IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-7, Issue-9, Sept 2019 E-ISSN: 2347-2693

Privacy Preserving for Cloud Computing Using Cryptography in Big Data: A Review

Anjali Kumari[1*], Varsha Namdeo[2]

[1,2]Dept. of Computer science and Engineering, RKDF Institute of Science and Technology (RKDFIST), Bhopal, India

Corresponding Author: anjalikashyap533@gmail.com

DOI: https://doi.org/10.26438/ijcse/v7i9.219225 | Available online at: www.ijcseonline.org

Accepted: 08/Sept/2019, Published: 30/Sept/2019

***Abstract*-**Now a days Cloud computing services highly demanded in all over the world due to its large size spaces for data storing. Cloud Computing provides the ability to utilize resources through Internet. As a lot of service providers of the cloud are available in the competitive computer world. Security in Cloud computing is an important and critical aspect, and has numerous issues and problem related to it. In this paper we will survey of previous author's research that how they analyses approaches for secure data from the unauthorized users and provide integrity to the users. It requires a very high degree of privacy and authentication. To protect the data in cloud database server, cryptography is one of the important techniques for the security purposes. Cryptography provides various symmetric and asymmetric algorithms to secure the data.

Keyword: Big data, cloud computing, security, cryptography, AES etc**.**

I. INTRODUCTION

Cloud is a common representation for an Internet accessible organization which is hidden from users. Cloud Computing can be described in simple words as a combination of technology that provides hosting and storage services over the internet. Cloud can be classified into public, private or hybrid. With the increasing popularity of Cloud based system, the cloud operators have been targeting at its consistency, safety, privacy-preserving and cost-efficient cloud design. Requirements of Cloud applications vary based on the resources which are demanded as services. Thus, the resources may rise to heavy computation resources, large storage resources, and high volume network resources and so on. Cloud computing in other words is a standard term for conveying hosted work over the Net. It offers abundant benefits for the initiative, though; there are also a number of issues, as with any new technology. And one of the major concerns relates to the safety and privacy of client information in terms of its placement, accessibility and security. Cloud computing may also be referred as permitting a network of remote server hosted over the internet to store, manage and process data.

As a last paragraph of the introduction should provide organization of the paper/article (Rest of the paper is organized as follows, Section I contains the introduction of cloud computing and about privacy preserving, Section II contain the related work of various previous work as we observed the so many researcher do the study earlier and approached a secure and important algorithm also found a beneficial for cloud computing. As per we seen the various cryptography method which secure the cloud commuting securely from the hacker. So many problem and given earlier and fined, Section III contain the some measures of Possible security risk in cloud computing Section IV contain the some secure method of cryptography, section V explain the application of Cloud computing , Section VI conclusion and after this we provides all supporting references.

II. LITERATURE REVIEW

1. Privacy-Preserving Public Auditing for Regenerating-Code-Based Cloud Storage [1] In this paper author proposed two schemes first for auditing scheme and second for privacy preserving. It proposed public auditing scheme which allows the public verifier to audit the correctness of data even in which the data owner is offline. They proposed the data owner is able to generate those authenticators in a new method, which is more efficient compared to the straightforward approach.

2. Enabling Data Integrity Protection in Regenerating-Coding-Based Cloud Storage: Theory and Implementation [2] In this paper Henry C.H. Chen implement the DIP scheme which is designed under a mobile and enable client to feasibly verify the integrity of random subsets of outsourced data. It works under the simple assumption of thin-cloud storage and allows different parameters.

3. NC-Cloud: A Network-Coding-Based Storage System in a Cloud-of-Clouds[3] This paper author implement an

auditing framework for cloud storage systems and it propose an efficient and privacy-preserving auditing protocol, further extended auditing protocol to support the data operation. It also checks the correctness of the data operation. It implements batch auditing for both multiple owners and multiple clouds.

4. An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing [4] this paper the author is focus on an auditing framework for cloud storage systems and proposes an efficient and privacy-preserving auditing protocol, further extended auditing protocol to support the data dynamic operation. The further extend auditing protocol to support batch auditing for both multiple owners and multiple clouds, without using any trusted organizer.

5. Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing [6] in this paper author focus on combination the public key based homomorphic authenticator with random masking to achieve the privacy-preserving public cloud data auditing system. It supports efficient handling of multiple auditing tasks. They explorer TPA can perform multiple auditing tasks simultaneously.

6. Distributed data possession checking for securing multiple replicas in geographically dispersed clouds [6] In this paper author will help it provide a novel efficient Distributed Multiple Replicas Data Possession Checking (DMRDPC) scheme to tackle new challenges. It also will help the cloud users to achieve efficient multiple replicas data possession checking. It is important to ensure that each replica should have availability and data integrity features. In this paper Remote data possession checking is a valid method to verify the replica's availability and integrity.

7. Toward secure and dependable storage services in cloud computing [7] In this paper author proposed a flexible distributed storage integrity auditing mechanism, utilizing the homomorphism token and distributed erasure-coded data. It proposed design allows users to audit the cloud storage with very lightweight communication and computation cost. The proposed design further supports secure and efficient dynamic operations on outsourced data, including block modification, deletion, and append. It proposed scheme is highly efficient and resilient against malicious data modification attack, and even server colluding attacks.

8. Secure and efficient privacy preserving public auditing scheme for cloud storage [8] in this paper author propose a new privacy preserving public auditing mechanism for shared data in an untrusted cloud. Here, It utilize ring signature so that the third party auditor is able to verify the integrity of shared data for a group of users without retrieving the entire data while the identity of the signer on each block in shared data is kept private from the TPA. This paper provides a privacy preserving public auditing scheme that supports public auditing and identity privacy on shared data stored in the cloud storage service for enhancing its security and efficiency.

9. Network coding for distributed storage systems [9] In this paper author introduce a general technique to analyze storage architectures that combine any form of coding and replication, as well as presenting two new schemes for maintaining redundancy using erasure codes. It shows how network coding can help for such distributed storage scenarios.

10. A survey on network codes for distributed storage [10] In this paper author proposed the demand for large scale data storage has increased significantly, with applications. The peer-to peer networks, redundancy must be introduced into the system to improve reliability against node failures. It realizes the increased reliability of coding however, one has to address the challenge of maintaining an erasure encoded representation.

11. NC-Cloud: Applying network coding for the storage repair in a cloud-of-clouds [11] In this paper author proposed cloud storage provides an on-demand remote backup solution. To provide fault tolerance for cloud storage to proposed data across multiple cloud vendors. It preserves data redundancy. It implements a proof-of-concept prototype of NC-Cloud and deploys it atop both local and commercial clouds.

12. HAIL: A high-availability and integrity layer for cloud storage [12] In this paper author proposed HAIL a distributed cryptographic system that permits a set of servers to prove to a client that a stored file is intact and retrievable. HAIL cryptographically verifies and reactively reallocates file shares. It explores unification to remote file-integrity assurance in a system that calls HAIL (High-Availability and Integrity Layer).

13. Enhancing Security and Privacy in Multi Cloud Computing Environment [13] In this paper authors implement the cloud computing is a cost-effective, service availability, flexible and on demand service delivery platform for providing business through the internet. It is a form of secret sharing. The use of cloud computing for many purposes including because this service provide fast access the Applications and reduce service costs.

14. Security Approach for Multi-Cloud Data Storage [14] In this paper author proposed transformation of information and storage of sensitive data has highest priority. Cluster of cloud storage is created and maintained accordingly to satisfy the user specific data access requirements. It is

important to ensure that each replica should have availability and data integrity features.

15. A Privacy Manager for Cloud Computing [15]
In this paper author proposed it describes a privacy manager for cloud computing, It also describes how Trusted Computing mechanisms can optionally be used to enhance privacy management. The result of the processing is by the privacy manager to reveal the correct result.

Table 1: Existing solutions advantages and limitations to Cloud Computing [16]

Existing scheme	Advantages	Limitation
Client based Privacy manage	Preserve Privacy	Require honest cooperation of service provider
Anonymity based methods	Simple and Flexible	Limited for number of services
Fully Homomorphic encryption	Powerful tool	Fails to use practically
Preventing data leakage from Indexing	Prevent leakage by data indexing	Indexing based
Public Auditability and data Dynamics for Storage Security	Highly efficient and secure	Require third party auditor for operation.
Privacy Persevering Repository	Achieves the confidentiality and availability	Not secure enough to achieve all issues of security
Privacy Preserving System	Preserve the privacy	Providing machine readable access rights
Privacy-Preserved Access Control	Maintain the privacy of data without disclosing	Challenging because of data outsourcing and untrusted cloud server
Securing the storage Data Using RC5	Very easy to use and secure	Challenges of cracking the algorithm
Fog Computing	Protects against misuse of data	Not resolve all issues
Keeping data Private while Computing	Efficient for privacy preservation as well robust to network delay	only concentrates on NP problems
Security using Elliptic Curve Cryptography	Preserve the confidentiality and authentication	Fails to preserve all the security issues
Privacy Preserving Public Auditing for Storage Security	No leakage of data with better performance	Require some amount of improvement
Service oriented identity Authentication	Preserve privacy of the data.	Not support for multiservice and not practical concept

III. POSSIBLE SECURITY RISK IN CLOUD COMPUTING

Businesses and governments are shifting more and more workloads to the cloud. However, some organizations remain resistant to the cloud's considerable attractions due to lingering concerns about data security in cloud computing.
The main security risks of cloud computing are:

- Compliance violations
- Identity theft
- Malware infections and data breaches
- Diminished customer trust and potential revenue loss

While the concern is understandable, today's reality is that—when implemented correctly—cloud computing security is just as reliable as traditional on-premise IT.

How secure is cloud computing?
To fully understand cloud computing security, firstly we need to ask, what does cloud mean? By the usual cloud computing definition, cloud providers make IT resources and applications available as a metered service that users can consume through the internet.

Cloud services are typically classified into Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) such as raw computing power or cloud storage. A good cloud security provider will offer a scalable solution that detects threats before they reach the data center, helping to allay the following security concerns:

1. Loss of data
By its very nature, cloud computing involves some ceding of control from the customer to the service provider. While this leaves users more time and financial resources to focus on other facets of the business, there is always the risk that sensitive data is in somebody else's hands. If the security of a cloud service is breached, hackers could potentially gain access to intellectual property or other personal files.

2. Malware infections
Due to the high volume of data stored on the cloud, which requires an internet connection to store this data, anybody using cloud services is potentially at risk of cyber-attacks. An increasingly common threat is Distributed Denial of Service (DDoS) attacks, whereby hackers send unprecedented volumes of traffic to a web-based application, thereby crashing the servers.

3. Legal/compliance issues
With increasing legislation on data protection, from GDPR in Europe to HIPAA for healthcare, staying compliant is becoming more difficult. Companies must have steadfast rules governing who can access what data and what they can do with it. With cloud computing's easy access to data on a large scale; it can be difficult to keep track of who can access this information [17].
In next section we will give the

IV. CRYPTOGRAPHY METHOD

Various Available Algorithms/Techniques
The encryption algorithms play vital role and acting as necessary tool for data protection and secured network communication. The encryption algorithms convert the data

into jumbled form by using the "key" and the decryption can be done by the user only using the same key. [4] The following are the various algorithms available in cryptography:

1) DES- Data Encryption Standard: DES is an out-of-date symmetric-key method of data encryption. DES uses the same key to encrypt and decrypt a message; hence, the sender and the receiver both must have and use the same private key. DES has been superseded by more secure Advanced Encryption Standard (AES) algorithm, which was originally designed by researchers at IBM in the early 1970s. The U.S. government as an official Federal Information Processing Standard (FIPS) in 1977 adopted later on DES.

2) AES- Advanced Encryption Standard (AES): It is a symmetric-key encryption standard. It uses 10, 12, or 14 rounds. Each of the ciphers has a 128-bit block size, with the key sizes of 128, 192 and 256 bits, respectively. It ensures that the hash code is encrypted in a highly secure manner. Its algorithm steps are as follows:
a) Key Expansion
b) Initial round
c) Add Round Key
d) Rounds
e) Sub Bytes
f) Shift Rows
g) Mix Columns
h) Add Round Key
i) Final Round
j) Sub Bytes
k) Shift Rows
l) Add Round Key

3) RC2: This algorithm is a conventional (secret-key) block encryption algorithm, which can be considered as a proposal for a DES replacement. The input and output block sizes are 64 bits each wherein the key size is variable ranging from one byte up to 128 bytes, even though the current implementation uses eight bytes. The algorithm is designed for easy implementation on 16- bit microprocessors. On an IBM AT, the encryption runs about twice as fast as DES.

4) 3-DES – Triple DES or Triple DEA: In this Triple Data Encryption Algorithm, the DES Cipher being used with a symmetric-key block cipher, which is being applied to each block three times. The actual cipher's key size was 56-bits when DES algorithm was designed originally. In general, this was adequate as well, but the computational power availability made the brute-force attacks feasible by being increased. This issue was overcome by Triple DES, which provided a moderate-n-easy method in which the key size is being increased to safeguard such attacks. In addition, this overrides the necessity of designing a complete new block cipher algorithm.

5) SDES - simplified DES: Professor Edward Schaefer of Santa Clara University developed this simplified DES. The encryption algorithm uses input as an 8-bit block of plaintext and a 10-bit key. The output would be an 8-bit block of ciphertext. The decryption algorithm uses an input of 8-bit block of ciphertext produced in encryption process and the same 10-bit key used in ciphertext production, wherein the output would be the original 8-bit block of plaintext.

6) RC5 – Rivest Cipher or Ron's Code RC5 is a symmetric-key block cipher distinguished by its simplicity. Ronald Rivest designed this during 1994. In RC5 both the encryption and decryption expand the random key into 2 (r+1) words that will be used in sequence. These will be used only once each during the encryption and decryption processes. RC5 will be using a variable block size of 32/64/128 bits, key size of 0-2040 bits and number of rounds would be 0-255, wherein the parameters proposed in original was 64 bits of block size. A key feature of RC5 is the use of data-dependent rotations; one of the objectives of RC5 was to swift the study and evaluation of such operations as a cryptographic primitive/with citation. RC5 also comprises of a number of modular additions and eXclusive OR (XOR) s.

7) RC6 - Rivest cipher 6: Ron Rivest, Matt Robshaw, Ray Sidney, and Yigum Lisa Yin designed RC6, which is a symmetric key block cipher. This was designed to meet the necessity of AES competition & derived from RC5. It has 128-bits of block size and supports 128,192 and 256 bits of key sizes up to 2040-bits. But it may be parameterized like RC5 to support a wide variety of word-lengths, key sizes, and number of rounds. RC6 and RC5 are similar in structure. Both would be using data-dependent rotations, modular addition, and XOR operations. In reality, RC6 could be viewed as interlacing two parallel RC5 encryption processes, although RC6 does use an extra multiplication operation, which is not present in RC5. This is to make the rotation dependent on every bit in a word, and not just the least significant few bits.

8) SSL Encryption – Secure Socket Layer: SSL is the standard security technology for launching an encrypted/encoded link between a web server and a browser to make sure that all data distributed between the web server and browsers persist private and integral. In SSL communications, the server's SSL Certificate comprises a pair of asymmetric public and private keys. The session key created during the server and the browser SSL Handshake is symmetric. The below given diagram illustrates this process:

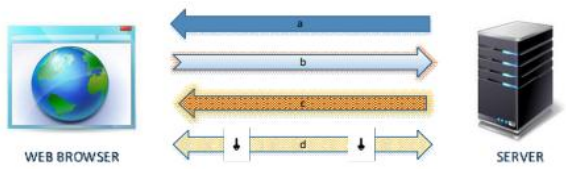

Figure 1: Secure Socket Layer

a) Server sends a copy of its asymmetric public key.
b) Browser creates a symmetric session key and encrypts it with the server's asymmetric public key.
Then sends it to the server
c) Server decrypts the encrypted session key using its asymmetric private key to get the symmetric session key.
d) Server and Browser now encrypt and decrypt all transmitted data with the symmetric session key. This process makes a secure channel as only the browser and server know the symmetric session key. In addition, the session key is only used for that particular session. If the browser connects to the same server after that, a brand new session would be created.

9) GEO Encryption: Geo-encryption is another type of encryption. The objective of this is to limit the data decryption to a specific location/time/position of the receiver. In this, the traditional encryption is enhanced, which uses any physical location or time to have additional security and its features. In addition, this does not replace any of the conventional algorithms, wherein an extra layer of security is added. The decryption/access of information is restricted to specified locations and/or times. The standard encryption algorithms like AES, 3DES, RSA etc. are used in building this Geo-encryption algorithm provided that the encryption key "geo-locked" is added on top of them using location/time/position of the anticipated recipient. The location based encryption ensures that the decryption cannot be done outside a particular facility/location; otherwise, this will result in decryption failure.

10) HABE (Hierarchical Attribute Based Encryption): A user can delegate the private key corresponding to any subset of an attribute set while he has the private key corresponding to the attribute set. Moreover, the size of the ciphertext is constant, but the size of private key is linear with the order of the attribute set in the hierarchical attribute-based encryption scheme.

11) Key-policy Attribute-Based Encryption (KP-ABE): The first KP-ABE construction was delivered by Goyal et al., The system was verified selectively secure under the Bilinear Diffie-Hellman assumption. KP-ABE schemes are suitable for structured organizations, wherein they are with rules, which deal with particular documents reading. Secure forensic analysis and target broadcast are typical applications of KP-ABE, wherein the cipher texts sent by sender labeled with a set of descriptive attributes. The user's private key is specified by a trusted attribute authority policy by which the decryption of cipher texts is defined.

12) CP-ABE (Cipher text Policy Attribute Based Encryption): This CP-ABE algorithm comprises of Setup, Encrypt, Key-Gen, and Decrypt processes. The inputs for this process would be a security parameter and attribute universe description wherein the PK-public parameters and MK-master key will be the output. In CP-ABE scheme, the user's private key/decryption key will be linked/tied to a set of attributes that will signify the concerned user's permissions. When a ciphertext is encrypted, a set of attributes is designated for the encryption, and only users tied to the relevant attributes are able to decrypt the cipher text.

13) Blowfish: Blowfish is a symmetric-key block cipher, designed in 1993 by Bruce Schneier. This is being used in a huge number of cipher suites and encryption products. Blowfish provides a good encryption rate in software. At the same time till date no effective cryptanalysis of it has been identified. Nevertheless, the Advanced Encryption Standard (AES) now gets more attention. The DES or IDEA can use blowfish as drop-in replacement wherein it takes 32-448 bits of a variable-length key for both domestic and exportable uses. This process uses large key-dependent S-boxes and a 16-round Feistel cipher, which resembles CAST-128 in structure where fixed S-boxes are used.

14) MA-ABE Multi-Authority Attribute-Based Encryption: A multi-authority ABE system comprises of any number attribute authorities and users as well. In the systems a set of global public parameters are defined [19]. A user can select an attribute authority and attain the equivalent decryption keys. The authority executes the corresponding attribute key generation algorithm and the result is reverted to the user. Global public parameters used in the encryption process and the cipher text is produced based an attribute set. In the same way, the decryption is also set using attribute set. [19]

15) RSA: RSA algorithm is used for public-key cryptography and it is an asymmetric algorithm being the first and still most commonly used. It involves two types of keys – public and private keys. The public key is known to all and used for encrypting messages. The encrypted message with a public key can be decrypted only by using private key.

16) MD5- (Message-Digest Algorithm-5): Cryptographic hash function algorithm which is a widely used one with a 128-bit hash value and processes a variable length message into a fixed-length output of 128 bits. In this, the input message is broken up into chunks of 512-bit blocks then the message is padded so that its total length is divisible by 512. Also, the sender of the data use the public key to encrypt the message and the receiver uses its private key to decrypt the message.

17) Digital Signature: Public key algorithms used in Cryptographic digital signatures for delivering data integrity. In this authentication scheme, public key authentication is implemented in the server by signing a unique message using a private key, thus creating is called as a digital

signature. Then the signature is returned to the client and later it is verified using the server's known public key.

V. APPLICATION OF CLOUD COMPUTING

Cloud Computing can run every programs and software as a normal computer can run. It can also provide us with numerous applications which are free of cost. So, let's start elaborating these Cloud Computing applications one by one [19]:

i. Storing File Online

Cloud Computing provides a benefit to store and access the software with the help of internet connection to the Cloud. The interface provided is very easy to operate and is economical too.

ii. Video Making and Editing Software

There is much software available which can access with the help of the cloud. This software helps to create and modify the videos. The videos create or modify are stored in the cloud itself and we can access anytime.

iii. File Converters

There are many applications which utilize to change to format of the file such that from HTML to PDF and so on. This software is available at cloud and access from anywhere with the help of internet connection.

iv. Anti-Virus Applications

There is software which is stored in the cloud and from there they fix the system. All the viruses and the malware are detected and analyzed by the software and the system is fixed. They also come up with a feature of downloading the software.

v. E-commerce Application

With the help of e-commerce application in the cloud, user and e-business allow responding quickly to the opportunities which are emerging. It also allows the user to respond quickly to the market opportunities and the challenges. Business tycoons focused on the usage of cloud computing without keeping time in the mind. Cloud-based e-commerce applications allow the companies, business leaders to evaluate new opportunities and making things done with the minimum amount possible.

vi. Business Process

Business management applications are based on the cloud service provider. The business utilizes the cloud computing to store the necessary data and all the relevant information. This information can be anything such as the personal data of the customer, analyzed records, and many more.

vii. Backup and Recovery

The cloud computing can be used as a backup option in which we can store the files, information, and the data. This data is stored will be protected and provided much security. When the data is lost the user can recover the data which he/she has stored in the cloud.

VI. CONCLUSION

Cloud computing is a promising and emerging technology for the next generation of IT applications. The barrier and hurdles toward the rapid growth of cloud computing are data security and privacy issues. Reducing data storage and processing cost is a mandatory requirement of any organization, while analysis of data and information is always the most important tasks in all the organizations for decision making. So no organizations will transfer their data or information to the cloud until the trust is built between the cloud service providers and consumers. A number of techniques have been proposed by researchers for data protection and to attain highest level of data security in the cloud. However, there are still many gaps to be filled by making these techniques more effective. More work is required in the area of cloud computing to make it acceptable by the cloud service consumers. This paper surveyed different techniques about data security and privacy, focusing on the data storage and use in the cloud, for data protection in the cloud computing environments to build trust between cloud service providers and consumers.

REFERENCES

[1] Jian Liu, Kun Huang, Hong Rong, Huimei Wang, and Ming Xian, "Privacy Preserving Public Auditing for Regenerating-Code-Based Cloud Storage", 2015.

[2] Henry C.H. Chen and Patrick P.C. Lee, "Enabling Data Integrity Protection in Regenerating-Coding-Based Cloud Storage: Theory and Implementation", 2014.

[3] Henry C.H. Chen, Yuchong Hu, Patrick P.C. Lee, and Yang Tang, "NCCloud: A Network-Coding-Based Storage System in a Cloud-of-Clouds", 2014.

[4] Kan Yang, Xiaohua Jia, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing", 2013.

[5] Yan Zhu, Hongxin Hu, Gail-Joon Ahn, and Mengyang Yu, "Cooperative Provable Data Possession for Integrity Verification in Multicloud Storage", 2012.

[6] Cong Wang, Qian Wang, and Kui Ren, Wenjing Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing", 2010.

[7] J.He, Y. Zhang, G. Huang, Y. Shi, and J. Cao, "Distributed data possession checking for securing multiple replicas in geographically dispersed clouds," J. Comput. Syst. Sci., vol. 78, no. 5, pp. 1345–1358, 2012.

[8] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward secure and dependable storage services in cloud computing," Apr.Jun. 2012.

[9] S. G. Worku, C. Xu, J. Zhao, and X. He, "Secure and efficient privacy preserving public auditing scheme for cloud storage", 2013.

[10] A. G. Dimakis, P. B. Godfrey, Y. Wu, M. J. Wainwright, and K. Ramchandran, "Network coding for distributed storage systems," Sep. 2010.

[11] Y. Zhu, H. Hu, G.-J. Ahn, and M. Yu, "Cooperative provable data possession for integrity verification in multicloud storage," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 12, pp. 2231–2244, Dec. 2012.
[12] A. G. Dimakis, K. Ramchandran, Y. Wu, and C. Suh, "A survey on network codes for distributed storage," Proc. IEEE, vol. 99, no. 3, pp. 476–489, Mar. 2011 .
[13] H. Shacham and B. Waters, "Compact proofs of retrievability," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2008, pp. 90–107.
[14] Y. Hu, H. C. H. Chen, P. P. C. Lee, and Y. Tang, "NCCloud: Applying network coding for the storage repair in a cloudof-clouds," in Proc. USENIX FAST, 2012, p. 21.
[15] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacypreserving public auditing for data storage security in cloud computing," in Proc. IEEE INFOCOM, Mar. 2010, pp. 1–9.
[16] Mahesh U. Shankarwar and Ambika V. Pawar "Security and Privacy in Cloud Computing: A Survey"CSE Department, SIT, Symbiosis International University, Pune, India 30 January 2016.
[17]https://www.akamai.com/us/en/resources/data-security-in-cloud computing.jsp?gclid=Cj0KCQjwgezoBRDNARIsAGzEfe6UcdRWLjMBG0wtc0jx1ORor0J-O9N80kNtAyihFePqk_fTPkyMcREaAjCXEALw_wcB&ef_id=Cj0KCQjwgezoBRDNARIsAGzEfe6UcdRWLjMBG0wtc0jx1ORor0J-O9N80kNtAyihFePqk_fTPkyMcREaAjCXEALw_wcB:G:s&utm_source=google&utm_medium=cpc
[18] Kishore Kumar"Role of Cryptography & its Related Techniques in Cloud Computing Security" International Journal for Research in Applied Science & Engineering Technology (IJRASET) ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887 Volume 5 Issue VIII, August 2017- Available at www.ijraset.com
[19]https://data-flair.training/blogs/cloud-computing-applications/

