iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** VI **Month of publication:** June 2020

DOI: http://doi.org/10.22214/ijraset.2020.6147

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VI June 2020- Available at www.ijraset.com

Secure Storing and Sharing of Cloud Data under Key Exposure: A Survey

Deepa Chandran P[1], Shamna H R[2]
[1]*M. Tech. Student, Dept. of Information Technology, Government Engineering College, Barton Hill, Kerala, India*
[2]*Associate Professor, Dept. of Information Technology, Government Engineering College, Barton Hill, Kerala, India*

Abstract: ***In the era of digitization and technological advancement, cloud computing is that the trending domain in several regards. Cloud computing permits us to form and customize business applications on-line. It allows the cost-efficient, easy approach by configuring the parts and also the applications on information centers. Whereas security remains a serious concern in cloud. Once the cryptography secret is exposed, the sole possible way to preserve information confidentiality is to limit the adversary's access to the cipher text. However, if information is encrypted, using the existing cryptography schemes and spreading the cipher text on multiple servers hasn't entirely solved the matter since somebody who may acquire the cryptography key, will still compromise single server and rewrite the cipher text keep therein. We in this paper tend to address confidentiality, user authentication and information integrity under key exposure***.
Keywords: ***Cloud Computing, Key Exposure***

I. INTRODUCTION

Computing is being fully changed to a model consisting of services that are commoditized and delivered using a fashion quite like many utilities which is usually available like water electricity, etc. In such models, users able to access services supported their requirements without relevancy where the services are hosted. Different computing paradigms deliver this utility computing which include Grid computing, Peer to Peer computing, and more recently cloud computing. [1].

Cloud Computing is a trending and emerging computing technology that uses the online and thus the remote servers to need care of data and applications. Cloud Computing refers to applications and services offered over the web. These services are offered from data centers everywhere the world, which collectively are mentioned because the "cloud. "Cloud computing is Pay Per-Use-On-Demand model which may conveniently access shared IT resources through the web Where the IT resources include social networking sites, web mail, online business applications and network Services. Cloud computing divulge infrastructure, platform, and software (application) as services, which are made available as subscription-based services to consumers. These services in industry are respectively mentioned as Infrastructure as a Service (Iaas) ,Software as a Service (SaaS) and Platform as a Service (PaaS).To realize cloud computing potential, vendors like Amazon, Google, Microsoft and IBM are started to make and deploy Clouds in various locations across the planet. Additionally, companies working across the planet require the faster response time and thus save time by distributing workload requests to multiple Clouds in various locations at the same time. This creates the necessity for flourishing a computing world for dynamically interconnecting and provisioning Clouds from multiple domains within and across enterprises. There are many difficulties involved in creating such Clouds and Cloud interconnections. Cloud computing companies' states that data is secure, but it isn't completely true. Only time will tell if your data is secure within the cloud. Since customer data and program are residing in provider premises cloud security concerns are arising tons. While cost and easiness to use are two major benefits of cloud computing, there are significant security concerns that require to be addressed while moving critical applications and crucial data to public and shared cloud environments.

With social networking services gaining popularity it has to concentrate on sharing data. Google Docs is one such cloud platform which provides data sharing capabilities as groups of scholars, or teams performing on a project can share documents and should collaborate with one another effectively. There's an assumption that data servers will be trusted to stay the info secure. However, this assumption isn't any longer valid today since services are increasingly storing data across many servers that are shared with other data owners. The Cloud is prone to many privacy and security attacks. The largest obstacle hindering the development and also the wide adoption of the Cloud is that the privacy and security issues related to it. An example of this can be cloud data storage where cloud service providers aren't within the identical trusted domains as end users, and hardware platforms aren't under the direct control of information owners. To mitigate user's privacy concerns about their data, a typical solution is to store data in encrypted form so as that it will remain private, whether or not data servers or storage devices aren't trusted or compromised.

Cryptography is that the science of using mathematics to encrypt and decrypt data. It's the art of protecting information by transforming the initial message, called plaintext into an encoded message, called a cipher or cipher-text. It enables us to stay sensitive information or transmit it across insecure networks so as that it cannot be read by anyone except the intended recipient. Many cryptographic techniques are utilized in many cloud security platforms. Now a day cryptographic techniques seems to become essential for security in cloud. [2] There are two differing types of cryptography, private key cryptography and public key cryptography. In private Key cryptography the identical secret is used for both encryption and decryption. Example for personal key cryptography are AES, Blowfish, DES and Caesar Cipher. Public key cryptography, two keys are needed, one for encryption and one for decryption. Example for public key cryptography are RSA and YAK. Encoding using symmetric or public key cryptography isn't amenable to scalable access control. An initial promising approach to handle this issue is attribute-based encryption (ABE), ABE schemes will be divided into two categories: Cipher text- Policy ABE (CPABE) and Key-Policy ABE (KP-ABE), counting on the access policy is embedded into the cipher text or the user's private key. Here, Both CP-ABE and KP-ABE can prevent any unauthorized users from accessing data, whether or not the user stores data in an untrusted server.

This paper is organized as follows. Section 2 describes about cryptographic security services, Section 3 describes the prevailing cryptographic security principles and algorithms, Section 4 discuss the main points of cryptographic cloud storage, Section 5 address the cryptographic methods that are employed in cloud environment. Section 6 gives the conclusion about this text.

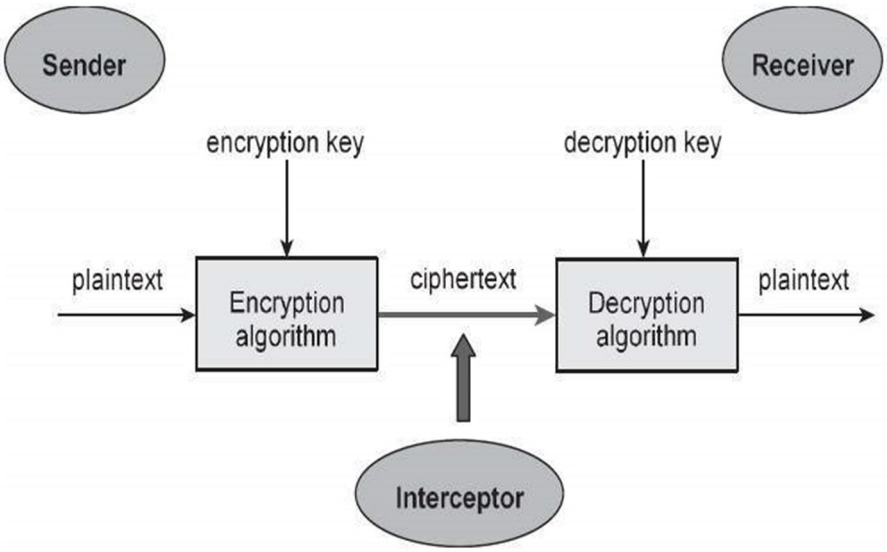


Fig. 1 Flow Diagram of cryptography

II. CLOUD SECURITY SERVICES

When data stores by using the third party the safety issue become more challenging and conflicting [3]. Availability, Integrity and Confidentiality are the main characteristics of security. These three properties became the key concept utilized in designing secure systems, especially, within the case of cloud computing architecture. 1) Confidentiality: It refers only to the authorized parties to allow accessing protected data. Outsourcing data, delegating its control to a cloud provider and making it accessible to different parties increase the danger of data breach. A number of concerns evolve relating to the issues of multi-tenancy, data remanence, application security and privacy. Multi-tenancy indicates the cloud characteristic of resource sharing. The cloud computing architecture consists of different sorts of shared resources to enable multiple clients to use the same resource at the same time which presents an amount of privacy and confidentiality threats. 2) Integrity: It refers to a process of protecting data from unauthorized deletion, modification or fabrication. The absence of any alteration in data between the two updates of data records indicates the accuracy and consistency of the stored data. Authorization is the mechanism employed by the system to work out what level of access a specific authenticated user should have to secure resources. According to the rise of the number of parties involved during a cloud environment, authorization is important to enforce data integrity. 3) Availability: It is the term which ensures that data continue to be available in situations starting from normal to disastrous. System availability indicates a systems ability to carry on operations even when some authorities misbehave. To ensure availability, the system should be capable to operate even if there is a security threat. The user of a cloud environment relies on the availability of the hardware requirements and ubiquitous network.

III.CRYPTOGRAPHIC PRINCIPLES AND ALGORITHM

Cryptography can help in the integration of Cloud Computing by increasing it privacy. The initial level of privacy where cryptography can help cloud computing is to provide safe and secure storage. Cryptography is the science of storing messages securely by converting the data into forms which isn't readable. In today's world, cryptography is considered as a collection of three main algorithms. These algorithms are Symmetric-key algorithms, Asymmetric-key algorithms and Hashing [4]. In Cloud computing, Data security, network traffic, file storage system, and security of the host are the main problems are associated, and cryptography can solve these issues to great extents alone. For a secure and secure communication between the guest domain and so the host domain, or from hosts to management systems, encryption technologies, like Secure HTTP, encrypted VPNs, TLS, Secure Shell, then on should be used. Encryption will help us prevent such exploits like man-in-the-middle, spoofed attacks, and session hijacking [5] Cloud computing provides clients with a computing facility or infrastructure on top of which they'll store data and run applications. While the benefits of cloud computing are pretty clear, it introduces new security challenges as cloud operators are speculated to manipulate data for clients without being trusted. Cloud data storage increases the danger of leakage of knowledge and doesn't give access to unauthorized users. Cloud data management can not be fully trusted by data providers. Cloud data process and computation could expose the privacy of users, owning the data or related entities to parities which doesn't have unauthorized access. For overcoming the above problems, cryptography has been widely applied to create sure data security, privacy and trust in cloud computing.

A. Symmetric Key Algorithms

Symmetric algorithm uses single key, which works for both encryption and decryption. The symmetric systems provide two main features to users. It ensures authentication and authorization. Symmetric-key algorithms are those algorithms which uses only one key for both. The key is kept as secret. Advantages of Symmetric algorithms is that it takes less computation power, and it works with very high speed in encryption. Types of Symmetric-key algorithms are Block cipher and Stream cipher. In bock cipher input is taken as a fixed sized block of plaintext depending on the different types of symmetric encryption algorithm, key of fixed size is applied on the set of plain text then the output block of the same size as the block of plaintext is obtained. In Case of stream cipher one bit is encrypted at a specific time. Major Symmetric-key algorithms used in cloud computing includes: Data Encryption Standard (DES), Triple-DES, and Advanced Encryption Standard (AES).

1) *Advanced Encryption Standard:* In cryptography, the Advanced Encryption Standard [6] is type of symmetric key encryption algorithm. Rounds, Sub Bytes—According to a table each byte is substituted with another. Rows are shifted— a transposition step where each row of the state is shifted cyclically a particular number of steps. In AES algorithm the Hash code is encrypted in a secure manner. Block size of AES is 128 bits. Its algorithm is Key Expansion, Initial Round - Round Keys are added. Rounds, Sub Bytes—According to a table each byte is substituted with another. Rows are shifted— where each row of the state is shifted cyclically a particular number of steps. Columns are mixed—A mixing operation on the columns of the state, combining the four bytes in each column 8. Add Round Key— each byte of that specific state is combined with the round key; each round keys derived from the given cipher key employing a key schedule. The DES algorithm was finally broken 1998 employing a system that costs about 250,000.Triple DES clothed to be too slow for efficiency because the DES algorithm was developed for mid-1970's hardware and didn't produce efficient and effective software code. The number of rounds of triple DES has thrice as many rounds as DES and is correspondingly slower.
2) *Data Encryption Standard:* The Data Encryption Standard (DES) is a block cipher and is a symmetric key cryptography found in January 1977 by the National Institute of Standards and Technology, named as NIST. [7] At the encryption side, DES takes a 64-bit plaintext and generate a 64-bit cipher text, at the decryption process, it takes a 64-bit cipher text and generate a 64-bit plaintext, and same 56 bit cipher key's used for both encryption and decryption. The encryption process is made with two permutations (Pboxes), which we call initial and final permutation, and sixteen Fiestel rounds. Each round uses a special kind of 48-bit round key which is generated from the cipher key consistent with a predefined algorithm.
3) *International Data Encryption Algorithm (IDEA):* IDEA is a symmetric key square cipher. [8] It utilizes a block cipher with a 128 bit key and is for the most part thought to be essentially secure. In this, 64-bit plaintext block is distributed into four 16-bit sub-blocks, since all the logarithmic exercises used as a piece of the encryption procedure work on 16-bit numbers. Another procedure produces for each one of the encryption rounds, six 16-bit key sub-blocks from the 128-bit key. Since a further four 16-bit key-sub-blocks are required for the subsequent yield transformation, a whole of 52 (= 8 x 6 + 4) various 16-bit sub-blocks must be delivered from the 128-bit key [9]. The 16-bit key sub-blocks of 52 in number, which are made from the 128-bit key are taken as: First, the 128-bit enter is allocated eight 16-bit sub-blocks which are then specifically used as the underlying

eight key sub blocks. The 128-bit key is then reliably moved to the other side by 25 positions, after which the ensuing 128- bit block is again apportioned into eight 16-bit sub blocks to be straightforwardly used as the accompanying eight key sub-blocks. This cyclic move system is repeated until most of the required 52 16-bit key sub-blocks have been created.

4) *Blowfish:* Blowfish also comes under symmetric block cipher which will be used as a substitute for DES.[10] It takes a variable-length key, making it considerably better for both domestic and exportable use. Bruce Schneider was designed Blowfish in 1993 as a free, fast substitute to existing encryption algorithms. Since then it has been verified and gained popularity as a strong encryption algorithm. Blowfish is available free for all uses.

B. Asymmetric key Algorithms

It is relatively a replacement concept unlike symmetric cryptosystem. Various keys are used for encryption and decryption process. This feature which make this scheme different than symmetric encryption scheme. Each receiver possesses a decryption key of its own, generally mentioned as his private key. Receiver must generate an encryption key, mentioned as his public key. Generally, this type of cryptosystem undertakes a trusted third party which officially declares that a particular public key belongs to a specific person or entity only. [11]

1) *RSA Cryptosystem:* This cryptosystem is one the foremost and oldest of asymmetric cryptosystem. It becomes the most employed and used cryptosystem even now. The system was invented by Ron Rivest, Adi Shamir, and Len Adelman and hence, it's termed as RSA cryptosystem. This algorithm is used for public-key cryptography and not private key cryptography. It is the first and most commonly used asymmetric algorithm. It involves two keys such as public key and private key. The public key is used for enciphering messages and is known to everyone. Messages encrypted with public key can be decrypted only by using the private key. In this verification process, the server implements public key authentication by signing a unique message with its private key, which is named as digital signature. The signature is then get back to the client. Then it get verifies with the server's known public key.
2) *Diffie-Hellman Key Exchange:* Developed by Whitfield Diffie and Martin Hellman a key exchange protocol with the help of the discrete logarithm problem in 1976. In this key exchange protocol sender and receiver will manage to line up a secret key, using an unsafe channel. to line up a key Alice chooses a random integer aE[1; n] computes ga, similarly gb is computed by Bob for random bE[1;n] and sends it to Alice. ga is Bob's secret key,(gb)a computes by Alice and Bob computes (ga)b. The important concepts on which the safety of the Diffie-Hellman Protocols defend on DDH, DHP, DLP like etc.
3) *Homomorphic Encryption:* Cloud user encrypts its data before sending to the Cloud provider, But, each time he has to work on that will have to decrypt that data. The consumer require the private key to the server to decrypt the data before to perform the calculations required, which might influence the confidentiality of data stored in the Cloud. Homomorphic Encryption systems are needed to perform operations on encrypted data without decryption. Only the consumer will have the secret key. When we decrypt the result of any operation, it's an equivalent as if we had performed the calculation on the plaintext (or original data).[12]
4) *Hashing Algorithms:* MD5- (Message-Digest algorithm 5): A 128 bit hash is the widely used hash function algorithm in cryptography that possesses a variable length message into a fixed length output of 128 bits. First the input message is divides up into 512- bit blocks then the message is padded so that its total length is divisible by 512. The sender of the data uses the public key to encrypt the message and the receiver uses receiver's private key to decrypt the message.

IV. CRYPTOGRAPHIC CLOUD STORAGE

The data may get disclosed or modified by any unauthorized access. It is essential that a special care must be taken to protect our sensitive data. A secure storage must be achieved in cloud computing. So we develop cryptographic techniques for the secure storage. The data encryption is done by the data owner before the data is uploaded to the cloud. The major feature of a cryptographic storage is that the security properties that are described above are accomplished. The data may get disclosed or modified by any unauthorized access. It is essential that a special care must be taken to protect our sensitive data. A secure storage must be achieved in cloud computing. So we develop a cryptographic techniques for the secure storage. The data encryption done by the data owner before the data is uploaded to the cloud. The major feature of a cryptographic storage is that the security properties that are described above are accomplished. The above diagram represents cryptographic cloud storage. The owner of the data applies cryptographic methods to the sensitive data to protect the information from unauthorized access. The data owner uploads the encrypted data to the cloud environment. The authorized user can decrypt the data and download the required file. The Strength of Cryptographic storage are Confidentiality and Integrity.

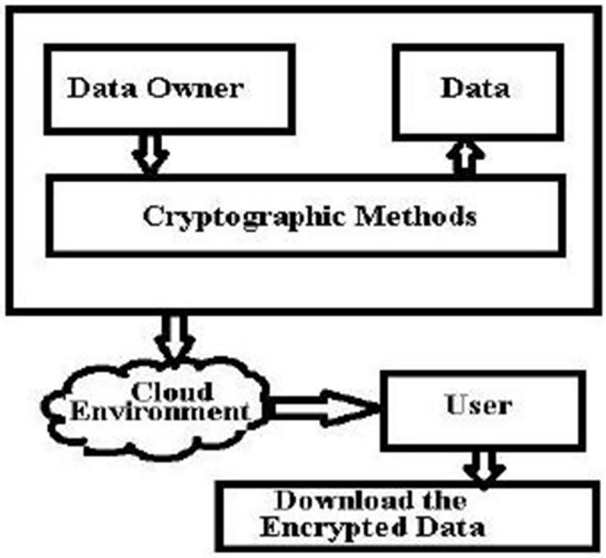


Fig. 2 Cryptographic Cloud Storage

V. METHODS FOR DATA PROTECTION IN CLOUD

A. *Public Key Encryption*

This type of encryption is also called asymmetric cryptography. As we have discussed above it uses both public and private keys to encrypt and decrypt data.

1) *Identity Based Encryption:* An Identity Based Encryption scheme is a public-key cryptographic algorithm, which consists of 3 elements: key generation, encryption and decryption where any string is a valid public key. In [15] Jianghong et al. proposed a revocable storage identity based encryption. This was mainly adopted to overcome various disadvantages faced by data sharing over cloud. Some of the issues faced are confidentiality of data and they are compromised sometimes as the cloud server are not reliable they may outsource data for their own benefits. The main advantage posed by this paper was to not make the data available for access once the user is denied access or his authority has been expired. The major drawback in this approach is it uses a decrypt then re-encrypts which involves user's secret key information which makes the data open to new attacks and vulnerable and furthermore the paper does not discuss on authenticity and availability of shared data.
2) *Attribute Based Encryption:* Attribute based encryption is a public-key encryption. Here the attributes are made to be dependent on the secret key and cipher text. It decreases the number of keys used and make faster the encryption and decryption process. In [16] Ruixuan et al. proposes an algorithm called lightweight data sharing scheme with an addition to cipher text policy attribute based encryption is used to offer efficient access control and proxy servers are used for encrypting and decryption operations this reduces computational overhead. Here it uses lazy re-encryption to reduce the overhead caused by revocation. The major disadvantage posed by this paper is verification of data integrity is not done properly and cipher text retrieval over existing data sharing schemes are not pointed out. Existing data sharing schemes are not properly mentioned.
3) *Key-Policy Attribute-based Encryption:* In [17] C.Wang.Introduced KP-ABE with constant size cipher. In Key-Policy Attribute-based Encryption, the encrypted data is constructed with the set of attributes. The person is authorized to decrypt the Cipher text if and only if the attributes that are the access structure of their private or secret keys are done by built with the cipher text satisfy. The four steps in Key-Policy Attribute Based Encryption are Setup, KeyGen, Encrypt, and Decrypt. The KeyGen and Decrypt algorithms get differed as per Attribute Based Encryption. In Key-Policy Attribute-based Encryption, private key of the user is related with the access structure. However, people may decrypt the information when unauthorized access may occur. This can be overcome in the Cipher text Policy Attribute Based Encryption which construct the access policy within the encrypted data i.e., cipher text and employs a set of attributes to describe the private key of the user. Also, in some applications that uses this scheme, the owner of the data must have a firm belief with the key provider.
4) *Cipher text Policy Attribute based Encryption:* In [18] Bethencourt et al. developed a cryptographic technique namely cipher text policy attribute-based method. The access policy introduced with the data that has been encrypted. In CP-ABE the cipher text is identified with access structure and therefore the private keys with the attributes. In Key-Policy Attribute Based

Encryption, the main disadvantage is that the access policies were not created by the encryptor. This provided a route to the establishment of Cipher text Policy Attribute Based Encryption which allows the access policies to be built with the encrypted data. The owner who encrypts the data, model the access policy. Data owner have the power of defining the access policies. This prevents unauthorized access and promotes security. In CP-ABE, revocation is not achieved efficiently. Thus, it's not very easy for the info owner to switch the access polices whenever needed.

5) *MultiAuthority Attribute based Encryption*: Multi-Authority Attribute Based Encryption is introduced by Chase [19] The Multi-Authority Attribute Based Encryption (MAABE) is also a cryptographic technique which consists of many authorities to manage the attributes and the distribution of the secret keys. The user who wish to download the information will request the decryption keys from the attribute authority. MA-ABE is attribute based key algorithm. This algorithm run by authority and authority will distribute the keys to the users. An authorized user who has the appropriate decryption keys can view the information. The algorithms involved in this scheme include Set up, Attribute Key Generation, Central Key Generation, Encryption, and Decryption. This cryptographic scheme handles more number of users.In cloud environment Data confidentiality can be achieved using this. As it is suitable well for multiple authorities' scenario, this cryptographic technique is most suitable for the applications which contains various sectors. This cryptographic scheme improves security and reduces key management complexity which are the major advantages.

B. Deduplication

Deduplication is the process of avoiding repeated storage of a single file so as to reduce the storage overhead. It is also called as single instance storage as it does not allow redundant copies of a file to be stored in the storage device. This helps in enhancing the storage utilization and it can be used in network data transfers to control the number of bytes that must be sent. In [20] Yifeng et al. Propose a functionality that can be added to the cloud service which vanishes the duplicate copies of a particular file. The cloud service may encounter such a problem because of hosting images, videos or even text from different sources. This functionality is just an addition to the existing framework to perform secure deduplication. Different from the existing work which ensures protection against offline brute-force attacks, this paper propose a comprehensive protection system. This framework resists data leakage and also the off-line brute-force attack. The system architecture consists of an encrypted cloud media and an agency server. This agency server properly executes encryption of data in a way that will help achieve efficient deduplication. The main disadvantage is this is done over only predictable videos and data. It also proposes a heterogeneous data storage management scheme is proposed where Deduplication is performed on multiple Clouds. The duplicate files which are present in different Clouds are removed due to which storage wastage is reduced.

In this scheme, every user has a secret key about ABE and this key is used to generate the ABE decryption key of the users based on the attribute ID which is known as secret key attribute. Here, Deduplication is not only performed on multiple clouds but also tends to maintain unique data in all the clouds. When a user selects a file to upload, Hash Code is generated for the data, which is used for duplicate data checking. After Hash Code, signed Hash Code is generated which is used for originality verification of the file. Then the signed Hash Code is placed at CSP for replica check. If duplicate data are not found at any CSP, then the data owner encrypts the data with the randomly generated symmetric key data encryption key (DEK). DEK is then splits into two parts i.e.; DEK1 and DEK2. DEK1 is encrypted with the public key of authorized party (AP) and DEK2 is encrypted with the public key of the user. Once the encryption is completed, encrypted DEK1 and DEK2 are passed to the CSP along with encrypted data. The Disadvantage with the existing system is that if the symmetric key is known to hackers, they can easily decrypt the data and access it.

C. Key Exposure Cryptosystem

1) *Deniable Encryption:* Deniable Encryption was introduced to ensure that the sender or the receiver in the communication able to create and encrypt fake messages into various cipher texts to produce the real messages from a coercing adversary. In [21] R Canetti et.al propose that an encryption scheme is "deniable" if—when coerced to reveal the encryption key—the legitimate owner reveals, "fake keys" thus forcing the cipher text to "look like" the encryption of a plaintext different from the original one— hence keeping the original plaintext secure. Deniable encryption therefore aims to develop an adversary who does not know the "original" encryption key but, e.g., can only acquire "fake" keys. The Disadvantage with the existing system is that if the symmetric key is known to hackers, they can easily decrypt the data and access it.
2) *Secret Sharing*: Secret sharing schemes allow a dealer to distribute a secret among variety of shareholders, such that only authorized subsets of shareholders can reconstruct the secret. A Shamir [22] et.al proposes threshold secret sharing schemes. The dealer defines a threshold t and each set of shareholders of cardinality adequate to or greater than t is permitted to

reconstruct the secret. Secret sharing guarantees security against a unauthorized group of shareholders. Disadvantage is that it incurs a high computation/storage cost, which makes them impractical for sharing large files. Rabin [23] et al.proposed an Information Dispersal Algorithm (IDA).IDA breaks a file F into n pieces so that every m pieces suffice for reconstructing F.The dispersal and reconstruction are computationally very efficient. In Secret sharing scheme overhead is less when compared to other scheme. And also it is space efficient. The Disadvantage is that it does not provide any security guarantees when a little number of shares are available(less than the reconstruction threshold). In [24] krawczyk et.al combine both Shamir's [22] and Rabin's approaches [23]; a file is first encrypted using AES and then dispersed using the scheme in [23], while the encryption key is shared with this scheme specified in [22]. In Krawczyk's scheme, disadvantage is that individual cipher text blocks encrypted with AES are often decrypted once the key's exposed.

3) *Leakage-resilient Cryptography*: Leakage-resilient cryptography aims at designing cryptographic primitives that can resist an adversary who learns partial information about the secret state of a system, e.g., through side-channels [25].Different models give way to reason about the "leaks" of real implementations of cryptographic primitives [25]. All of these models, however, limit when secret information knowledge when exposed to the adversary

4) *All-Or-Nothing Transforms (AONTs)*: The family of the all-or-nothing transforms is composed of different types of algorithms aiming at transforming a sequence of input messages into a sequence of output messages, in a way that recovery of the input messages is impossible only if all the splits of (or almost all) output messages are present. During descriptions, we denote input messages as X = x1,. . . xn and output messages as follows Y = y1, . . . , ym. Usually, an all-or-nothing transform is applied on the cipher text in order to make its partial decryption impossible (in some cases even when the encryption key is known) Rivest's AONT.

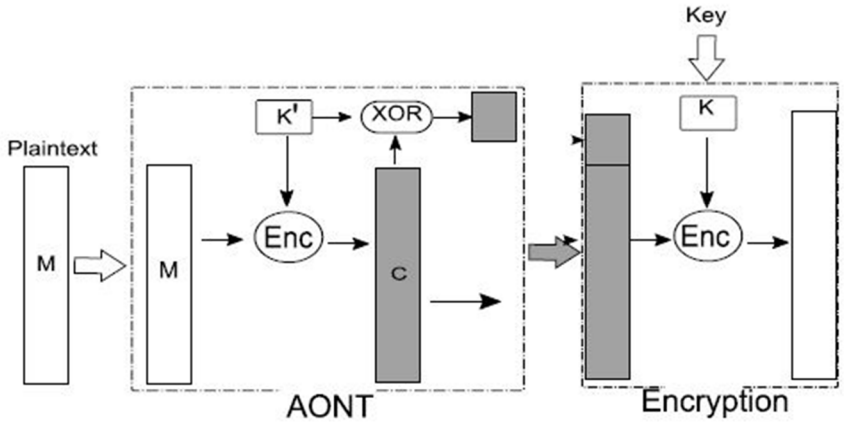


Fig. 3 AONT Strategy

Rivest [26] was the first one to introduce an all-or-nothing transform. In his proposal, the transformation is finished before encryption of knowledge. During this transformation step the sequence of n input messages is transformed into a sequence of m= n + 1 output messages. First, each input message xi is encrypted with a randomly generated key K: yi = xi E (K, i), where E could be a symmetric encryption function.Second, a hash value of the output message is decided which is: hi = H (K0, yi),using a public key K0 (H could be a keyed hash function). Third, the ultimate output message is generated using an exclusive-or of K and of all its hashes: ym = Kn i=1 hi. The obtained sequence of output messages Y is then able to be encrypted. Rivest's pre-processing protects against the exposure of the key accustomed encrypt output messages after the transform. However, it doesn't protect against a situation when an attacker managed to tackle the random key K used during the pre-processing additionally to the encryption key used after the pre-processing. Moreover, Rivest's development requires two rounds of encryption (one during pre-processing and one after) that would be a burden for performance.Desai's AONT. Desai [27] proposed a modification to the Rivest's proposal that skips the round computing hashes. Instead, the last output message yn is outputted as an exclusive or of the random key and of all previously obtained n output blocks: ym = Kn i=1 yi. Such processing improves the performance. However, the knowledge of the encryption key K allows the recovery of an output message.

a) *AONT-RS:* AONT-RS [28, 29] limited the Rivest's proposal to a single encryption round, but in a different way than the Desai's transform. In AONT-RS, input messages X are encrypted by taking a random key K into output messages. Then one hash of X is then computed and exclusive-ored with the key. Moreover, AONT-RS treats the problem of data integrity and availability by adding a canary to the input messages and by generating additional output messages using systematic Reed-Solomon codes [32]. Similarly to Desai's proposal, AONT-RS allows a smaller reconstruction of the input messages under the situation of key exposure.

b) *Bastion's AONT:* Ghassan O Karame et al. Inspired by Stinson's work [30], Bastion's AONT [31] ensures that input messages cannot be recovered as long as the adversary has access to all but two output messages. Input messages consist of encrypted data (a message corresponds to a block of a cipher text.).During the transformation, the sequence of input messages is then multiplied by a square matrix A, such that: (i) all diagonal elements are taken as to 0, and (ii) the remaining off diagonal elements are taken to 1 (matrix are invertible and A = A1, so the inverse transform X = A1 • Y = A • Y). The multiplication Y = A • X ensures that each output message yi will depend more on all output messages yj except from yi. Bastion achieves excellent performance by transformation using only 2m exclusive-or operations.

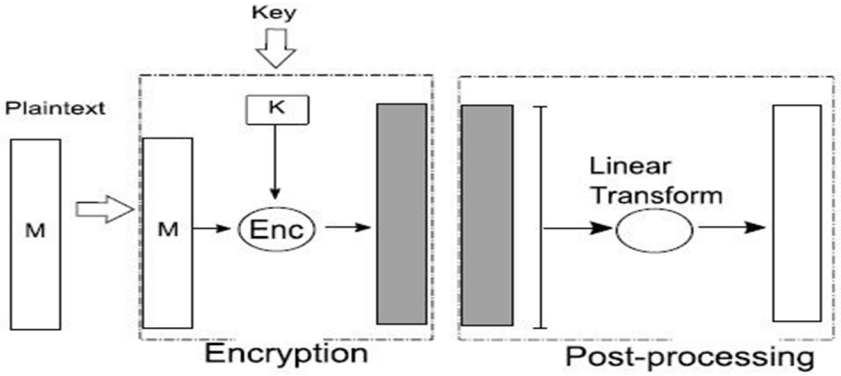


Fig. 4 Bastion Strategy

c) *Mix and Slice:* Mix Slice [33] is an approach to improve access revocation on resources stored at external cloud providers. Interdependencies are build inside an outsourced resource composed of encrypted data, so re-encrypting even a small portion of the resource with a fresh key revokes the access to a user who does not possess the new key. The algorithm used for resource transformation can be seen as a case of an all-or-nothing transform, as it has similar property: data decryption is not possible without the possession of the whole cipher text. In Mix Slice, input messages are composed of already encrypted data. The transformation into final output messages is performed using multiple encryption rounds – each encryption round re-encrypts (and thus creates dependencies between) different sets of the output messages are obtained during the previous encryption round. The following paper demonstrates as to how erasure codes can be used effectively to store data on different nodes in a distributed system. Erasure codes are space optimal and it effectively replicates data on different nodes so that it can be recovered in times of failure. The algorithm proposed in this paper keeps erasure codes consistent even during concurrent access. The "full: read and write algorithm" depicts on how concurrent write operation is managed using swap. The "recovery algorithm" provides security mechanisms when a particular client crashes.

d) *Privacy Preserving:* Privacy preserving is just a term used for accessing documents only for the user's purpose. It involves two users who own a confidential database. It runs a data mining technique on the union of their database without revealing sensitive information. In [34] Bernardo et al. propose a secure system for privacy enhanced storage and retrieval of dynamically updated image repositories. This paper focuses on image data as it is the major part of the global internet traffic. The proposed system based on Image Encryption Scheme (IES) with Content-Based Image Retrieval (CBIR) properties. By using this image is separated into its color based and texture based data and each portion is encrypted using different algorithms. Mostly the texture information is more useful while compared to color information in object recognition. Therefore, in this paper texture information is encrypted using semantically secure algorithms and colour information is encrypted using a less secure algorithm. The system model architecture consists of Cloud Infrastructure, Key Distribution Service and end users. The main advantage of this paper is that by using this framework ensuring privacy is executed without overloading the client overhead (for encryption purposes). The main disadvantage of this framework is that it cannot be extended to other data sets.

Techniques	Parameters			
	Confidentiality	Authenticity	Integrity	Storage Utilization
Public Key Encryption IBE	✓		✓	
ABE	✓	✓	✓	
Deduplication			✓	✓
Key-Exposure Cryptosystem	✓	✓		
Privacy Preserving	✓	✓		

Comparative Analysis

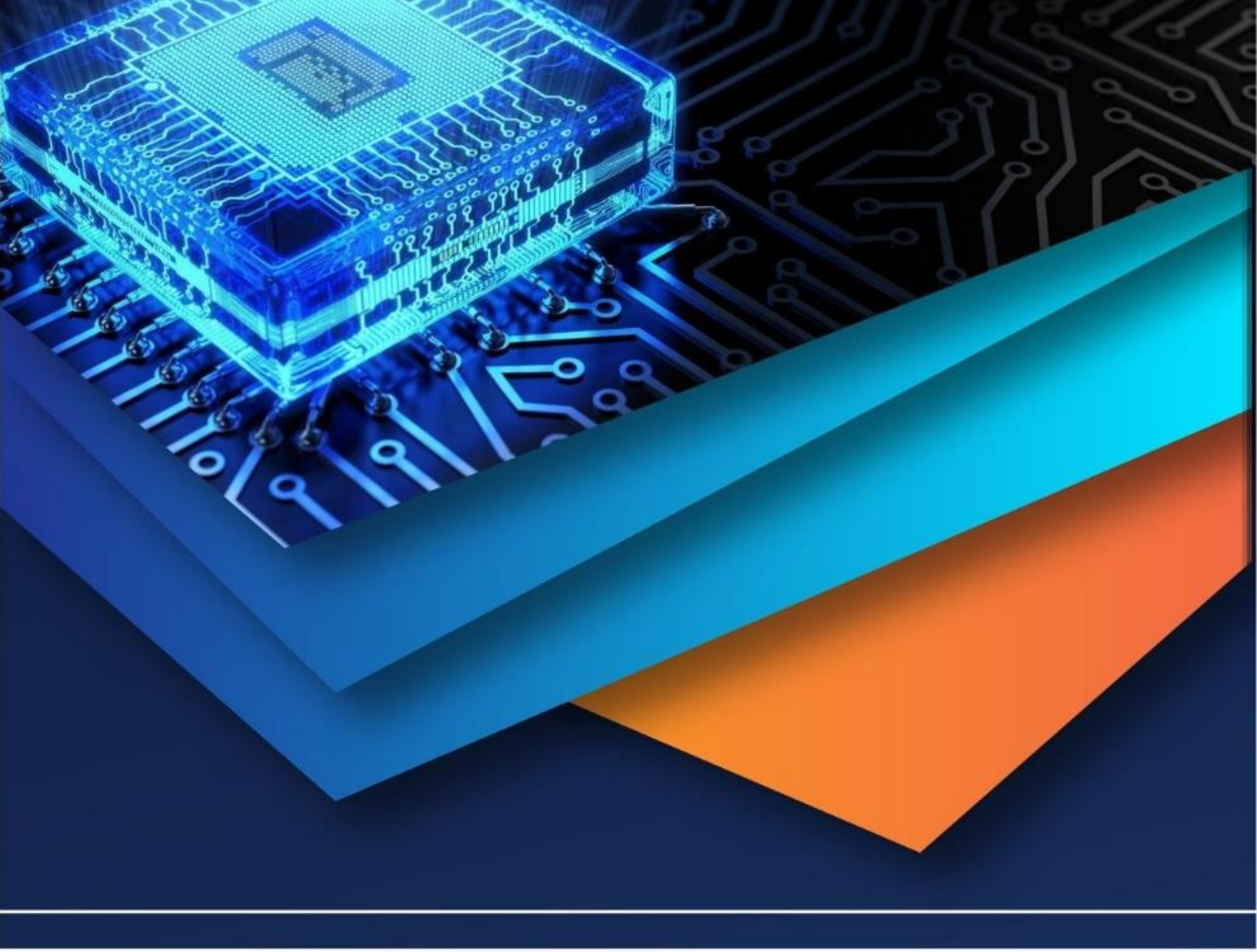
VI. CONCLUSION

The data sharing have always been a problem in cloud as there can be no way of identifying data stealing or other attacks. This paper helps in identifying the pros and cons of using various techniques that have been employed for secure transaction or data sharing over cloud server. However, in both domains based storage protection and key exposure techniques both confidentiality and integrity are maintained. Some of the other features that are added to the cloud for data sharing are deduplication, privacy preserving which maintains the cloud free of duplicate data and to make the data available only for the user's purpose. As a result, there is a need to build a secure

REFERENCES

[1] R. Buyya, "Cloud computing: The next revolution in information technology," 2010 First International Conference On Parallel, Distributed and Grid Computing (PDGC 2010), Solan, 2010, pp. 2-3.doi: 10.1109/PDGC.2010.5679963
[2] S. Dahiya and R. Sharma, "Comparative Study of Popular Cryptographic Techniques," 2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), London, 2018, pp. 36-43.doi: 10.1109/WorldS4.2018.8611581
[3] Vishwa gupta, " Advance cryptography algorithm for improving data security ", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 1, January 2012 ISSN:2277 128X.
[4] Hussein, Nidal Salih, Ahmed Khanfar, Khalid," A Survey of Cryptography Cloud Storage Techniques",International Journal of Computer Science and Mobile Computing 186-191,2016
[5] Rashmi Nigoti, Manoj Jhuria, Dr. Shailendra Singh, "A survey of Cryptographic algorithms for cloud computing", International Journal of Emerging Technologies in Computational and Applied Sciences,March 2013, ISSN (online)-2279-0055.
[6] Bokefode Jayant.D, Ubale Swapnaja A, Pingale Subhash V., Karane Kailash J. , Apate Sulabha S. ,"Developing Secure Cloud Storage System by Applying AES and RSA Cryptography Algorithms with Role bases Access Control Model", International Journal of Computer Applications,Volume 118-No.12, May2015
[7] S. Chandra, S. Paira, S. S. Alam and G. Sanyal, "A comparative survey of Symmetric and Asymmetric Key Cryptography,"2014 International Conference on Electronics, Communication andComputational Engineering (ICECCE), Hosur, 2014, pp. 83-93.doi:10.1109/ICECCE.2014.7086640.
[8] N. L. Kodumru and M. Supriya, "Secure Data Storage in Cloud Using Cryptographic Algorithms," 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), Pune India, 2018, pp. 1-6. doi: 10.1109/ICCUBEA.2018.8697550
[9] Chang, How-Shen. "International data encryption algorithm." jmu. edu,googleusercontent. com, Fall (2004).
[10] Ms NehaKhatri – Valmik1,Prof. V. K Kshirsagar,"Blowfish Algorithm",IOSR Journal of Computer Engineering (IOSR-JCE)e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. X (Mar-Apr.2014), PP 80-83
[11] M. G. V. Kumar and U. S. Ragupathy, "A Survey on current key issues and status in cryptography," 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, 2016, pp. 205-210.doi: 10.1109/WiSPNET.2016.7566121.
[12] R.Kirubakaramoorthi*, D. Arivazhagan and D. Helen,"Survey on Encryption Techniques used to Secure Cloud Storage System",Indian Journal of Science and Technology, Vol 8(36), DOI: 10.17485/ijst/2015/v8i36/87861, December 2015.
[13] T. A. Mohanaprakash, A. Irudayapaulraj Vinod, S. Raja, Ari Pavan Kalyan,C.B.Babu,Golla Vivek "A Study of Securing Cloud Data Using Encryption Algorithms",International Journal of Scientific Research in Computer Science, Engineering and Information Technology 2018 IJSRCSEIT Volume 3 Issue 1,ISSN : 2456-3307
[14] G. Kishore Kumar, Dr.M.Gobi"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.
[15] J. Wei, W. Liu and X. Hu, "Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption," in IEEE Transactions on Cloud Computing, vol. 6, no. 4, pp. 1136-1148, 1 Oct.-Dec.2018. doi: 10.1109/TCC.2016.2545668
[16] R. LI, C. Shen, H. He, X. Gu, Z. Xu and C. Xu, "A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing," in IEEE Transactions on Cloud Computing, vol. 6, no. 2, pp. 344-357, 1 April-June 2018. doi: 10.1109/TCC.2017.2649685
[17] C. Wang and J. Luo, "A Key-policy Attribute-based Encryption Scheme with Constant Size Ciphertext," 2012 Eighth International Conference on Computational Intelligence and Security, Guangzhou, 2012, pp. 447-451. doi: 10.1109/CIS.2012.106
[18] J. Bethencourt, A. Sahai and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," 2007 IEEE Symposium on Security and Privacy (SP '07), Berkeley, CA, 2007, pp. 321-334. doi: 10.1109/SP.2007.11.
[19] Chase M, "Multi-authority Attribute Based Encryption" ,Theory of Cryptography. TCC 2007. Lecture Notes in Computer Science, vol 4392.Springer, Berlin, and Heidelberg.

[20] Y. Zheng, X. Yuan, X. Wang, J. Jiang, C. Wang and X. Gui, "Toward Encrypted Cloud Media Center With Secure Deduplication," in IEEE Transactions on Multimedia, vol. 19, no. 2, pp. 251-265, Feb. 2017. doi: 10.1109/TMM.2016.2612760.
[21] R. Canetti, C. Dwork, M. Naor, and R. Ostrovsky, "Deniable Encryption,"in Proceedings of CRYPTO, 1997.
[22] A. Shamir, "How to Share a Secret?" in Communications of the ACM, 1979, pp. 612–613.
[23] M. O. Rabin, "Efficient dispersal of information for security, load balancing, and fault tolerance," J. ACM, vol. 36, no. 2,pp. 335–348,1989.
[24] H. Krawczyk, "Secret Sharing Made Short," in Advances in Cryptology (CRYPTO), 1993, pp. 136–146.
[25] S. Micali and L. Reyzin, "Physically observable cryptography (extended abstract)," in Theory of Cryptography Conference (TCC), 2004, pp. 278–296.
[26] Rivest, R.L.: All-or-nothing encryption and the package transform. In: Biham, E. (ed.) FSE 1997. LNCS, vol. 1267, pp. 210–218. Springer, Heidelberg (1997). https://doi.org/10.1007/BFb0052348
[27] Desai, A.: The security of all-or-nothing encryption: protecting against exhaustive key search. In: Bellare, M. (ed.) CRYPTO 2000. LNCS, vol. 1880, pp. 359–375. Springer, Heidelberg (2000).https://doi.org/10.1007/3-540-44598-6 23.
[28] Chen, L., Laing, T.M., Martin, K.M.: Revisiting and extending the AONT-RS scheme: a robust computationally secure secret sharing scheme. In: Joye, M., Nitaj, A. (eds.) AFRICACRYPT 2017. LNCS, vol.10239, pp. 40–57. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-57339-7 3
[29] Resch, J.K., Plank, J.S.: AONT-RS: blending security and performance in dispersed storage systems. In: Proceedings of the 9th USENIX Conference on File and Storage Technologies, FAST 2011, p. 14, Berkeley,CA, USA (2011). http:// dl.acm.org/citation.cfm?id=1960475.1960489.
[30] Stinson, D.R.: Something about all or nothing (transforms).Des. Codes Cryptogr. 22(2), 133–138 (2001).https://doi.org/10.1023/A:1008304703074.
[31] Karame, G.O., Soriente, C., Lichota, K., Capkun, S.: Securing cloud data under key exposure. IEEE Trans. Cloud Comput., p. 1 (2019).https://doi.org/10.1109/TCC.2017.2670559
[32] Reed, I.S., Solomon, G.: Polynomial codes over certain finite fields. J. Soc. Ind. Appl. Math. 8(2), 300–304 (1960). https://doi.org/10.1137/0108018.
[33] Bacis, E., De Capitani di Vimercati, S., Foresti, S., Paraboschi, S., Rosa, M., Samarati, P.: MixSlice: efficient access revocation in the cloud. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, CCS 2016, pp. 217–228. ACM, New York (2016). https://doi.org/10.1145/2976749.
[34] Bernardo Ferreira, Joao Rodrigues, Joao Leitao, Henrique Domingos,"Practical Privacy-Preserving Content-Based Retrieval In Cloud ImageRepositories" IEEE Transactions on Cloud Computing, Vol.PP, Issue.99, 2017. doi: 10.1109/TCC.2017.2669999



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY