International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 4 Issue: 2
ISSN: 2454-4248
319 – 325

Secure Image Sharing on Cloud using Cryptographic Algorithms: Survey

Jaspreet Kaur[1], Er. Sumit Sharma[2]
M. Tech (Scholar), Assistant Professor
Department of Computer Science& Engineering
Chandigarh University
Email:jaspreetkaurpaul@gmail.com, cu.sumitsharma@gmail.com

Abstract: Mobile devices are making major changes in the world. Nowadays, every person has a mobile and they capture every moment in their life in mobile in the form of images and videos. These devices produce alarge amount of data. Cloud computing (CC) providers are basic storage where a person can store their data and share with other persons. They share those images and videos on an unsecured channel which are vulnerable to attacks. For stopping unauthorized access we have to encrypt our data before storing in the cloud. Security is the main concern while storing and sharing data in the cloud. Cryptography is the best way for encryption. In this, we review different encryption algorithms forencrypting the images and secure image sharing on the cloud using cryptography. This review provides the basic concept of CC and security while sharing data on the cloud.

Keywords: *Cloud computing, security, Encryption algorithms, secure image sharing.*

*****

I. INTRODUCTION

Mobile devices are becoming very popular nowadays and data is produced by these devices are also in huge amount. Such large amount of the statistics is pushing ahead the idea of storage of facts outsourcing. Cloud is now not it only a platform for the economical simple storage & computing energy but it becoming an important hub and responsible for widespread and rapid data analytics/processing, on-call for records dissemination (DD) and big new records era[3].

Cloud provides the various benefits to the user because it enables the capabilities of data sharing over the network. Todays, IT organizations and other enterprises use the cloud for storage and sharing a purpose. Cloud provides the storage space according to their and business needs. Cloud is also used in the medical field because huge data and images of patient's tests are produced on the daily basis. To handle that large data cloud provides that benefits in the medical field. They share images such as selfies, buildings, dishes, landmark etc. The user can upload & download images and other data to/from the cloud. They can access that data by mobile phones or PC's from any part of the world at any time.

Security is the main concern while storing and sharing data in the cloud. Every user wants their data should be secure so that no unauthorized person can access their data. For that reason, cryptography techniques are used to encrypt user data and prevent any attacks or unauthorized access. Cryptography converts the original data into ciphertext which is an unreadable form (Encryption) and again converts the ciphertext into original form (Decryption) [5].

Cryptography used three types of algorithms for providing security to data.

- Hash functions (HF): HF uses some mathematical transformations to encrypt the user data. HF uses a hash value instead of any key. HF is used to check the integrity of our message. It ensures that message which is shared with other client isn't altered or infected with the virus.
- Symmetric key algorithms (SKA): SKA makes use of the similar key for encryption & decoding purpose. This secret key is known to the holder of the records and the legal person of the data [5].Various SKA algorithms are used for security such as AES (Advanced encryption standard), Data encryption standard (DES), triple DES (3DES), and Ron's Code etc.
- Asymmetric key algorithms (AKA): AKA makes use distinctive keys for encryption and decoding purpose. The encryption key is known as an open key which is known to everybody. Another key is the private key which is utilized to decode the data is only known to the user of the data at the receiver side[5]. Various AKA algorithms are used for the security purpose such as EC (Elliptic Curve), DSA (Digital Signature Algorithm), DH (Diffie-Hillman) key exchange, RSA (Rivest, Shamir &Adleman) algorithms etc.

II. CLOUD COMPUTING

Cloud computing is a vast network of various frameworks which can be related in public or private systems. Cloud computing (CC) gives the adaptable foundation to the information, record and application stockpiling over the

 ISSN: 2454-4248
319 – 325

system. CC enhances multiple users to simultaneously contribute and access the projects without any concern about using the same OS, browser, or software due to the fact that the clients data is stored inside the cloud rather than on their computer systems. NIST is 'National Institute of Standards and Technology'.CC haven't any international accepted definition, but NISTdefine CC as "a model for enaing ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [2]."

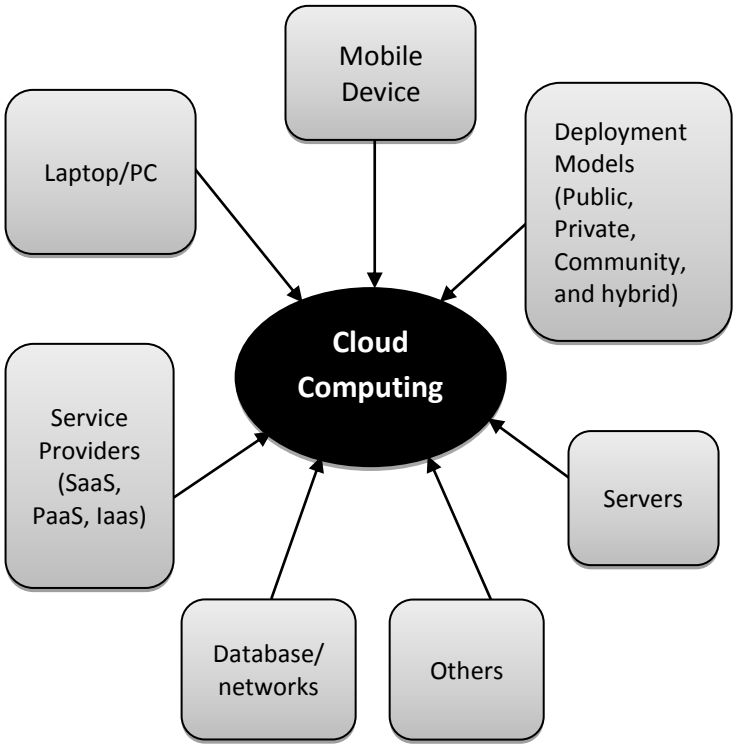

Fig 1: Cloud Computing Architecture

Cloud computing is based on two types of models such as service and deployment models. Service models are classified as IaaS, PaaS, SaaS. In this type of models, all the services are presented to different users by the cloud providers [3].

- SaaS (Software as a service): In SaaS model whole software or application is offered to the user when he demands service. In this model single instance of the service is runs on the network and multiple users are serviced together. Today SaaS is offered by different companies such as Microsoft, Google, Salesforce, Zoho, etc.
- PaaS (Platform as a Service): In PaaS provider can only offer to the user development environment or a single layer of the software as a service. The user can build his own interest software or service with a higher level which runs on the providers providing the platform. The main requirement of any application is manageability and scalability, and to meet these requirements providers of PaaS offered a combination of application servers and OS which is predefined. Like LAMP platform (Php, Linux, MySQL,and Apache), Ruby etc. Some of the most popular examples are Force.com, Window Azure, Google's App Engine etc.
- IaaS (Infrastructure as a Service): In IaaS model service providers offered basic storage or computing capabilities as services to different clients. In IaaS data center space, storage, networking equipment's are collected and made available over the internet to handle the workload. The user can develop his own software and run on the cloud infrastructure, they also store their applications or data in a cloud environment. Examples of IaaS are Amazon, cloud renders farms, GoGrid, Window server, 3 Tera, etc.

2.1 Deployment models

In deployment models, adifferent type of cloud is providing to users according to their requirements. It provides cloud space to different subscribers according to their needs [4].

- **Public Cloud** – As from the name public cloud a cloud space which is accessible by any subscriber which has internet connectivity. This open cloud is made accessible to any well-known public or any gathering or association, and furthermore claimed by any association for offering cloud services. Illustrations: Amazon ECC (Elastic-Compute-Cloud), IBM's BC (Blue Cloud), Sun Cloud, Google AE (App Engine).
- **Private Cloud** – A private cloud is only accessed by some specific set of persons or any particular organization who have limited access to use any service. In cloud computing private cloud is provided a limited and secure space where the particular group can operate or we can say that resources which are provided by the private cloud are only accessible by one organization.
- **Community Cloud** – When two or more groups/organizations have the same set of requirements for cloud space and services then community cloud is shared with them. Google's "Gov Cloud" is an example of community cloud.
- **Hybrid Cloud** – When within the same organization two different clouds are used as a combination, then in that organization hybrid cloud is established. This is a blend of at least two clouds (public, private, or community). In a hybridcloud, two different clouds are used together and allowed to replicate the local data in the public cloud.

 ISSN: 2454-4248
319 – 325

2.2 Advantages/ disadvantages of cloud

Cloud computing has many advantages like:

- cost efficiency,
- Unlimited stockpiling,
- Backup and recuperation,
- Centralization to user data,
- Automated Software Integration,
- Smooth get entry to data,
- Quick Deployment,

2.3 Applications of cloud

Applications of cloud computing: Cloud computing is used in various fields from small to large business.

- ✓ BCM (Business contact management)
- ✓ Google Docs and Google App
- ✓ OP (Office productivity) like Office 365 and MS Office
- ✓ BAS (Business Accounting Systems) like Peachtree and QuickBooks
- ✓ OSM (Online Storage management)
- ✓ Medical imaging and patient urgent care
- ✓ Line of business applications
- ✓ Communications and collaborations application
- ✓ Email & Instant Messaging Applications
- ✓ CRM (Customer relationship management) like SalesForce.

III. LITERATURE REVIEW:

Over the years to keep the message or image/video secret diverse varieties of techniques had been advanced to encrypt and decrypt that image or message. Cryptography is the approach for providing security to communication between users and keeps their data secure.

H. Cui et al [6] proposed a secure and mobile-friendly design for mobile clients. In this paper, theauthor uses two encryption mechanisms such as AES and SHA to provide the high security. This design ensures that mobile client can save transmission cost, bandwidth, and energy consumption while uses different assets in the cloud. This secure design allows the users to securely find the data from encrypted datasets with less time. In this paper five parameters are calculated such as index building time, candidate selection time, saving bandwidth, image reproduction, and saving energy. Author's main focus is only on the security guarantees of candidate selection time.

J. Wu et al [7] suggest novel data assisted image transmission framework DAC-Mobi. DAC-Mobi is named as data-assisted communication of mobile image and based on analog visual communication (AVC). Authorsalso discover the two techniques to improve the SE (spectrum efficiency) of data and VQ (visual quality) of image. 1st

- Simpler scale of offerings,
- Deliver new administrations and so forth.

Besides many advantages, it also has some disadvantages such as

- Security breaches,
- Possible downtime,
- Inflexibility,
- Lack of support,
- No internet no cloud etc.

technique is Coset coding which is two layered and 2nd one is internal & external denoising.

Vartiainen et al [8] present a service for Image Exchange (IEx). That service is a photo sharing IS (Internet service) that was composed from the CC viewpoint. The author describes IEx thru two different user researches. Results of this paper describe essential implications for CC on cell phones. Users can utilize their photographs to interact with other clients in real-time on cloud environment and additionally receive up-to-date facts.

Y. Wu et al [9] present in their paper secure method for image sharing and hiding secret images. Their approach is based on steganography. In their proposed method each image is shared in thecloudin a secure way. Numbers of shadow images are generated from the original image. Each shadow image is called as stego image. For providing security so that no hacker can access user's secret images. For that every stego image is covered up in the ordinary or common photograph. If there are n stego /shadow images then any t images of them may be utilized to reconstruct the original picture. Size of stego image is 1/t. For eg, if there are 6 shadow images then any 4 photographs can be utilized to recreate the original picture.

Hashing is the popular method used for retrieval the content from the web or cloud. But various traditional hash methods are not achieved recall and high precision with multiple shots. It only learns the binary code in a single shot and using only single hashing table. To achieve the high precision P. Li, J. Cheng and H. Lu [10] proposed a DCH (Dual complementary hashing) method. This method helps to learn the binary code for the image description with multiple hashing tables. DCH helps in nearest neighbor search with similar data on web/cloud.

Encryption and decode procedure can creates overhead on the system. To overcome this problem Q. Liu et al[11] proposed ElGamal symmetric key encryption which is based on ECC (Elliptic Curve Cryptography).This method is a secure method and privacy-preserving method for storage on the cloud. This approach is based on keyword searching scheme. A cloud service provider (CSP) plays a very important role in cloud computing. CSP of Cloud provides different services to various users. According to the authors,

 ISSN: 2454-4248
319 – 325

their proposed method allows the CSP to contribute in the decryption process of cipher data. Results of this method show that the overhead of decipherment can be overcome by reducing the communication & computational cost.

Encrypted data is retrieved from the cloud using SSE (Searchable symmetric encryption), but there is some data privacy issue of using SSE. To support ranked keyword search in anefficient way, J. Yu et al [12] present an approach named as Two-Round Searchable Encryption (TRSE). This approach is based on the ranking of data and also supports the top-k multi-keyword recovery of data. This TRSE method utilized a model of vector space (VS) and homomorphic encryption (HE) scheme. VS help in achieving an accuracy of data search on cloud and in ranking process involvement of users can be enabled by HE. In the approach, two round communication procedures are used for retrieval of data from the server. Proposed method reduced the data leakage and additionally ensures the data security.

When data is stored in cloud then it can be stored on multiple or third-party servers and that storage is not cared by the user they don't know where exactly their data is stored. CSP is responsible for the storage but they do not provide full security and privacy to our data. ArjunKumar et al [13] proposed a method in his paper, which allow users to access and store their data securely from the CS. They use ECC algorithm for encryption and decryption process and protect data files. This method guarantees that user data can't access by unauthorized users and the CSP.

Security threats in cloud computing while storing and sharing data are addressed by the N. Tirthani, G.R [14]. They proposed a design for cloud architecture and this also ensure the secured transmission of user's information from sender to receiver sides. In this research paper, two encryption mechanisms are used one is ECC and DH key exchange for connection establishment between clients. With these two algorithms, authors provide four step practices which can ensure the authenticity of the client. Three security checkpoints have also used such as authentication, encryption of data, and key generation. Proposed design provides better security to data while storing and sharing, and reliability to data in the cloud for maintaining the integrity of data.

N. Gajra et al [15] proposed a hybrid mechanism for providing security guarantee while storing data in the cloud. For hybrid mechanism, they used Blowfish and AES algorithms for data encryption process. For generating key they used ECC (Elliptic curve Cryptography) and Diffie-Hellman for key agreement. Authors use both of these algorithms and proposed a new approach as ECDH key exchange. ECDH is Elliptic curve Diffie-Hellman. Authors used ECDS (Elliptic Curve Digital Signature) for authentication. Their proposed method provides the security protection for data which is outsourced to the cloud.

B. Acharya et al [16] implemented in his paper amodified Hill cipher (MHC) approach. This approach and 'key image' both are used for encrypt the user images. At that time utilize the similar key image to decode the encrypted images to acquire those images which contain real data. Hill cipher is a polygraph substitution cipher and non-public cryptosystem. This algorithm is depends on matrix multiplication. This technique has numerous advantages in encryption while decoding requires in this inverse of the key matrix. Due to various disadvantages of Hill Cipher author's used MHC approach for providing security to user images with the goal that images ends up secure for any assault.

Sandeep K. Sood [17] proposed a framework which comprising of various methods and specialized procedures that could be efficient help in protecting the data from start to end means sender to receiver. The author classifies the data on basis of three cryptographic parameters confidentiality, availability, and integrity. Encryption is performed using 128-bit Secure Socket Layer (SSL), for check integrity and data division Message Authentication Code (MAC) is used.

IV. ENCRYPTION ALGORITHMS

Security is the main concern while storing and sharing data in the cloud. Cryptography is the best way for encryption. The generation, modification, and transportation (GMT) of every algorithm keyhave been done by the different encryption algorithms. These encryption algorithms are part of cryptography. To encrypt the data various cryptographic algorithms are available. The quality of any encryption algorithm closely depends upon the computer device utilized for the generation of key. Some popular algorithms to encrypt the data are discussed here:

- *AES (Advanced Encryption Standard)*

SKA makes use of the similar key for encryption & decoding purpose AES Algorithm is an SKA algorithm. This algorithm [18] [19] uses one key for encryption and decoding purpose by the sender and the receiver. Block size of data is 128 bits which are fixed, but it can be 128, 192, and 256. This data block is divided into 16 bytes. These 16 bytes are represented by a 4 x 4 array. This 4 x 4 array is known as the State. All the inner operations of the AES are performed on these States. Further, this algorithm is an iterative algorithm and every iteration is known as a round. The overall range of rounds is 10 for 128, 12 for 192, and 14 for 256-bit.

- *DES (Data Encryption Standard)*

DES [18] is openly accessible and widely accepted cryptographic systems. This system was evolved by IBM in the 1970s yet was later received by the NIST. DES is a

 ISSN: 2454-4248
319 – 325

block Cipher Algorithm that is created to encode and decode the blocks of data consisting of 64 bits. It uses the 64-bit key for that process. Basically, DES's Input key is 64 bits long, however, the real length is 56 bit. DES goes through the 16 iterations for converting plain text into cipher text. DES converts the 64-bit input into 64-bit output in series of steps. At the receiverside, for decrypt, the data same steps are followed and decryption is performed by the similar key.

- *3DES (Triple Data Encryption Algorithm)*

DES algorithm has some flaws and 3DES [19] was developed to address those flaws without creating the entire cryptosystem new. DES utilizes a 56-bit key and that key is not enough to encrypt the users or organizations sensitive data. The 3DES algorithm uses a 3 key with EDE (Encrypt-Decrypt-Encrypt) mode. 3DES extend the key length by using the algorithm 3 times and the key size of the 3DES algorithm is 168 bit long, which is 3 time of 56. It uses a three 64 bit keys K1, K2, K3. The K1 key is used forencryptingthe records, K2 key is utilized to decrypt the records and the K3 key is for again encrypt the records.

- *RSA (Rivest-Shamir-Adleman)*

RSA algorithm is one of the best Asymmetric cryptosystems for encryption of blocks of data or digital signatures or key exchange [18] [19]. This algorithm uses a variable size key and encryption block. It is based on number theory and utilization of two prime numbers to produce the public and non-public keys. These public and non-public keys are utilized for encrypting & decrypting the data. RSA processes are divided into 3 main steps.1st is a key generation, 2nd is for data encryption & 3rd for decryption. But this algorithm has many flaws in its design that's why it isn't preferred for business use. While designing a key if small values are chosen for RSA then it makes encryption process very weak and if takes too large values then it consumes time and also affected the performance. With small values of a key generation, anyone can easily decrypt the encrypted data by using the side channel attacks or random probability theory.

V. COMPARISON OF DIFFERENT ENCRYPTION ALGORITHMS

In the below-giventable, comparative study of encryption algorithm is presented. Encryption algorithms are AES, DES, 3DES, RSA [19] [20] are presented into fourteen factors, which are Algorithm type, Encryption, Decryption, Key length, Block size, No. of rounds, key used, Key for Ciphering and deciphering, Algorithm for Ciphering and deciphering, Algorithm scalability, Security, Vulnerability, Speed of simulation, H/w and S/w Implementation

Factor	**AES**	**DES**	**3DES**	**RSA**
Algorithm type	Symmetric	Symmetric	Symmetric	Asymmetric
Encryption	Fast	Moderate	Slower	Slower
Decryption	Fast	Moderate	Slower	Slower
Key length in bits	128,192 & 256	56	56,112 or 168	1024 or greater
Block size in bits	128	64	64	512 or more
No. of rounds	10,12 & 14	16	16	1
Key used	Same for both encode and decode data	Same for both encrypt and decrypt data	Three different keys to encrypt, decrypt and again encrypt	Different keys to encrypt and decrypt data
Key for Ciphering and deciphering	Same key	Same key	Three different keys	Different
Algorithm for Ciphering and deciphering	Different Algorithm	Different Algorithm	Different algorithm	Same algorithm
Algorithm scalability	Not scalable	Scalable	Scalable	Not scalable
Security	Higher security	Not secure	Effective Security	Less security
Vulnerability	BFA (Brute Forced Attack)	BFA, Linear & differential cryptanalysis attack	BFA, sweet32 attack	BFA and Oracle attack
Speed of simulation	Faster	Faster	Faster	Faster
H/w and S/w Implementation	Fast implementation	As compared to software better in hardware implementation	Efficient in hardware but not in software	Not efficient

Table 1 Comparison of encryption algorithms

 ISSN: 2454-4248
319 – 325

VI. IMAGE UPLOAD IN CLOUD

The image can be store and share on a cloud in a different format such as direct storage, use API & S3 sockets, upload in pieces, Asynchronous uploads, compression.

Images are uploads on the cloud using Mobile devices. The speed of uploading and downloading images/files depends upon the network speed which user uses. Different networks have different speed and upload/download data rates.

Image size (3 MB .png)	GPRS	EDGE	HSPS	HSPA+	4G
Upload data rate	20 Kbit/s	60 Kbit/s	2Mbit/s	22Mbit/s	1Gbit/s
Download data rate	114 Kbit/s	384 Kbit/s	7.2 Mbit/s	56 Mbit/s	100Mbit/s
Downloading time	7min 35sec	2min 31sec	8sec	1sec	.02 sec

Table 2: Speed of uploading and downloading

VII. SECURE SHARING ON CLOUD USING CRYPTOGRAPHY

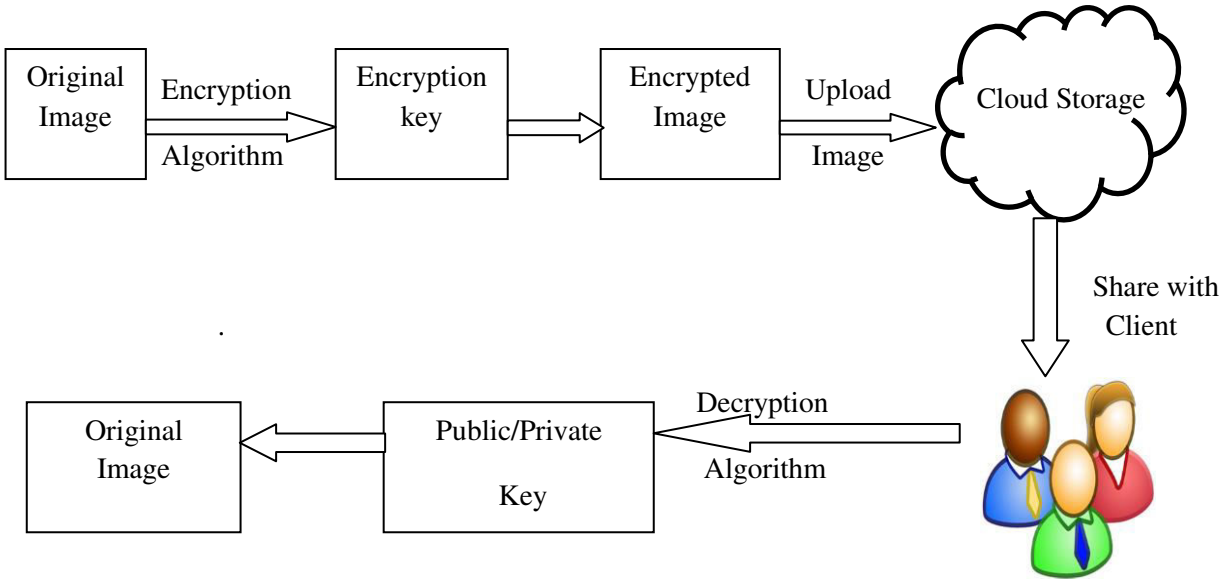

Fig. 2 Secure image sharing

The original image is fed into the encryption algorithm as an input. Encryption algorithms are applied to that image and perform substitution and various transformations. The encryption key is the public key which is applied to the original image and converts it into cipher (Encrypted) image. Encrypted image is uploading on cloud and sharing with other clients. At the receiver, side decryption is performed to decrypt the encrypted image. Decryption algorithm is applied to the encrypted image. This process is reverse of the encryption and converts the cipher image into an original image.

Conclusion

The growth of Cloud is tremendous nowadays and also must the security of data in the cloud. Cryptography provides the greatest security while sharing the images in the cloud. In this paper, we studied various cryptography algorithms. This survey provides the solution for achieving the security. Data owner encrypts his data before storing into the cloud so that unauthorized user does not access his personal data. Out of many encryption algorithms, AES is the best and fast algorithm. AES provides the highest security as compared to other algorithms. Comparison table of all the encryption algorithms shows that AES Algorithm is the best algorithm for the security of sensitive data. DES algorithm is suited for small data encryption; this algorithm provides the less security. To overcome the security issues of DES new 3DES algorithm is introduced which provide the efficient security. Figure 2 of secure image sharing on cloud shows that best way is the cryptography to encrypt the images before storing in the cloud. It can implement the proposed work in the secure image sharing in the cloud with a hybrid algorithm using AES, SHA3and optimized ECC algorithms. It will calculate the index building time and candidate selection time parameters.

Reference:

[1] H. Cui, X. Yuan,and C. Wang, "Harnessing Encrypted Data in Cloud for Secure and Efficient Mobile Image

Sharing", *IEEE Transactions on 8Mobile Computing*, vol. 16, no. 5, pp. 1315-1329, 2017.

[2] https://www.nist.gov/news-events/news/2011/10/final-version-nist-cloud-computing-definition-published

[3] " CLOUD COMPUTING – An Overview ", Torry Harris Online at http://www.thbs.com/downloads/Cloud-Computing-Overview.pdf

[4] C. Rao, M. Leelarani,and R. Kumar, "Cloud: Computing Services And Deployment Models", International Journal Of Engineering And Computer Science ISSN: 2319-7242, vol. 2, no. 12, pp. 3389-3392, 2013.

[5] Pancholi, V. R., & Patel, B. P. "Enhancement of cloud computing security with secure data storage using AES", International Journal for Innovative Research in Science and Technology, 2(9), pp.18-21, 2016.

[6] H. Cui, X. Yuan, and C. Wang, "Harnessing Encrypted Data in Cloud for Secure and Efficient Mobile Image Sharing", IEEE Transactions on 8Mobile Computing, vol. 16, no. 5, pp. 1315-1329, 2017.

[7] J. Wu, J. Wu, H. Cui, C. Luo, X. Sun and F. Wu, "DAC-Mobi: Data-Assisted Communications of Mobile Images with Cloud Computing Support", IEEE Transactions on Multimedia, vol. 18, no. 5, pp. 893-904, 2016.

[8] E. Vartiainen and K. Väänänen-Vainio-Mattila, "User experience of mobile photo sharing in the cloud", Proceedings of the 9th International Conference on Mobile and Ubiquitous Multimedia - MUM '10, 2010.

[9] Y. Wu, C. Thien, and J. Lin, "Sharing and hiding secret images with size constraint", Pattern Recognition, vol. 37, no. 7, pp. 1377-1385, 2004.

[10] P. Li, J. Cheng and H. Lu, "Hashing with dual complementary projection learning for fast image retrieval", Neurocomputing, vol. 120, pp. 83-89, 2013.

[11] Q. Liu, G. Wang and J. Wu, "Secure and privacy preserving keyword searching for cloud storage services", Journal of Network and Computer Applications, vol. 35, no. 3, pp. 927-933, 2012.

[12] J. Yu, P. Lu, Y. Zhu, G. Xue and M. Li, "Toward Secure Multikeyword Top-k Retrieval over Encrypted Cloud Data", IEEE Transactions on Dependable and Secure Computing, vol. 10, no. 4, pp. 239-250, 2013.

[13] Kumar, A., Lee, B. G., Lee, H., &Kumari, A." Secure storage and access of data in cloud computing". In ICT Convergence (ICTC), International Conference, pp. 336-339, IEEE. 2012

[14] N. Tirthani, G. R, "Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography", IACR Cryptology ePrint Archive, 2014.

[15] N. Gajra, S. Khan, and P. Rane, "Private cloud security: Secured user authentication by using enhanced hybrid algorithm", 2014 International Conference on Advances in Communication and Computing Technologies (ICACACT 2014), 2014.

[16] B. Acharya, N. Thomas, D. Arasu and N. Prasad, "Encryption and decryption of informative image by key image using modified Hill cipher technique based on non-invertible matrices", Proceedings of the 2011 International Conference on Communication, Computing & Security - ICCCS '11, 2011.

[17] S. Sood, "A combined approach to ensure data security in cloud computing", Journal of Network and Computer Applications, vol. 35, no. 6, pp. 1831-1838, 2012.

[18] P. Mahajan, &Sachdeva, A. "A study of encryption algorithms AES, DES and RSA for security." Global Journal of Computer Science and Technology, 2013.

[19] G. Singh, Supriya. "A study of encryption algorithms (RSA, DES, 3DES and AES) for information security." International Journal of Computer Applications, 67(19), 2013.