in terms of legal compliance and user trust and this need to be considered at every phase of design. The key challenge for software engineers to design cloud services in such a way as to decrease privacy risk and to ensure legal compliance. The following tips are recommended for cloud system designers, architects, developers and Testers [3].

- Minimize personal information sent to and stored in the cloud.
- Protect personal information in the cloud.
- Maximize user control.
- Allow user choice.
- Specify and limit the purpose of data usage.
- Provide feedback.

D. Data Integrity

Data integrity in the Cloud system means to preserve information integrity (i.e., not lost or modified by unauthorized users). As data is the base for providing Cloud Computing services, such as Data as a Services, Software as a Service, Platform as a Service, keeping data integrity is a fundamental task [7]

V. DERIVATION OF MD5, AES,RSA AND DES

A. Rivest Shamir Algorithm

RSA is architectures by Leonard Adleman, Ron Rivest and Adi Shamir in 1978. This is 1 of best recognized crypto systems public key for key altercation or else signatures digital data encryption blocks. This uses 2 prime numbers to create private as well as public keys. RSA usages variable size key and a variable size encryption block. These 2 dissimilar keys are used for decryption and encryption purpose.

Sender encrypts the message using

1. Select2 distinct large random prime numbers p & q such that $p \neq q$. [S2]
2. Compute $n= p \times q$.
3. Calculate: phi (n) = (p-1) (q-1).
4. Select integer e such that 1<e<phi(n)
5. Calculated to satisfy congruence relation d × e = 1 mod phi (n); d is kept as key private exponent.
6. Private keys are (n, d) and public key is (n, e). Keep each values d, p, q as well as phi secret.

B. DES Algorithm

The DES is Cipher block which is architecture to decrypt and encrypt block of data involving of 64 bits through applying a

64-bit key. Although input key for DES is 64 bits long, actual key used with DES is 56 bits in length.DES is 1 of extensively recognized, available publicly cryptographic systems. This was established through IBM in 1970s but was later adopted through NIST, as FIPS PUB 46. Most important bit in all byte is equality bit, and must be set so that there are always a number odd of 1s in every byte.

- Preferred option, services3 mutually independent keys (K1 ≠ K2 ≠ K3 ≠ K1). This provides key space of 3 × 56 = 168 bits.
- Services 2 commonly independent keys as well as3 key that is same as 1stkey (K3 = K1and K1 ≠ K2). It provides key space of 2 × 56= 112 bits.
- Key bundle of 3 identical (K1 = K2 = K3) keys. It option is equal to DES Procedure.

The 3 times iteration is useful to growth average time and encryption level in DES. This is called fact that DES is slower than further block cipher approaches.

The flow of DES Encryption procedure. The algorithm processes with an initial permutation, sixteen rounds block cipher and a final permutation [8].

C. MD5 Algorithm

In August 1992, Ronald L. Rivest submitted a document to the IETF entitled, MD5 Message Digest Algorithm, which defines theory of it algorithm. For security and publicity of algorithm, this has been widely used to verify data integrity in a variety of program languages since 1990sMD5 was developed from MD, MD2, MD3 and MD4.

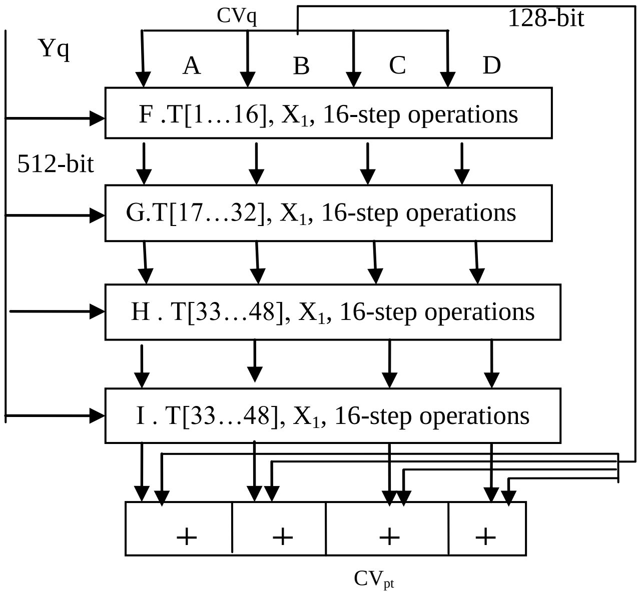
CVq
128-bit
Yq
A
B
C
D
F .T[1…16], X1, 16-step operations
512-bit
G.T[17…32], X1, 16-step operations
H . T[33…48], X1, 16-step operations
I . T[33…48], X1, 16-step operations
+
+
+
+
CVpt

Fig.1.5 The Processing logic

MD5 is an irreparable transformation transforming a collection of data of any length into a hash value of 128-bit length and this is a consecutive processing system. This 1st fills data to be processed and adds 64-bit binary digits to end of data representing bit length of original data before operation. The bit length of data which is existence processed becomes a multiple of 512 after filling,. Then data are distributed into groups of 512 bits and calculations are executed on all groups orderly. The input of 1stgroup operation is a 128-bit initial value; input of next group operation is a 128-bit output of previous group operation. The 4 rounds of processing have like structure but all of them has dissimilar logic function. The function used in every round is as follows. [3].

F(x,y,z) = (x & y) | ((~x) & z) (1)
G(x,y,z) = (x & z) | (y & (~z)) (2)
H(x,y,z) = x ^ y ^ z (3)
I(x,y,z) = y ^ (x | (~z)) (4)

D. AES Algorithm

AES procedure operates on a 128bit block of information and performed Nr - 1 loop times. Key length is 128, 256or192 bits in extent respectively. The 1stand last rounds diverge from further rounds in that there is additional Add Round Key transformation at start of 1stround as well as no Mix Coulmns transformation is executed in last round. We use key length of 128V bits as a model for general explanation in paper. An outline of AES encryption is given in Fig. 2.a)

Shift Rows Transformation:
Rows of state are cyclically left shifted over dissimilar offsets in Shift Rows transformation. Row 0 isn't shifted; row 1 is shifted 1 byte to left; row 2 is shifted 2 bytes to left and row 3 is shifted 3 bytes to left in Shift Rows transformation.

Mix Columns Transformation:
Columns of state are deliberated as polynomials over GF and multiplied by modulo x4 + 1 using a fixed polynomial c(x) in Mix Columns transformation, given by:
c(x)={03}x3 + {01}x2 + {01}x + {02}.

Add RoundKey Transformation:
Round Key is additional to State resulted from operation of Mix Columns transformation through a simple bitwise XOR operation in Add Round Key transformation. Round Key of all round is derived from primary key with Key Expansion procedure. The decryption/encryption algorithm essentials eleven 128-bit Round Key, which are denoted Round Key [9].

VI. LITERATURE SURVEY

SaskoRistov et al. presented that, Cloud computing providers‘ and customers‘ services are not only exposed to existing security risks, but, due to multi-tenancy, outsourcing the application and data, and virtualization, they are exposed to the emergent, as well. Therefore, both the cloud providers and customers must establish information security system and trustworthiness each other, as well as end users. In this paper we analyze main international and industrial standards targeting information security and their conformity with cloud computing security challenges. We evaluate that almost all main cloud service providers (CSPs) are ISO27001:2005 certified, at minimum. As a result, we propose an extension to the ISO 27001:2005 standard with new control objective about virtualization, to retain generic, regardless of company's type, size and nature, that is, to be applicable for cloud systems, as well, where virtualization is its baseline. We also define a quantitative metric and evaluate the importance factor of ISO 27001:2005 control objectives if customer services are hosted on-premise or in cloud [10].

Varun et al. presented that, The Cloud Computing offers service over internet with dynamically scalable resources. Cloud Computing services provides benefits to the users in terms of cost and ease of use. Cloud scaling large for data processing and storage needs. Cloud computing environment have various Computing services need to address the security during the communication of sensitive data and critical applications to shared and public cloud environments. The cloud environments are advantages as well as disadvantages on the data security of service consumers. This paper aim is to emphasize the main security issues existing in cloud computing environments. The security issues at various levels of cloud computing environment is identified in this paper and categorized based on cloud computing architecture. This paper also focuses on the usage of Cloud services and security issues to build these cross-domain Internet-connected collaborations. Among the many IT hulks driven by trends in cloud computing, it seems almost everyone has brought good news in this field of research [11].

Anjana Chaudhary et al. presented that, Cloud computing is becoming very popular computing paradigm for network applications. Cloud computing is basically an on-demand utility. Cloud computing provides different types of services and applications in the internet cloud. In cloud computing, Data Storage as a service (DaaS) allows users to store their data on remote servers and also have instant access to their data from any location using the internet connection. The data communication on the internet or over any networks is at risk to the attackers attack. So in order to secure the data some encryption scheme is used. In this project, we study the architecture of the cloud and also secure our network so that only authorized persons can access the data. For this, we propose a method for data storage and securing data in cloud computing environment by using the encryption method. In this report, we give the overview of data storage as well as security in cloud system. The main idea behind this report is to provide integrity to the cloud storage area. In order to provide security in cloud computing we use RSA algorithm. In this method some important security services including key generation, encryption and decryption are provided in Cloud Computing system. Here the TPA is the trusted entity that has expertise and capabilities to assess cloud storage security on behalf of a data owner upon request. The main goal is to securely store and manage the data so that only authorized users can have access over the data. Cloud computing is a model of information processing, storage, and delivery in which physical resources are provided to clients on demand. Instead of purchasing actual physical devices servers, storage, or any networking equipment, clients lease these resources from a cloud service provider as an outsourced service. It can also be defined as "management of resources, applications and information as services over the cloud (internet) on demand" [12]

Y. Ghebghoub et al. presented that, We propose to incorporate a frame work between the client and the cloud; sharing the network into three parts (client control framework, cloud).This layer controls user access through RBAC model that shares the users according to roles whose role is so abstract function in an organization and for each role are associated privileges which are a set of rights to duties can be achieved by each part. And thanks to the multi-level policy is associated to each role a level of security to provide Cloud Data Storage layer has two different network entities that can be identified as follows: cloud users which has data to be stored in the cloud and rely on the cloud for data computation. Cloud security platform has significant resources expertise in building and managing distributed cloud data storage servers, owns and operates live cloud computing systems.[13]

B. Rex Cyril1et al. presented that, Data security has a major issue in cloud computing environment; it becomes a serious problem due to the data which is stored diversely over the cloud. Data privacy and security are the two main aspects of user's concern in cloud information technology. Numerous techniques regarding these aspects are gaining attention over the cloud computing environments and are examined in both industries and academics. Data privacy and security protection are becoming the most significant aspects for the future enhancement and development of cloud computing technology in the field of business and government sectors. Thus, in this paper, the cloud computing security techniques are assessed and its challenges regarding data protection are discussed. The main aim of this proposed work is to enhance the data privacy and security for the reliable cloud environment. This comparative research investigation of the existing cloud security approach regarding the data privacy and security techniques utilized in the cloud computing. It will be useful to enhance the security of data storage in a cloud environment [14].

PradnyeshBhisikar et al. presented that, we investigated the problem of data security in cloud data storage and data transmission, which is essentially a distributed storage system. To ensure the correctness of users' data in cloud data storage, we proposed an effective and flexible distributed scheme. our scheme achieves the integration of storage correctness insurance and data error localization. In the data transmission proposed, method transferred data is encrypted in the upper-layer on top of the transport layer instead of using IPSec or SSL. Thus, the scheme for the performance improvement can be applied without modifying the implementation of IP layer, and efficient secure communications by pre-processing of encryption in the upper-layer are realized. We have used file uploading as service as web application, the security is applied over to the data at the background using the encryption algorithms like AES, Triple DES and DES. Through detailed security and performance analysis, we show that our scheme is highly efficient and resilient to Byzantine failure, malicious data modification attack, and even server colluding attacks [15].

VII. CONCLUSION

cloud computing is one of the most attractive area of research where lots of work done regarding in this field in our work we provide security using authentication and cryptographic technique in future we use secure operating system so that attacks are easily not depict in cloud computing.

References

[1] Pradeep Kumar Tiwari1, Dr. Bharat Mishra2 'Cloud Computing Security Issues, Challenges and Solution'International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 8, August 2012)

[2] Ronnie D. Caytiles1 and Sunguk Lee2* 'Security Considerations for Public Mobile Cloud Computing' International Journal of Advanced Science and Technology Vol. 44, July, 2012

[3] Yasir Ahmed Hamza1, Marwan Dahar Omar1 'Cloud Computing Security: Abuse and Nefarious Use of Cloud Computing' International Journal of Computational Engineering Research||Vol, 03||Issue, 6||

[4] Monjur Ahmed1 and Mohammad Ashraf Hossain2 'CLOUD COMPUTING AND SECURITY ISSUES IN THE CLOUD' International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014

[5] Prince Jain 'Security Issues and their Solution in Cloud Computing' International Journal of Computing & Business Research

[6] R. Sumithra1 & Sujni Paul 'A SURVEY PAPER ON CLOUD COMPUTING SECURITY AND OUTSOURCING DATA MINING IN CLOUD PLATFORM' International Journal of Knowledge Management & e-LearningVolume 3 • Number 1 • January-June 2011 • pp. 43-48

[7] Vahid Ashktorab2, Seyed Reza Taghizadeh1' 'Security Threats and Countermeasures in Cloud Computing'International Journal of Application or Innovation in Engineering & Management (IJAIEM) Volume 1, Issue 2, October 2012

[8] Gurpreet Singh and Supriya "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security" International Journal of Computer Applications (0975 – 8887) Volume 67– No.19, April 2013

[9] Ashwini R. Tonde, Akshay P. Dhande "REVIEW PAPER ON FPGA BASED IMPLEMENTATION OF ADVANCED ENCRYPTION STANDARD (AES) ALGORITHM" International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 1, January 2014.

[10] SaskoRistov, MarjanGusev and Magdalena Kostoska 'CLOUD COMPUTING SECURITY IN BUSINESSINFORMATION SYSTEMS' International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012

[11] Varun Gandhi1 '"CLOUD COMPUTING SECURITY ARCHITECTURE- IMPLEMENTING DES ALGORITHM IN CLOUD FOR DATA SECURITY" International Journal of Innovative Research in Engineering & Science ISSN 2319-5665(September 2013, issue 2 volume 9)

[12] Anjana Chaudhary1 Ravinderthakur and Manish Mann3 'A Review: Data Security Approach in Cloud computing by using RSA Algorithm'International Journal of Advance Research in Computer Science and Management Studies

[13] Y. Ghebghoub, S. Oukid, and O. Boussaid 'A Survey on Security Issues and the Existing Solutions in Cloud Computing' International Journal of Computer and Electrical Engineering, Vol. 5, No. 6, December 2013

[14] B. Rex Cyril1, DR. S. Britto Ramesh Kumar2'Cloud Computing Data Security Issues, Challenges, Architecture and Methods- A Survey' Cloud Computing Data Security Issues, Challenges, Architecture and Methods- A Survey

[15] PradnyeshBhisikar and Prof. AmitSahu ' 'Security in Data Storage and Transmission in Cloud Computing' International Journal of Advanced Research in Computer Science and Software Engineering