International Journal of Education and Science Research Review
E-ISSN 2348-6457
Volume-11, Issue-1 January-February-2024 P-ISSN 2349-1817
www.ijesrr.org Email- editor@ijesrr.org

DATA FORTIFICATION APPROACHES IN THE CLOUD COMPUTING

Manoj Kumar, Research Scholar, School of Technology and Computer Science, Glocal University, Mirzapur Pole Saharanpur (U.P)

Prof.(Dr.) Pratap Singh Patwal, Research Supervisor , School of Technology and Computer Science, Glocal University, Mirzapur Pole Saharanpur (U.P)

ABSTRACT:

In this data that are kept in the cloud to take many advantages that are made available by the features of cloud computing. These advantages include storage management, ubiquitous access, cost reductions in hardware installation, software licensing, and service management. The cloud computing platform offers its customers a variety of processing and storage options. One of the delivery modelsthat the cloud uses is called Infrastructure as a Service (IaaS), and it is used to supply cloud storage. All of these advantages drive enterprises to store their data in the cloud. The fact that the data is kept on the cloud (a distant server) which is shared by many users and the data is not under the direct control of the data owner raises some severe concerns about the security of the data that is stored. The integrity ,confidentiality, and availability of the data are all components of data security. In this work, we have explored the data security concerns that develop as a result of the nature of cloud computing, namely in terms of confidentiality, integrity, and availability, and we have presented numerous solutions that are purposed by the researcher to counteract these security difficulties. We have high hopes that the researcher will be able to better grasp the current approach that is used to secure cloud storage after reading this study, and we believe that in the future, even more secure cloud storage strategies will be developed.

Keywords: *Cloud storage, Symmetric key cryptography, ,Proxy re-encryption, Asymmetric key cryptography . Secure data sharing, Confidentiality, Integrity, availability,*

[1] INTRODUCTION

Cloud computing offers a broad variety of services, including compute, storage, and infrastructure, and these services are deliveredusing one of three delivery model, IaaS is for "Infrastructure as a Service," PaaS stands for "Platform as a Service," and SaaS refers to "Software as a Service."Since the beginning of the last few years, there has been a tremendous growth of people using cloud computing.. A wide variety of companies, such as Amazon Web Services (AWS), Google CloudStorage, HP, and IBM, are providing cloud computing services to its customers.

The storage of data on a cloud server has numerous benefits, but it also raises several problems, the most important of which is the safety [1, 2] of any data that is outsourced. To ensure that one's data in the cloud is secure, one must implement security measures such as integrity, confidentiality and availability, sometimes known as the CIA triad. In addition to these measures, an audit and access control system must be in place. According to the research [3, 4, 5, 6, 7], a poor level of system security is the cause of many incidents that result in the loss of data.

Data Integrity: Integrity of data relates to the correctness of data and is concerned with unlawful change, deletion, or data

fabrication [8]. The guarantee of the stored data's authenticity, consistency, or regularity may be obtained via the use of cloud computing's data integrity protection feature.

Data Availability: Data Availability means that data should be available, accessible, and useable when valid users make a demand for it in accordance with SLA agreements. When data availability is ensured, the user is provided with the peace of mind that all of the data hosted by the user is safely kept on the cloud server, without any accidental or intentional deletion of any portion of the data from the server.

Data Confidentiality: The term "data confidentiality" refers to the act of not disclosing data to users who are not allowed to access it. There are many distinct kinds of active and passive attack exits, each of which has the potential to jeopardize the data's secrecy. The user is given the peace of mind that their data will not be accessed by unauthorized employees if the confidentiality of their data is protected.

Access Control: It is necessary to have an appropriate access control in place in order to ensure that data is only shared with authorized users. The cloud server stores several sets of data, and while many users have permission to access the system, those users are restricted from accessing any other data; rather, they are only able to view the data for which they have permission.

Audit: Audit is used to examine the availability and integrity of the data that has been stored. Either the user him/herself, or a third party, is responsible for carrying it out. In most cases, the data that is kept in the cloud is enormous, and since it is both costly and beyond the capabilities of most cloud users, the task of storing the data is almost always delegated to a third party.

Two distinct types of attacks may be done against cloud computing:

i) Internal Attack: Internal assaults are a major cause for worry when it comes to the safety of data stored in the cloud. An internal attack is carried out when a dishonest employee of a cloud service provider has access to private information belonging to a company's customers. They could risk compromising the sensitive information in order to get financial gains.

ii) External Attack: In an external attack, the malicious user is located outside of the cloud service provider and is responsible for carrying out the attack. They are able to use the internet to launch a variety of active and passive forms of attack. Phishing, port scanning, IP spoofing, and DNS poisoning are some of the attack methods that may be used to obtain access to cloud services.

If a wicked user, whether it be an insider or an outsider, was successful in performing assaults on the cloud resources, this might lead to the company incurring a significant amount of damage, either in terms of money or in terms of the reliability of the service provider.

[2] CLOUD COMPUTING SYSTEM MODEL

The cloud computing structure for the storage of data may be considered as the entities that are engaging in the interaction. These entities include the Cloud users, Data owner, Cloud Service provider, and the trustworthy third party.

The system model of cloud computing is shown here by figure [1]

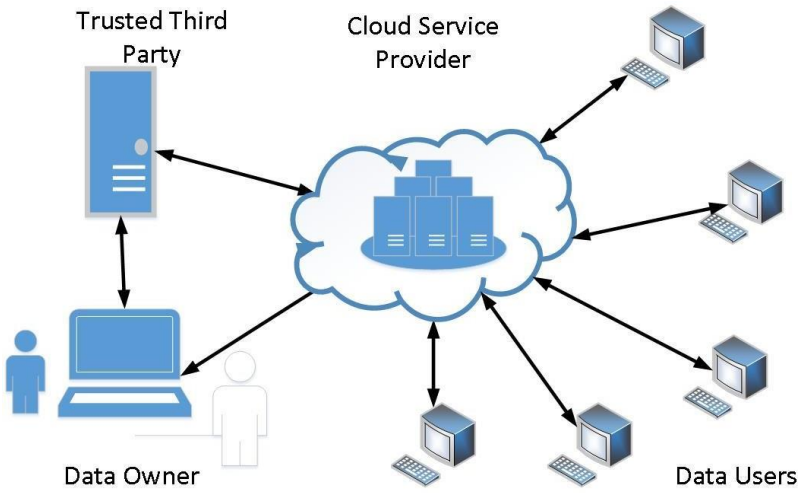

Fig 1: System Model of cloud computing for Data Storage

2.1 Cloud User: Someone who has been given permission to access the data in accordance with the access control policy that the data owner has defined. The data user may be given read/write permission by the data owner. If the cloud user only has read permission, he is able to read the data, but he is unable to edit the data. On the other hand, if the cloud user also has write access, he is able to read the data as well as modify it.

2.2 Data Owner: A data owner is a person or company that has outsourced the management of their data to a cloud server in order to take advantage that cloud computing has to offer. It is possible that the owner of the data will also be the user of that data, or that the data may be shared among several users, including the owner of the data.

2.3 Cloud Service Provider: The data owner stores his data on the cloud server, which is managed by the cloud service Provider. The responsibility of a cloud service provider includes the establishment and configuration of a data center, the monitoring of the system for availability and performance, the repair of hardware and software, the implementation of an appropriate security mechanism to ensure the security of data and the physical security of the machine, and the guaranteeing of a virtual machine level and file level restore in the event that data is lost or corrupted.

2.4 Trusted Third Party: The trusted third party is a third party that is trusted by both of the parties involved in the transaction. The protection of the data should be the primary objective of a trusted third party. In a cryptographic system that uses public keys, the certificate authority functions as a trusted third party that issues digital certificates to validate ownership of public keys [9]. The public later be used to decode data. A trusted third party also performs the function of an auditor on the cloud user's behalf to guarantee that the data's availability and integrity are maintained.

[3] CONCERNS WITH DATA SECURITY: CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY

The confidentiality of the data, the integrity of the data, the availability of the data, and the secure access and access control are all to be considered in relation to cloud data storage security.

3.1 Data Confidentiality

The cryptographic techniques are used in order to guarantee the secrecy of the data that is saved. In this method, the data will be encrypted before being sent to the cloud storage service. This will allow the secrecy of the data to be protected both during transmission and while it is being stored. On the basis of the key that is used, cryptographic methods may be broken down into two distinct categories: symmetric key cryptography [10] and asymmetric key cryptography [11]. [10] and [11] respectively. A symmetric key is faster than an asymmetric key and requires fewer computational resources. In general, symmetric keys are used to encrypt data, while asymmetric keys are employed for the process of key distribution. The use of cryptographic techniques to guarantee user privacy brings up a number of issues that need to be resolved, including: the distribution of the secret key; data dynamics, including the insertion, modification, and deletion of data; the searching for required data; user revocation; and the resolution of the issue of how to fix accountability of users. A lot of researchers have developed different strategies in order to protect the privacy of the data. According to the research that Kamara et al. intended to use AES to encrypt the data in order to maintain its secrecy and searchable encryption in order to encrypt the index in order to make searching through the data more accessible. In the work [12] Zarandioon at el. purposes Attribute Based Hierarchical Key Updating system (AB-HKU), which protect the secrecy of data using a Key-Policy Attribute-Based encryption technique. In the article [13], Sandeep and his colleagues employ a numeric number to describe the amount of secrecy that is necessary based on the SR (Sensitivity Rating) value. The author suggests using SSL, which stands for secure socket layer, to encrypt both the data and the index. In [14] Tang at el. aim of using symmetric key (such as AES) to encrypt data, and the key of symmetric, referred as the data key, is encrypted using blinded RSA (or Blinded Decryption [15]) to guarantee confidentiality via a hierarchy of key encryption and decryption processes. In [16], Jaberi at el. purpose to use advanced encryption standard (AES) and RSA-based partial homomorphic encryption method, AES to encrypt the Data, and RSA-based PHE is used to encrypt AES encryption keys.

As a result of the fact that these strategies consider more than one aspect of security, we will discuss them in more depth in section number 4.

3.2 Data Integrity Protection:

It is necessary to secure the data's integrity both while it is being sent and when it is being stored. It is possible for it to be compromised as a result of illegal changes, additions, or deletions to the data. A cryptographic method may be employed, not only to protect the privacy of the data but also to keep the data's integrity intact. The employment of cryptographic methods may be expensive if the data that has to be safeguarded is not very sensitive. This is because the encryption of data requires not just time but also the usage of computer resources. Message Authentication code, or MAC, may be used to guarantee merely integrity, but a digital signature can be used to guarantee integrity, non-repudiation, and authentication of data that has been transferred or stored. Before uploading a file to the server, the owner of the data must first create a MAC and save it on the local machine. In order to ensure that the data has not been tampered with, the data owner will compute the MAC after downloading the file from the server and then compare it with the value that was previously calculated; if there is no difference, the file may be considered to be unchanged. If the data is accessible to a large number of users, the MAC may be saved with the data; but, in order to prevent its disclosure, the MAC must be encrypted. Any combination of the public key and the private key may be used for encryption and decryption. Digital Signature is based on the principles of public key cryptography, which employs two keys: the public key and the private key. The key that is exposed to the general public is called the public key, while the key that is kept a secret is called the private key. If a communication is encrypted using a private key, then anybody may verify the message's integrity by decrypting it with the associated public key. If someone tamper the signature while it was being sent or stored, the signature would no longer verified correctly and would be invalid. Since the message could be lengthy, encrypting the whole thing would increase the size of the message by a factor of two, use up a significant amount of bandwidth and storage space, and take up a lot of processing power. Since the public key is cumbersome and time-consuming to generate, just the message digest is encrypted rather than the whole

thing [17]. Due to the fact that digital signatures are slower than MAC, they are only employed in situations when authentication, non-repudiation, and integrity are necessary, or in situations where there is no shared secret. The researchers have come up with a variety of different strategies in order to guarantee the honesty of the communication. If a user has write permission, [12] Zarandioon at el. states that they may use AB-Sign to sign the data, and readers are required to authenticate the writer's signature to guarantee that the data was produced or edited by an authorized writer. In [13] Sandeep at el. intended to make use of MAC in order to guarantee the accuracy of the data. If the user wishes to verify the file's integrity, he will compute the MAC and compare it to the value that was precalculated. If there is no change detected in the MAC, this indicates that the file's integrity has been maintained. In this scheme, the MAC will be calculated by the owner of the data using a secret key, and the file will be uploaded along with the MAC value. In [18] Wang at el. homomorphic token and distributed erasure-coded data were used in order to guarantee the data's integrity and locate the offending server. As stated in the article [14] Tang at el. employs HMAC signature to secure the integrity of the data; the HMAC signature is kept with the files; when a user downloads a file, the user must first check the validity of the HMAC signature; only if the signature is valid file will be decrypted. Wang at el incorporated a homomorphic linear authenticator with a method called random masking in their work [19], which was done to secure the integrity of data. In the work [20], Lifei at el. proposed to use Merkle hash tree [21] to safeguard the integrity of the data, which is built in the form of a binary tree and has a goal to utilize hash values of genuine data values as each leaf of the tree. In [16] Jaberi at el. utilizes the hash value to verify the integrity of the data before storing it, the client application portal (CAP) will compute the hash value, and then transmit it to the integrity checking service so that it can be used to validate the data's integrity. In [22] Wang at el. intention to affix a signature to each block of data; initially, each block of data will be signed by the data owner; once a block of data has been updated, it will be signed by the new user signature. The data's integrity may be verified with the use of signatures.

3.3 Data Availability

When it comes to storing data on the cloud, data availability is another worry. There are a lot of things that may go wrong and result is data not being accessible, such as a loss in communication, a financial problem for the CSP, a fire, an earthquake, or a flood. In the event that this failure occurs, it is assumed that the data stored on the cloud server would still be accessible in accordance with the specifications of the SLA. Researchers have devised a variety of cryptographically based strategies in order to guarantee the resource's availability. These schemes are either private or public verifiable, and their foundation is proofs of retrievability (PoRs) or proven data possession (PDP). PoRs can repair tiny errors by using an error correcting code, and it can identify huge corruption by using spot checking, while PDP just checks the availability of files, which means it detects only corruption and does not use an error correcting code. PoRs can also detect massive corruption using spot checking. In [23] Ateniese at el. designed a system that can offer probabilistic confirmation that a third party has a data file without the need to actually retrieve the information. This protocol makes use of tags that are homomorphic and verifiable. The owner of the data will pre-compute the tag to be used for each file block, after which they will store both the tag and the file on the server. In the event that the owner of the data decides at a later time that he wants to prove his ownership of the data stored on the server, he must first choose a random set of file blocks. The server will then use these blocks and the tags associated with them to construct proof of possession. In [24], Juels at el purposed another scheme for large files that was referred to as "Proof of Retrievability" (PoR). This scheme uses distinguished blocks that are called sentinel, and they are hidden among the regular file blocks. Since the regular file block and the sentinel are both encrypted together, the server can not differentiate between the regular and the sentinel block. The user will utilize Key to check the retrievability of the file by making use of the Challenge and response protocol. Due to the fact that each task requires certain sentinel blocks to complete, this strategy can only handle a limited amount of challenges. According to Shacham [25], at el. devised two Proof-of-Responsibility Schemes, one utilizing BLS [26] signature and the other using pseudo random function (PRFs). The first method has the shortest query and answer with public verifiability, while the second strategy has the shortest response with private verifiability. Both schemes were invented by the same person.

3.3 Access Control

Controlling who has access to the data is still another problem that is connected to the safety of the data. A cloud server is responsible for the storage of a substantial volume of data as well as a user authorization list. Because each user on the server accessed the data for a unique reason, they all need a unique set of access permissions. On the same data, some of them are only permitted to read it, while others can have the ability to write on it. It is necessary to have a security mechanism that will regulate who has access to the data. This data access control may either be coarse grained or fine grained. Coarse grained data access control operates on bigger data chunks, while fine grained data access control operates on smaller data chunks. The employment of cryptographic techniques is possible in order to permit access on both a fine and coarse grain level. The author of the aforementioned piece of written work [27] intended to combine KP-ABE [28], PRE (Proxy Re-Encryption) [29], and Lazy re-encryption [30] in order to create safe, scalable fine-grained access control on the data that was outsourced and stored in the cloud. In this particular method, KP-ABE is used, which assigns an access structure based on the characteristic. The data included in the file will be encrypted using a certain attribute set, and the user's decryption key will be connected with the access structure. When an attribute connected with data is satisfied by the Decryption key access structure, it becomes possible to decode the data. With PRE, the majority of the computational work may be sent to a cloud server where it will be processed without the data being shared. In [31] Kamara at el. Access control is one of the primary attributes that utilizes attribute-based encryption (ABE) . The unique key that is used to encrypt the data is encrypted with ABE. In [14], Tang at el uses attribute-based encryption to provide fine-grained access control of data. It employs a hierarchy of keys, with data key being used to encrypt data, control key being used to encrypt data key and being held by the key manager, and access key being held by the FADE client. Control key and access key are both based on attribute-based encryption (ABE). In [32], Liu at el combined time with ABE and PRE. Data is associated with access structure and access time. Each user is associated with a set of attribute and eligible time period, which will define the period of validity of user access right. Data is also related with access structure and access time.

[4] TECHNIQUE USED BY RESERCHERS TO ENSURE DATA SECURITY

A number of researchers have purposed a solution to assure confidentiality, integrity, and availability of data together with the access control. This was done in order to safeguard the data that is stored in the cloud. This section has provided some coverage of the works that researchers have carried out. We have tried to include works that are either widely referenced by other scholars or that have been published relatively recently

4.1 Provable data integrity of cloud storage service with enhanced security in the internet of things using erasure-coded hierarchical log structure and homomorphic tags

The researchers He, J.; Zhang, Z. at el. [33] made use of cloud services and came up with a plan to facilitate the updating of several data blocks at the same time. As a result, we were able to overcome the efficiency barrier. In order to facilitate

the delayed updating of numerous blocks and the retrievability of data, the technique used an erasure-coded hierarchical log structure. In addition, homomorphic tags are used so that the quantity of data transfers may be decreased, hence improving the efficacy of data updates. Nevertheless, the outcomes of their plan demonstrated that there would be a significant amount of computational work. The increasing prevalence of information technology has led to an increase in the pace at which data storage is used. The use of cloud computing has helped to speed up this expansion, but it does have drawbacks in terms of users' privacy and safety. The verification of the integrity utilizing public key infrastructure has resulted in an increased security risk as well as an increase in the cost of computation.

4.2. Cloud-based storage protected by cryptography

In [31] Kamara at el. uses a high-level architecture to safeguard data in cloud environment. The writers have considered two different possible outcomes, the first of which is consumer architecture, and the second is enterprise architecture. In consumer architecture, a secure communication is accomplished between two users and the cloud. In enterprise architecture, data is exchanged between two organizations and the cloud service provider. One organization is the data owner, while the other organization is the data user. In consumer architecture, a secure communication is achieved between two users and the cloud. Both scenarios make use of the same fundamental component, which consists of a Data Processor (DP), a Data Validator (DV), and a Token Generator (TG). All of these components are situated at the location of the data owner. When data has to be saved, it is first processed by DP, which creates an index and encrypts the data using a symmetric encryption scheme (Extended Advanced Encryption Standard, or Exp AES) using a secret key. Index will be encrypted using searchable encryption, and the authors have addressed many various ways to searchable encryption, such as SSE [34, 35, 36,37], ASE [38], ESE [39], and MSSE [40], all of which have distinct characteristics and may be employed appropriately. Index will be encrypted using searchable encryption. The confidential key has been encoded using ABE [41,42,43,44] in accordance with the prescribed access policy. Last but not least, this approach encodes the index as well as the encrypted data in such a manner that the data verifier may verify the data's integrity by utilizing the proof of storage.

4.3 Secure data exchange and data leakage detection in an untrusted cloud

D. Ulybyshev at el. [45] presents an approach for privacy-preserving data sharing, data leakage detection and prevention that makes use of access control that is based on roles and attributes for data exchange across services. These services include services that are housed in environments that are not trusted. Active Bundles (AB), whose contents include key-value pairs whose values are stored in encrypted form, metadata, access control rules, and a policy enforcement engine, are used by the technique. The active bundle approach ensures the data's secrecy and integrity while also shielding it from the prying eyes of cloud administrators who may have nefarious intentions. The data leakage identification technique was shown to incur a computational overhead of 60.8% based on the results of the implementation.

4.4 K2C: cryptography cloud storage with lazy revocation and anonymous access

According to the findings of the study [12] Zarandioon at el. developed a plan they call k2C (key to Cloud), which is designed to protect the data that is kept in the cloud. K2C is made possible by using a key Updating Scheme known as AB-HKU (Attribute Based - Hierarchical key Updating) and a signature scheme known as AB-SIGN (Attribute Based - Signature).

The K2C protocols is between the root user, the end user (Reader or Writer), and cloud providers. The root user is responsible for assigning access privileges to the end user. A user key will often have a validity term built into it so that access privileges may be revoked from end users. Three different repositories are used by the K2C protocol.

Meta data store, all meta data that is associated with the hierarchies and the data objects is stored in the meta data store.

Data Store: This feature allows you to save the real data item.

Key Store: This is where all read/write keys for end users are saved

This protocol may operate in four different modes, which are read, write, delegation, and revocation respectively. When the end user is in the Write mode, they are able to write into certain data objects. End users are able to get individual data objects from the data store while operating in the Read mode. Through the use of delegation, a user may give another user some of the access privileges that he has. Revocation is a method that may be used to remove a user's access to a certain directory or data item.

4.5 Practical attribute-based encryption: Outsourcing decryption, attribute revocation and policy updating

A CP-ABE approach is presented by Liu et al. [46] as a means of lowering the computing cost of heavy decryption at the user end, which rises in proportion to the level of difficulty of the access policy. This technology made decryption outsourcing, revocation attributes, and policy updating possible even as user attributes were being modified. The efficiency of the suggested system is assessed in terms of overhead for storage and processing power, however it lacks in terms of privacy protection. The rigorous evaluations are done in order to evaluate the efficiency of the system that is suggested.

4.6 A combined approach to ensure data security in cloud computing

As mentioned in the article [13] Sandeep at el. developed a system that provides the data owner with the option to rate the confidentiality, availability, and integrity of their data on a scale from 1 to 10, and then based on these values, developed a Sensitivity Ratio (SR). The author had the intention of dividing the cloud storage space into three sections, each of which would have a different access level: S3 (Public), S2 (Private), and S1 (Limited). The SR value is used to identify the partition that will be responsible for storing the data. If the SR value is less than or equal to three (3), then the public partition will be used. If the SR value is more than three (3) but less than or equal to six (6), then the private partition will be used. If the SR value is above six (6) but less than or equal to ten (10), then the limited access partition will be used.

The procedure consists of two stages: the storage phase and the retrieval phase. During storage, 128-bit SSL is used to encrypt the data. Along with the encrypted data, a MAC is also kept so that it can be checked to see whether the data was received at the server in the right format. This allows the store to give search capabilities to the data. If a user wishes to access the public area during retrieval, no authentication is necessary, and the user may download and decrypt the data. On the other hand, authentication is required to access the private and restricted sections of the database. If the user has been given permission to view the restricted portion, he will also have permission to access the private section.

4.7 Toward Secure and Dependable Storage Services in Cloud Computing.

In [18] Wang at el. developed a system that enables users to check the cloud storage provider's claims about the data's integrity. In order to do this, the author made use of homomorphic tokens and data with distributed erasure data. Prior to the data being stored on the cloud servers, the homomorphic function is used in order to calculate tokens. If a user wants tomake sure that the data is accurate, he should verify the cloud server storage integrity by sending a set of randomly generateddata block indices to the cloud server. When the cloud server receives the data block indices, it should compute a token andsend it back to the user. If the token computed by the server matches the value that the user has computed, this indicates that the integrity of the data has been checked and found to be correct. In the event that the server's integrity is not validated,this approach will also identify the server that is acting improperly. This technique is particularly successful against malicious data modification attacks, Byzantine failure attacks, and server colluding attacks. It supports dynamic data update,delete, and append operations.

4.8 Privacy-Preserving Public Auditing for Secure Cloud Storage.

A titled "Privacy-Preserving Public Auditing for Secure Cloud Storage" is presented by the authors of [19]. With the help of this system, an audit of the data's integrity was performed on the cloud server. Due to the fact that TPA is unable to get any information on the content of the data, the confidentiality of the data is maintained. The inventor of this protocol employs the homomorphic linear authenticator [28] in conjunction with the random masking approach. Because the system uses randomizing, the TPA is unable to reveal data; hence, the TPA does not have all of the information that is required to generate the right group of linear equation.

The operation of these protocols is described below.

1. The user is responsible for generating both public and private parameters.

2. Each file block has its own unique code, which serves as both an authenticator and a file tag.

3. The cloud receives the file block codes together with the file blocks.

4. Challenge messages are sent from TPA to CSP. These messages provide the positions of the blocks that are going to be reviewed during the audit.

5. In addition to this, CSP applies a mask and performs a linear combination of the blocks that have been chosen. A unique PRF key should be used for each auditing, and the aggregate authenticator and masked combination of blocks should be sent to the TPA.

6. TPA will compare the aggregate authenticator that they have got with the one that they have received from CSP.

4.9 Security and privacy for storage and computation in cloud computing

The authors Wei et al. presented a protocol in the article [20] that would give security to both the data and the computation. The bilinear pairing algorithm is used to produce the key that is required by the participating entity user, the cloud, and the third party (Verification Agency). The information is then digitally authenticated by a reliable third party after being segmented into m different portions. After being encrypted using the session key, the data and signature are then sent to the cloud service provider for storage. The data is first decrypted on the cloud server, and then the signature is verified. If both of these steps are successful, the data is then saved on the cloud server.

The author implements a Merkle Hash tree for the purpose of ensuring the safety of the computational process. In order to validate the correctness of the results of the calculation, an independent and reliable third party will rebuild the Merkle tree..

4.10 Secure overlay cloud storage with access control and assured deletion

In [14] Tang at el. developed a plan known as FADE, which offers access control as well as guaranteed removal of the outsourced data. This method utilizes a key management operation to limit who may access files and ensures that files are deleted completely. In this system, each file has its own data key and access policy associated with it. The data key is a symmetric key that is used to encrypt files, and the control key that is linked with each policy is what encrypts the data key. Each policy also has its own unique control key. The key manager is responsible for maintaining control keys. The policy that is connected with the file will be revoked, and the control key that is associated with that policy will be withdrawn, in order to accomplish the goal of achieving guaranteed deletion of the file.

The fundamental activities of FADE are file uploading, downloading, and revoking policies.

File Upload

1. The data owner will transmit the policy pi to the key manager. The key manager will then produce two secret big RSA prime numbers, pi and qi, for each policy i, and calculate ni = pi qi for each policy.

2. The key manager will choose a Random RSA public and private control key pair, which will then be sent to the cloud. The di key will be kept by the key management.

3. The owner of the data should use the data key *k* to access file *f* and the control key *si* to access for *pi*.

4. The owner of the data is responsible for uploading it together with $p_i, \{ f \}_{k,} k_{si,} si^{ei}$ to the cloud server for storage.

File Download

1. The cloud server will provide the data owner the values $p_i, \{f\}_{k,} k_{si,} si^{ei}$.

2. The owner of the data selects a random number called R and blinds s_i^{ei} with r^{ei} and send to the key manger along with pi so that it may be decrypted.

3. Key manager decrypt s_i^{ei} r^{ei} and send back to the data owner.

4. The owner of the data should retrieve and unblind s_i.

5. Using s_i data owner get K and using K data owner obtain file F.

Policy Revocation

The Key manager delete (n_i, e_i, d_i), in order to revoke policy p_i, all of the files related with p_i are now unavailable. As a result, successful deletion of the file was accomplished.

4.11 Time-based proxy re-encryption scheme for secure data sharing in a cloud environment.

The authors of [32] propose a time-based proxy re-encryption technique for the goal of achieving fine-grained access control over data sharing in a group. This approach makes use of a mix of ABE and PRE. In contrast to other PRE-schemes, in which the user is required to be online in order to withdraw access permission and generate a new re-encryption key, in this scheme, to revoke access permission of a data, the author purpose to use time attribute which specify the time length for which user is permitted to access data. This allows the author to revoke access permission of a data. When the allotted amount of time has passed, the user access permission will be immediately and permanently removed by the CSP. The re-encryption key is generated with the use of a Master key that is known to both the owner of the data and the CSP. Rather of ensuring or auditing the integrity of the data kept on the cloud server, it only protects users' privacy and makes their data more accessible.

4.12 Data Integrity and Privacy Model in Cloud Computing

The author of [16] devised a plan to ensure the confidentiality and authenticity of the data that was saved. The model used four components i.e. Integrity checking service (ICS), Client application portal (CAP), Key management and storage service (KMSS), and Cloud storage service provider (CSSP). Before being uploaded to the server, the data are encrypted by CAP using AES, and the key is encrypted with RSA-based partial homomorphic encryption (PHE), which is then kept on the KMSS. A check for the data's integrity is performed using the calculated value of the data's hash before it is stored on the server by CAP.

4.13 Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing

According to the research published by Shucheng at el.[27] utilizing Key Policy- Attribute Based Encryption (KP-ABE), Proxy Re Encryption (PRE), and Lazy Re-Encryption, the authors devised a strategy for secure, scalable, and fine-grained data access control in cloud computing. Authors utilizes KP-ABE to provide fine-grain access control of the data file. Data files are connected with attributes, and access Policies are related with user secret keys. A combination of PRE and Lazy revocation is used by the author to handle user revocation. This allows the users to outsource the majority of the computationally difficult operation to the cloud server.

As a result of the data being encrypted using KP-ABE, confidentiality is preserved.

4.14 Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud

The author of Paper [22] proposes a system that is referred to as "Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud." This system is designed to be used for auditing the integrity of data that has been saved and for the administration of user revocations. In this configuration, one user inside the group acts as the group manager. A group manager has the authority to revoke user access if it is necessary. When a user's access is revoked, every data block that was previously signed by that user will be reallocated with a user key that already exists. For the Author purpose, either the signature of the group manager or a priority list, which includes every existing user ID listed in the order of re-signing priority, may be used. Alternatively, the priority list can be utilized. In the beginning, in order to maintain the reliability of the Shared Data, each data block will be signed by the user who is responsible for its modification. In order to verify the accuracy of the data, the author intends to employ block less verifiability, and the auditor will use linear combination of data blocks. In order to verify that the data is accurate, the author intends to employ the homomorphic authenticator [23]. In this particular technique, the auditor uses a linear combination of data blocks. That is, the auditor verifies the accuracy of the m' block using a challenge and answer protocol without knowing the m1 and m2 blocks.

4.15 PORs: Proofs of Retrievability for Large Files

In the article Juels at el. [24] uses a protocol known as proof of retrievability (POR) to confirm that a file is available on the cloud server. In the event that POR is successfully conducted, this indicates that the file may be completely recovered from the cloud server. POR employs sentinel, which is a randomly valued check block that is inserted in the file; the file is then encrypted. This is done so that availability may be guaranteed. The verifier must issue a challenge to the cloud server by indicating the position of the sentinel and requesting that the cloud server provide the value associated with the sentinel in order to complete the verification of the cloud server's stored file. If he removed certain sections of the file, then he probably also erased some sentinel, and in that case, it is doubtful that he would answer with the right sentinel value. The author additionally makes use of error correcting code in order to identify and fix any minor errors that may be present in the file.

5 Discussions

The concept of "cloud computing" refers to an emerging, cost-effective form of network-based computing that has gotten an immense reaction from the many communities of computer users, ranging from academia to business. Data is the most important component of any computer-based system; for example, in cloud computing, data is transported from the location of the data owner to a distant site, which does not fall under the administrative authority of the data owner. Because of this feature of cloud computing, there is a growing worry about the safety of the data that is housed. Confidentiality, integrity, availability, and safe access to the data are the different concerns about data security that have arisen.

In section 3 we covered these problems and the potential remedies that the researchers proposed. Researchers have studied the confidentiality of stored data in the articles [12-14,16,19,20,22,32]. They used both symmetric encryptions like (AES) and asymmetric encryption- Attribute based encryption scheme as instruments to assure confidentiality. Researchers in [13,14,18-20,26,29] purposed solutions based on MAC and digital signature in order to assure the integrity of the data that was being kept. MAC ensures just the integrity of the data, while digital signature ensures the integrity, authenticity, and non-repudiation of the data. Another problem, namely the availability of data, has been taken into consideration by the researcher in the articles [13,18,26,24,29]. POR and PDP are the two-key works in this respect. POR may correct tiny errors in addition to ensuring the availability of the data, while PDP just ensures the availability of the data. POR can correct small errors in addition to ensuring the availability of the data. Another aspect of physical safety that has been looked at for the purpose of this article is access control. This topic was discussed by the researchers in [12-14,32]. When it comes to controlling secure access, the majority of researchers have turned to attribute-based encryption methods like KP-ABE.

Despite the fact that experts from both academia and business are devoting a great deal of time and energy to their work, there are still many problems that have not been solved. Only one or two concerns have been kept in mind throughout the whole of the study that has been carried out by the researcher. Integrating all of these different techniques to ensure data safety is not practical. The performance of the cloud computing services is another significant concern, since these services may be accessed by a wide range of devices, and many of these devices have limited resources in terms of their processing power and memory. Therefore, there is a need to design comprehensive and integrated solutions that must cover the majority of the concerns that are brought up by the storing of data in the cloud. The security concerns that have been identified and the strategies and procedures that are used to address are outlined in Table1.

Table. 1.Concerns method used for acloud. Security and the researcher secure

Author's	Title of the Papers	Security Aspects				Methods (Techniques)
		C	I	A	Access Control	
He J. at el.	Provable data integrity of cloud storage service with enhanced security in the internet of things		√	√		erasure-coded hierarchical log structure and homomorphic tags
Sandeep at el.	A combined approach to ensure data security in cloud computing	√	√	√	√	A breakdown of the information into three groups: Encryption that can be searched, Secure Sockets Layer (SSL) for data encryption, and the MAC protocol for data security
Kamara at el.	Cryptographic cloud storage	√	√		√	Attribute Based Encryption (Key), symmetric encryption(data), Searchable encryption (Index),

[6] CONCLUSIONS

cryptography as a technique to safeguard the data, whether it be for auditing requirements, confidentiality requirements, integrity requirements, availability requirements, or secure access requirements. The majority of the studies only concentrate on a subset of the security challenges and do not consider the required processing power. Some of these devices have limited memory and compute capacity, which is why it is necessary to concentrate on the computational power needed by those techniques. Cloud computing may be accessible through a variety of devices, and some of these devices have these limitations. In the future, we think it's possible that some novel approaches will be used, to provide full integrated security solutions while using less computer power and memory.

REFERENCES:

[1] Coppolino, L. &D'Antonio, Salvatore &Mazzeo, Giovanni. (2016). Cloud security: Emerging threats and current solutions. Computers & Electrical Engineering. 10.1016/j.compeleceng.2016.03.004.

[2] D. Zhe, W. Qinghong, S. Naizheng and Z. Yuhan, "Study on Data Security Policy Based on Cloud Storage," 2017 ieee 3rd international conference on big data security on cloud (bigdatasecurity), ieee international conference on high performance and smart computing (hpsc), and ieee international conference on intelligent data and security (ids), 2017, pp. 145-149

[3] A. Hussain, C. Xu, and M. Ali, “Security of Cloud Storage System using Various Cryptographic Techniques,” International Journal of Mathematics Trends and Technology (IJMTT), vol. 60, no. 1, pp. 45–51, 2018.

[4] G. Jain and A. Jaiswal, “Security Issues and their Solution in Cloud Computing”, Concepts journal of applied research(CJAR), vol. 02,no. 03, pp. 1-6, 2018.

[5] Amazon.com. Amazon S3 Availability Event: July 20, 2008, http://status.aws.amazon.com/s3-20080720.html. July 2008.

[6] Wilson S. Appengine Outage, http://www.cio-weblog.com/50226711/appengine_outage.php, June 2008.

[7] Krebs B. Payment Processor Breach May Be Largest Ever, http://voices.washingtonpost.com/ securityfix/2009/01/ payment_processor_breach_may_b.html, Jan. 2009.

[8] Dimitrios Z, Dimitrios L. Addressing cloud computing security issues. Future Generation Computer Systems. 2012; Volume 28(3):583-592.

[9] http://en.wikipedia.org/wiki/Certificate_authority Accessed on 24.04.15

[10] Stallings W. Cryptography and Network Security, Principle and Practice. 6th Edition,'Pearson Education.2014: 28-31.

[11] Stallings W. Cryptography and Network Security, Principle and Practice. 6th Edition, 'Pearson Education. 2014:256-262.

[12] Zarandioon S, Yao D, Ganaphthy V. K2C: cryptography cloud storage with lazy revocation and anonymous access. Securecomm, 2011

[13] Sandeep KS. A combined approach to ensure data security in cloud computing. Journal of Network and Computer Applications. 2012; Volume 35(6):1831-1838.

[14] Yang T, Patrick PCL, John CSL, Radia P. Secure overlay cloud storage with access control and assured deletion. IEEE Transactions on Dependable and Secure Computing. 2012; Vol. 9(6): 903-906.

[15] Perlman R. File System Design with Assured Delete. Proc. Network and Distributed System Security Symp. ISOC (NDSS). 2007.

[16] Mohammed Faez Al-Jaberi, Anazida Z. Data Integrity and Privacy Model in Cloud Computing. International Symposium on Biometrics and Security Technologies (ISBAST), IEEE. 2014

[17] https://technet.microsoft.com/en-us/library/cc962021.aspx Accessed on 20.03.18

[18] Cong W, Qian W, Kui R,Ning C and Wenjing L. Toward Secure and Dependable Storage Services in Cloud Computing. IEEE TRANSACTIONS ON SERVICES COMPUTING. 2012; VOL. 5.

[19] Cong W, Sherman SMC, Qian W, Kui R and Wenjing L. Privacy-Preserving Public Auditing for Secure Cloud Storage. IEEE TRANSACTIONS ON COMPUTERS. 2013; VOL. 62(2).

[20] Lifei W, Haojin Z, Zhenfu C, Xiaolei D, Weiwei J, Yunlu C, Athanasios, Vasilakos. Security and privacy for storage and computation in cloud computing. Information Sciences. 2014; Volume 258: 371-386.

[21]Merkle R. Protocols for public key cryptosystems. in: IEEE Symposium on Security and Privacy, Oakland, California, USA, April. 1980.

[22] Boyang W, Baochun L, Hui L. Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud. IEEE TRANSACTIONS ON SERVICES COMPUTING. 2015; VOL. 8(1).

[23]Ateniese G, Burns R, Curtmola R,Herring J,Kissner L,Peterson Z,Song Z. Provable data possession at untrusted stores. in: Proc. of ACM CCS, Alexandria, VA.(2007)

[24] Juels A,Burton J, Kaliski J. Pors: proofs of retrievability for large files, in: Proc. of ACM CCS, Alexandria, VA, October 2007.

[25] Shacham H, Waters B. Compact proofs of retrievability. in: Proc. of Asiacrypt, Melbourne, Australia. 2008.

[26] Boneh D,Lynn B, and Shacham H. Short signatures from the Weil pairing. J. Cryptology. 2014; Vol 17(4):297-319.

[27] Yu. S, Wang C, Ren K, Lou W. Achieving secure, scalable, and fine-grained data access control in cloud computing. in: Proc. of IEEE INFOCOM, San Diego, CA, March 2010.

[28] Goyal V, Pandey O, Sahai A, and Waters B. Attribute-based encryption for fine-grained access control of encrypted data. in Proc. of CCS'06. 2006.

[29] Blaze M, Bleumer G, and Strauss M. Divertible protocols and atomic proxy cryptography. in Proc. of EUROCRYPT '98, 1998.

[30] Kallahalla M, Riedel E, Swaminathan R, Wang Q and K. Fu. Scalable secure file sharing on untrusted storage. in Proc. of FAST'03, 2003.

[31] Kamara S, Lauter K. Cryptographic cloud storage. 14th International Conference on Financial Cryptography and Data Security, LNCS 6054, IFCA/Springer-Verlag.136−149. (2010)

[32] Qin Liu, Guojun Wang, Jie Wu: Time-based proxy re-encryption scheme for secure data sharing in a cloud environment. Information Sciences. 2014; Vol 258: 355–370.

[33] He, J.; Zhang, Z.; Li, M.; Zhu, L.; Hu, J. "Provable data integrity of cloud storage service with enhanced security in the internet of things". IEEE Access 2018, 7, 6226–6239.

[34] Bardin J, Callas J, Chaput S, Fusco P, Gilbert F, Hoff C, Hurst D, Kumaraswamy S, Lynch L., Matsumoto S, O'Higgins B, Pawluk J, Reese G, Reich J, Ritter J, Spivey J, Viega J. Security guidance for critical areas of focus in cloud computing. Technical report, Cloud Security Alliance. 2019.

[35] Goh EJ. Secure indexes. Technical Report 2003/216. IACR ePrint Cryptography Archive (2003), http://eprint.iacr.org/2003/216

[36] Chang Y, Mitzenmacher M. Privacy preserving keyword searches on remote encrypted data. Springer, Heidelberg.2005; vol. 3531,: 442–455.

[37] Curtmola R, Garay J, Kamara S, Ostrovsky R. Searchable symmetric encryption: Improved definitions and efficient constructions. In: Juels, A., Wright, R., De Capitani di Vimercati, S. (eds.) ACM Conference on Computer and Communications Security , New York. 2006; 79–88.

[38] Boneh D, Crescenzo D, Ostrovsky R. Persiano G. Public key encryption with keyword search. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 506–522. Springer, Heidelberg (2004)

[39] Bellare M, Boldyreva A., O'Neill A. Deterministic and efficiently searchable encryption. In: Menezes, A. (ed.) CRYPTO, Springer, Heidelberg, LNCS. 2007; vol. 4622: 535–552.

[40] Curtmola R, Garay J, Kamara S, Ostrovsky R. Searchable symmetric encryption: Improved definitions and efficient constructions. In: Juels A, Wright R, De Capitani di Vimercati, S. (eds.) ACM Conference on Computer and Communications Security, New York. 2006; 79–88.

[41] Sahai A, Waters B. Fuzzy identity-based encryption. In: Cramer, R. (ed.) EUROCRYPT , LNCS, Springer, Heidelberg. 2005; vol. 3494: 457–473.

[42] Goyal V, Pandey O., Sahai A, Waters B. Attribute-based encryption for fine grained access control of encrypted data. In: ACM conference on Computer and communications security, ACM, New York. 2006; 89–98.

[43] Ostrovsky R, Sahai A, Waters B. Attribute-based encryption with non-monotonic access structures. In: ACM conference on Computer and communications security, ACM, New York. 2017;195–203.

[44] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption. In: IEEE Symposium on Security and Privacy, IEEE Computer Society, Los Alamitos. 2017; 321–334.

[45] D. Ulybyshev, B. Bhargava, and A. Oqab-Alsalem, ''Secure data exchange and data leakage detection in an untrusted cloud,'' in Applications of Computing and Communication Technologies. Singapore: Springer, 2018, pp. 99–113.

[46] Z. Liu, Z. L. Jiang, X. Wang, and S. M. Yiu, ''Practical attribute-based encryption: Outsourcing decryption, attribute revocation and policy updating,'' J. Netw. Comput. Appl., vol. 108, pp. 112–123, Apr. 2018.