IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

Review Paper on Security in Cloud Computing

Sharad Srivastava[1], Manjula R[2]

School of Computer Science and Engineering, VIT University, Vellore, India[1]

Associate Professor, School of Computer Science and Engineering, VIT University, Vellore, India[2]

Abstract: Every day the data that we produce is growing at an exponential rate and the growth of which is only going to increase with time. In such a scenario the transfer, security and storage become factors of critical importance. A big step in resolving these issues was the development of cloud computing, but development of such a large and complex system brought about its own concerns mainly in terms of security. Remote data access control is of crucial importance in public cloud. Based on its own inclinations, the data owner predefines the access policy. When the user satisfies the data owner's access policy, it has the right to access the data owner's remote data. To improve flexibility and efficiency of remote data access control, attribute-based encryption (for short, ABE) is used to realize the remote data fine-grained access control. For the basic systems with low resources, secure outsourced decryption is a very useful technique. In the real application scenarios, the user's attributes are usually managed by many authorities. This paper is intended towards discussing the issue and single point of failure in access control for cloud infrastructure and suggesting a solution for the same.

I. INTRODUCTION
II.

Cloud computing is the practice of using interconnected network of servers and storage devices to host an array of service which include but are not limited to data backup, online services, etc. Cloud computing grew exponentially with the development in technology, the more technology became a household item the more data it produced which created an increase in the demand of resources to manage this data.

Cloud computing has attracted great attention of both academia and information technology industry. Built on the architecture of parallel and distributed computing, this new computing paradigm possesses numerous advantages including low cost, high-efficiency, flexibility and scalability. From the bottom layer to the top, cloud computing can be divided into three delivery models, namely infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS) [1]. Nowadays, there are many kinds of cloud service systems providing services via the Internet, such as Amazon's EC2, IBM's Blue Cloud, Google App Engine, Microsoft's Azure, etc. With the envisioned advances of cloud service systems, enterprise users can access to the resource on the cloud anytime and anywhere, without the need to manage the underlying hardware/software systems.

Without any doubt, DATA is an extremely important asset for all organizations, especially for enterprise users. But this deserves special attention in the era of cloud computing. Different from the conventional local storage, cloud computing stores data on remotely located servers via the Internet. The data owner needs to upload his/her own data into the cloud server, and authorized users can retrieve the data from the cloud. In cloud computing, it is the semi-trusted Cloud Service Provider (CSP) that manages the cloud and all data on the cloud [2], and as a result, data confidentiality is at the top of the list of concerns on cloud computing [3].

While encryption can provide data confidentiality, classic encryption methods alone cannot meet another requirement in many applications of cloud storage, namely flexible and fine-grained data access control [4]. With the development of group-oriented applications, access control is confronted with the requirement of different and flexible access privileges.

Along with the development of cloud computing, more and more corporations and individuals upload their data to public cloud server (for short, PCS). They will delegate PCS to store and manage their remote data. By using public cloud, the corporations and individuals are relieved of the burden of storage management, universal data access with independent geographical locations, capital expenditure on hardware, etc. Public cloud can provide data storage service, computation service, etc. Thus, cloud computing attracts all kinds of clients.

For the low-capacity terminals, outsourced computing makes them efficiently access the remote data. Since PCS takes part in the decryption process, the dishonest PCS must be defended. Verifiable outsourced decryption can be used to defend the dishonest PCS. At the same time, to efficiently protect the remote data confidentiality, the uploaded data will be encrypted by combining the distributed ABE encryption and symmetric encryption. For the real scenario, the

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

users' attributes are managed by many different authorities. Thus, the distributed (i.e., multi authority) ABE with verifiable outsourced computing can be used for the distributed fine-grained access control in public cloud.
Despite many advantages of cloud storage, there remain various challenging obstacles, among which, privacy and security of users' data have become major issues, especially in public cloud storage [5], [6]. Traditionally, a data owner stores his/her data in trusted servers, which are generally controlled by a fully trusted administrator. However, in public cloud storage systems, the cloud is usually maintained and managed by a semi-trusted third party (the cloud provider). Data is no longer in data owner's trusted domains and the data owner cannot trust on the cloud server to conduct secure data access control.

Therefore, the secure access control problem has become a critical challenging issue in public cloud storage, in which traditional security technologies cannot be directly applied.

In the real environment, the user's attributes are managed by different authorities, e.g., nationality, academic title, profession, etc. Thus, every user has many attribute secret keys which come from different authorities. When the user uses the low-capacity terminals, e.g., mobile phone, etc, the user has to use the outsourced computation. When PCS takes part in the outsourced computation, the dishonest PCS may send incorrect response to the user in order to save its own computation overhead. Of course, the incorrect response may come from the system errors, faulty attack, etc. Generally speaking, the incorrect response exists in the real environment.

Thus, we have to study the verifiable outsourced decryption algorithm. Verifiability can guard against the dishonest PCS or system errors. It is necessary to study the distributed fine-grained access control protocol with verifiable outsourced decryption. Let us consider the following scenario. In order to save the expenses, media corporations would like to store their television programs on PCS. PCS will be responsible for the uploaded data security, e.g., integrity, availability.

To protect the media corporations' benefits, the stored television programs will be encrypted before they are uploaded to PCS. In order to make money, the media corporation will design the concrete access control structure. When the user pays money to the media corporation, he will be given some secret information by the media corporation. By owning the secret information, the user is authorized and has the right to access and enjoy the remote media programs. When the user accesses the exceptive programs, it is important to preserve the identity privacy of the user. The user does not want to reveal its identity to other users, even to PCS. For example, when the user would like to enjoy adult programs, murder programs, he hopes to enjoy them anonymously. Even if the user would like to enjoy the other programs, he also hopes to enjoy them anonymously. Thus, it is necessary to study anonymous distributed fine-grained access control protocol with verifiable outsourced decryption in public cloud.

A. Cloud Computing Types
1) Private Cloud

Private cloud can be characterized as a cloud infrastructure that is worked for the sole utilization of a solitary association and is overseen either inside or by an autonomous outsider, and facilitated either inside or remotely. Undertaking a private cloud venture requires a noteworthy level and level of engagement to virtualize the business condition, and requires the association to rethink choices about existing assets. When it is done well, there is great potential for enhancing business, yet every additional progression in the venture likewise raises the related security issues that must be routed to forestall conceivable vulnerabilities. Self-run server farms are by and large capital concentrated.

2) Public Cloud

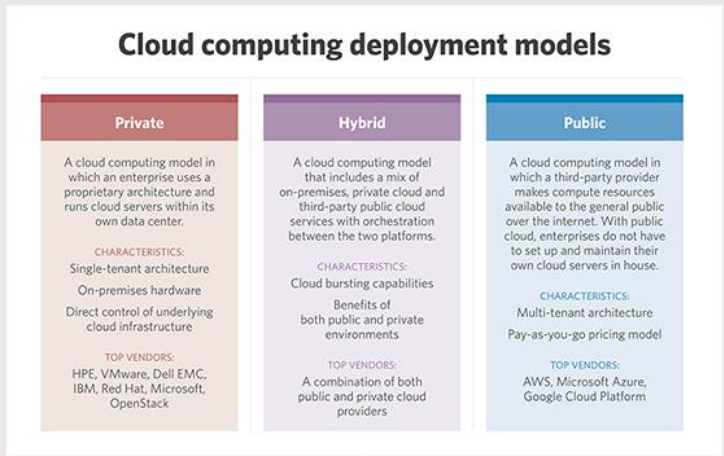
A cloud is known as a "public cloud" when the administrations are rendered over a system that is open for public use. Public cloud administrations might be free. For the most part there are either little or no distinction while thinking about a public cloud engineering and a private cloud design, security thought might be generously extraordinary for administrations that are made accessible by a specialist co-op for an open gathering of people and when correspondence is affected over a non-trusted network.

3) Hybrid Cloud

Hybrid cloud is a mix of numerous clouds that are particular elements yet are joined together in a system, and offer the advantages of different framework models. Hybrid cloud can likewise mean the capacity to associate collocation, oversaw and additionally committed administrations with cloud assets. Such a cloud benefit goes past detachment and supplier limits making it so it can't be essentially placed in one class either private, open, or group benefit.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

It enables one to broaden either the limit or the ability of a cloud benefit, by total, coordination or customization with another cloud benefit.



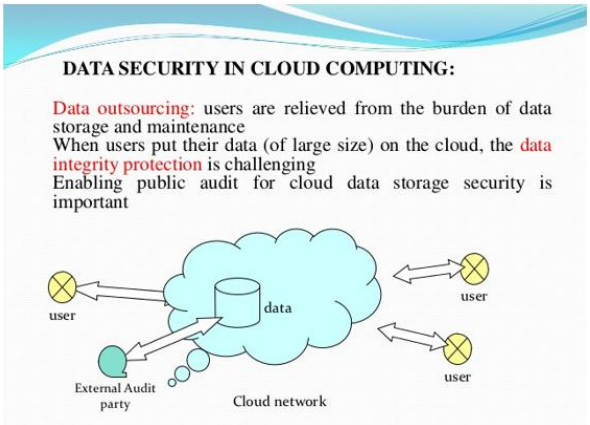
1.1 different models of cloud computing

4) Security in Cloud

In view of research done by the Cloud Security Alliance, the biggest dangers in the cloud are "Shaky Interfaces and API's", "Information Loss and Leakage", and "Equipment Failure". In a cloud supplier stage being shared by various clients there might be a probability that data having a place with various clients lives on same information server. Data spillage may emerge by mix up when data for one client is given to other. Eugene Schultz, chief technology officer at Imagined Security, said that programmers are investing generous energy and exertion searching for approaches to as have this information be ordered via web crawlers (influencing the data open) to enter the cloud. Information produced from a huge number of organizations can be put away on expansive cloud servers, these information stores are defenseless against programmers who can hypothetically pick up control of tremendous stores of data through a solitary assault. A process called "hyper jacking". Some examples of this include the Dropbox security breach, and Cloud 2014 leak. Dropbox had been breached in October 2014, having over 7 million of its user's passwords stolen by hackers in an effort to get monetary value from it by Bit coins (BTC). By having these passwords, they are able to read private data as well.

There is the issue of legitimate responsibility for information. Physical control of the PC gear (private cloud) is more secure than having the hardware off site and under another person's control (open cloud). This makes an extraordinary motivating force for people in general distributed computing specialist co-ops to guarantee and organize assembling and keeping up solid administration of secure administrations.

Some independent ventures that don't have ability in IT security could find that it's more secure for them to utilize an open cloud. There is the hazard that end customers don't understand the issues included when stamping on to a cloud benefit (individuals as a less than dependable rule don't read the various pages of the agreement document, and basically click "Acknowledge" without examining). This is basic now that disseminated figuring is getting the opportunity to be notable and required for a couple of administrations to work, for example something like an individual associate.



1.2 Security in cloud computing

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

Generally private cloud is viewed as more secure with more elevated amounts of control for the proprietor, however open cloud apparently is more adaptable and requires less time and cash venture from the client. Effective search on scrambled information is additionally an imperative worry in cloud service. The cloud service ought not to know the question but rather ought to have the capacity to return the records that fulfill the inquiry. This is accomplished by methods for accessible encryption. The keywords are sent to the cloud encoded, and the cloud restores the result without knowing the real catchphrase for the inquiry. The issue here is, that the information records ought to have catchphrases related with them to enable the inquiry. The right records are returned just when searched with the correct keywords.

Security and protection insurance in cloud are being investigated by numerous scientists. Numerous holomorphic encryption strategies have been proposed to guarantee that the cloud can't read the information while performing calculations on them. Utilizing holomorphic encryption, the cloud gets cipher of the information and performs calculations on the figure content and returns the encoded estimation of the outcome. The client can decipher the outcome, yet the cloud does not realize what information it has worked on. In such conditions, the client must be able to check that the cloud returns revise comes about.

B. Access Control in Cloud

Access control in cloud is picking up attention since it is critical that exclusive approved clients approach legitimate administration. A colossal measure of data is being put away in the cloud, and quite a bit of this is touchy data. Care ought to be taken to guarantee access control of this sensitive data which can regularly be identified with health, critical reports (as in Google Docs or Dropbox) or even individual data (as in person to person communication).

There are extensively three kinds of access control:

- User Based Access Control (UBAC),
- Role Based Access Control (RBAC),
- Attribute Based Access Control (ABAC).

In UBAC, the entrance control list (ACL) contains the rundown of clients who are approved to get to information. This isn't possible in clouds where there are numerous clients. In RBAC, clients are characterized in view of their individual parts. Information can be gotten to by clients who have coordinating parts. The parts are characterized by the framework. For instance, just staff members and senior secretaries might have access to data but not the junior secretaries. ABAC is more extended in scope, in which users are given attributes, and the data has attached access policy. Just clients with legitimate arrangement of attributes, fulfilling the access approach, can get to the information.

For example certain records may be available by employees with over 10 years of research involvement or by senior secretaries with over 8 years' understanding. There has been some work on ABAC in clouds all these work utilize a cryptographic crude known as Attribute Based Encryption (ABE). The extensible Access Control Markup Language (XACML) has been proposed for ABAC in clouds. A territory where access control is broadly being utilized is healthcare.

Clouds are being utilized to store delicate data about patients to empower access to therapeutic experts, healing facility staff, specialists, and arrangement producers. It is critical to control the entrance of information so just approved clients can get to the information.

Utilizing ABE, the records are encoded under some entrance strategy and put away in the cloud. Clients are given arrangements of properties and relating keys. Just when the clients have coordinating arrangement of traits, would they be able to decode the data put away in the cloud. Access control is additionally picking up significance in online long range interpersonal communication where clients (individuals) store their own data, pictures, recordings and offer them with chose gatherings of clients or groups they have a place with.

A titanic measure of information is continually chronicled in the cloud, and quite a bit of this is delicate information. Using Attribute Based Encryption (ABE), the records are encoded under a couple of access methodology besides spared in the cloud. Customers are given arrangements of attributes and comparing keys. Exactly when the customers have coordinating arrangement of characteristics, would they have the capacity to unscramble the information saved in the cloud. Access control is in like manner picking up hugeness in online informal communication where clients store their own information, pictures, movies and offers them with chose gathering of clients they have a place. The work done gives protection safeguarding validated access control in cloud. Nonetheless, the researchers take a centralized methodology where a single key distribution center (KDC) disperses secret keys and attributes to all clients.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

Unfortunately, a single KDC is not just a single point of failure however troublesome to uphold due to the vast number of clients that are upheld in a nature's domain.
Multi-authority ABE principle was concentrated on in, which obliged no trusted power which requires each client to have characteristics from at all the KDCs. Access control in online social networking has been studied in such data are being stored in clouds. It is very important that only the authorized users are given access to that information. A comparable circumstance emerges when information is put away in cloud, for instance in Dropbox, and imparted to specific gatherings of individuals. It is sufficiently not to store the substance safely in the cloud however it may likewise be important to guarantee namelessness of the client.

For instance, a client might want to store some sensitive data yet does not have any desire to be recognized. The client might want to post a remark on an article, however does not need his/her identity to be uncovered. The client ought to have the capacity to demonstrate to alternate clients that he/she is a substantial client who put away the data without uncovering the character.

There are cryptographic conventions like ring marks, Mesh marks, group marks, which can be utilized as a part of these circumstances. Ring mark isn't a plausible choice for clouds where there are large number of users. Group marks expect the pre-presence of a group which might not be conceivable in cloud. Mesh marks don't guarantee if the message is from a solitary client or numerous clients intriguing together. Consequently, another convention known as Attribute Based Signature (ABS) has been applied.

In ABS, clients have a claim predicate related with a message. The claim predicate distinguishes the client as an approved one, without uncovering its character. Different clients or the cloud can check the client and the legitimacy of the message put away. ABS can be joined with ABE to accomplish validated access control without uncovering the character of the client to the cloud. A key-arrangement (KP) ABE conspire that takes into consideration edge strategies. Key-approach implies that the encryption just gets the opportunity to mark a figure content with an arrangement of qualities. The expert picks an approach for every client that figures out which figure writings he can decode. In a multi-specialist ABE framework, we have numerous characteristic experts, and numerous clients. A client can go to a quality specialist, demonstrate that it is qualified for a portion of the property took care of by that expert, and demand the relating decoding keys. Any party can also choose to encrypt a message, in which case he uses the public parameters together with an attribute set of his choice to form the cipher text. Any user who has decryption keys corresponding to an appropriate attribute set can use them for decryption.

III. SECURITY IN CLOUD

In cloud computing, remote data access control is an important security problem. In 2005, Sahai et al. [7] introduced the concept of attribute-based encryption (ABE). By using access policy and ascribed attributes associated with private keys and ciphertexts, ABE enables access control over ciphertext. Based on the standard that the access policy is associated with the attribute key or the ciphertext, ABE is classified into two cases: key-policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE). In a CPABE protocol, the ciphertext is associated with an access policy on attributes, and every user's private key is associated with a set of attributes. If the user's attribute set satisfies the data owner's access policy, it can decrypt the data owner's ciphertext. On the other hand, in a KP-ABE protocol, the user's attribute set is used to annotate the ciphertexts and the data owner's access policy is associated with user's private key. In 2014, Chen et al. proposed and formalized outsourced attribute-based signature [8]. With the users' attributes are managed by multi-authority, multi-authority ABE was proposed.

Multi-authority ABE is also called as the distributed ABE. Many researchers have studied the distributed ABE [9], [10], [11]. To realize the distributed fine-grained access control, we take use of the idea of multi-authority ABE. Along with the requirements from the remote data access control, ABE has been used in the fine-grained access control in cloud computing. In 2014, Yang et al. designed an expressive, efficient and revocable data access control scheme for multi-authority cloud storage systems, where multiple authorities co-exist, and each authority can issue the attribute secret key independently [12]. Li et al. designed a new secure outsourced ABE system which supports both secure outsourced key-issuing and decryption [13]. In 2015, Jung et al. presented a semi anonymous privilege control scheme which addressed the data privacy and the user identity privacy in the existing access control schemes [14].

In 2011, Green et al. introduced the notion of ABE with outsourced decryption, which largely eliminates the decryption overhead for users. They also presented concrete ABE schemes with outsourced decryption [15]. To guard against the dishonest PCS, Lai et al. considered ABE with verifiable outsourced decryption [16]. Further, Mao et al. proposed generic constructions of CPA-secure and RCCA-secure (Replayable adaptive chosen ciphertext attack) ABE systems

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

with verifiable outsourced decryption from CPA (Chosen-Plaintext Attack)-secure ABE with outsourced decryption, respectively.
By introducing a verification key in the output of the encryption algorithm, Qin et al. formalized a security model of ABE with verifiable outsourced decryption [17]. Until now, there does not the literature which solves the verifiable outsourced decryption problem in the distributed fine-grained access control. In modern information society, the user identity privacy is also an important security issue. To preserve identity privacy, anonymity has been proposed and studied in the security protocol. In 2015, Zhou et al. introduced protection saving steady CP-ABE which lessens the ciphertext to a consistent size with any given number of traits. In the meantime, they additionally proposed a security protecting property based broadcast encryption convention [18]. Han et al. proposed a security protecting decentralized CP-ABE scheme where the central authority isn't required, to be specific every specialist can work autonomously without the participation to instate the framework [19]. Numerous different specialists have additionally considered the protection safeguarding plans [20], [21]. In 2001, Camenisch et al. provided a proficient anonymous certification framework.

In the framework, the client inquiries the CA (Certification Authority) a qualification which incorporates the client's pseudonym and characteristics. By using the credential and zero knowledge proof technique, the user can prove to a third party that he has the credential containing the given pseudonym and attributes without releasing any other information.

Anonymity is the state of being not identifiable within the anonymity set. The anonymity set is the set of all possible subjects who might cause an action. Pseudonyms are identifiers of subjects, such as sender, recipient. Sender pseudonymity is defined by the sender's use of a pseudonym, recipient pseudonymity is defined by the recipient's use of a pseudonym [22]. By adopting the multi -pseudonym technique, high anonymity was achieved for the users. By associating each attribute with a pseudonym, Chen et al. proposed the direct anonymous attestation scheme with attributes [23].

A. Existing Systems

1) Dacc: Distributed Access Control in Clouds

S. Ruj, A. Nayak, and I. Stojmenovic [2], proposed a data storage and access in which the multiple encrypted copies of data can be avoided. The principle novelty of this paper is creating the key circulation focuses where at least one KDCs disseminate keys to information proprietors and clients. KDC gives access to specific fields in all records. Single keys isolates the information and the information proprietors, utilizing this system the client possess the information by having the property it had, and this can be recovered just if the characteristic matches the information. The Author apply the quality based encryption (ABE) in view of bilinear pairings on elliptic bends. This plan is agreement secure in which two clients can't together decipher any information, that nobody has singular ideal to get to.

2) Attribute-Based Signatures: Achieving Attribute-Privacy Collusion Resistance

H.K.Maji, M.Prabhakaran, and M. Rosulek [3], proposed an Attribute based Signature in which the mark bears witness to not to recognize the person of the message by a client rather it assert in regards to the trait that delivered by the client. The mark was delivered by a solitary gathering whose traits fulfill the claim being made i.e. it isn't conspiring the all people rather it simply make the property together who pooled it.

The creator clarifies the security necessities of ABS as a cryptographic primitive, and after that tells that proficient ABS development in view of gatherings with bilinear pairings. In this manner by demonstrating the development is secure in the non-specific gathering model, ABS fill a basic security necessity in property based informing (ABM) frameworks. A capable component of ABS development is that dissimilar to numerous other quality based cryptographic natives, it can be promptly utilized as a part of a multi-specialist setting, wherein clients can make claims including combinations of properties issued by autonomous and mutually distrusting authorities.

3) Secure and Efficient Access to Outsourced Data

W. Wang, Z. Li, R. Owens, and B. Bhargava[8], proposed by providing secure and efficient access to outsourced data should be must in cloud computing .To encrypt every data block with a different key the flexible cryptography-based access control is used. Through this key derivation methods, the owner should maintain only a few secrets in the storage, and this key derivation procedure is used in hash functions which will introduce very limited computation. Thus, to use over-encryption and or lazy revocation to prevent revoked users from getting access to updated data

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

blocks. A Mechanism is used to handle both updates to outsourced data and changes in user access rights. Hence it is investigated in the overhead and safety of the proposed approach an encryptor can choose, for each authority, a number do and a set of attributes. Thus, this scheme tolerate an arbitrary number of corrupt authorities.

4) Secured Scheme for Secret Sharing and Key Distribution

A. Beimel[5], proposed the sharing of data, now a days take place in Computer Networks, and the data which is been communicated inside the network may affected through the bad users, to overcome this user users two Cryptographic tools such as Generalized Secret Sharing scheme and Key distribution scheme. This make it possible to store only the secret information in the network such that only good users can access the information, the secret sharing scheme mostly received through the threshold secret sharing schemes, only through the certain threshold the information can accessed and can used by the user. In generalized secret sharing it is capable of arbitrary monotone collection whereas in Key distribution scheme the keys can be used Communication key Distribution scheme does not help in unrestricted scheme on other hand secured and restricted scheme can be accessed only through limits. Linear Secret Sharing Scheme, Monotone Span programs, Secret sharing the public reconstruction computation function of shared secret keys are used.

5) Cipher text-Policy Attribute-Based Encryption

J. Bethencourt, A. Sahai, and B. Waters [6], proposed certain distributed system the user can access the data only if the data consist of credential or attributes. Only way of implementing such information in Cloud can be performed through the trusted server to store the information and getting to the cloud. In this paper the perplexing access control on the encoded information is performed in which the Cipher content strategy Attribute-Based Encryption is utilized. By using this scheme the storage data can be kept confidential even when the storage is untrusted, and this method secures against the collusion attack. The Previous Attribute Based Encryption systems used attributes to describe the encrypted data and even to build policies into user's keys; while in our system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt.

6) Multi-Authority Attribute Based Encryption

M. Chase [7], proposed personality based encryption the client utilize the identity to look through the information though in trait based encryption includes attribute to look through the information. Sahai and water presented a solitary authority attribute encryption plan and left the inquiry whether the various specialists permitted to circulate framework. This plan permits any polynomial number of free experts to screen characteristics and convey mystery keys.

7) Privacy Preserving Access Control with Authentication for Securing Data in Clouds

S. Ruj, M. Stojmenovic and A. Nayak [9], proposed a new privacy preserving authenticated access control scheme for securing data in clouds. In the proposed scheme, the cloud verifies the authenticity of the user without knowing the user's identity before storing information. It additionally has the additional component of access control in which just legitimate clients can decode the stored information. The plan anticipates replay assaults and backings creation, change, and perusing information put away in the cloud. In addition, the confirmation and access control scheme is decentralized and strong, dissimilar to different access control plans intended for clouds which are brought together. The correspondence, calculation, and capacity overheads are practically identical to brought together methodologies.
They displayed a protection saving access control scheme for clouds. The plan gives fine-grained get to control as well as verifies clients who store data in the cloud. The cloud however does not know the personality of the client who stores data, yet just confirm the client's certifications. Key distribution is done decentralized. One confinement is that the cloud knows the entrance strategy for each record put away in the cloud. In future, we might want to secure the protection of client characteristics also.

9) Toward Secure and Dependable Storage Services in Cloud Computing

C. Wang, Q. Wan, K. Ren, N.Cao and W.Lou [10], proposed a Cloud storage which enables users to remotely store their data and enjoy the on demand high quality cloud.

Applications without the weight of neighborhood equipment and programming administration. The advantages are clear, such an administration is likewise giving up clients' physical ownership of their outsourced information, which definitely postures new security dangers toward the rightness of the information in cloud. So as to address this new issue and further accomplish a safe and reliable distributed storage benefit, an adaptable disseminated storage integrity inspecting component, using the homomorphic token and conveyed deletion coded information. The proposed configuration enables clients to review the distributed storage with extremely lightweight correspondence and

calculation cost. The reviewing result guarantees solid distributed storage accuracy ensure, as well as at the same time accomplishes quick information mistake confinement, i.e., the distinguishing proof of acting up server. Considering the cloud information are dynamic in nature, the proposed configuration additionally bolsters secure and effective dynamic tasks on outsourced information, including square alteration, erasure, and annex. Examination demonstrates the proposed plot is very effective and versatile against Byzantine disappointment, vindictive information modification assault, and much server colluding assaults.

To accomplish the confirmations of cloud information trustworthiness and accessibility and authorize the nature of trustworthy distributed storage benefit for clients. A viable and adaptable circulated scheme with unequivocal dynamic information bolster, including square refresh, erase, and attach. What's more, depend on deletion revising code in the record dissemination planning to give excess equality vectors and certification the information reliability. By using the homomorphic token with appropriated confirmation of deletion coded information, our plan accomplishes the mix of capacity rightness protection and information mistake limitation, i.e., at whatever point information debasement has been recognized amid the capacity accuracy check over the conveyed servers, we can nearly ensure the concurrent distinguishing proof of the getting out of hand server(s). Thinking about the time, calculation assets, and even the related online weight of clients, we additionally give the augmentation of the proposed primary plan to help outsider inspecting, where clients can securely assign the honesty checking undertakings to third - party examiners and be effortless to utilize the distributed storage administrations. Through point by point security and broad analysis comes about, we demonstrate that our plan is very proficient and flexible to Byzantine disappointment, malevolent information adjustment assault, and much server conniving assaults.

2.1.9 Fuzzy Keyword Search over Encrypted Data Using Cloud Computing

J.Li, C. Wang, Q. Wan, K. Ren, N. Cao and W. Lou [11], proposed a Cloud processing technology that uses the web and focal remote servers to keep up information and applications. Distributed computing enables purchasers and organizations to utilize applications without establishment and access their own documents at any PC with internet access. This innovation considers considerably more productive figuring by bringing together capacity, memory, preparing and transfer speed. Maybe the greatest worries about distributed computing are security and protection. In the event that a customer can sign in from any area to get to information and applications, it's conceivable the customer's security could be bargained.

III. CONCLUSION

Cloud over the years has become the prominent field over the past couple of decades and is present everywhere around us. This makes it even more important that the security and privacy of data passed through cloud be taken seriously. The exponential growth of cloud and its diversity makes it hard to develop a “One size fits all” solution but it is also what makes it interesting, there are many solutions that do a great job of ensuring security of a cloud network and many are under development. Even though cloud has been around for a long time there is still a lot to be done there.

REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. A view of cloud computing. Communications of the ACM, 53(4):50–58, 2010.
[2] K. Yang and X. Jia. Data storage auditing service in cloud computing: challenges, methods and opportunities. World Wide Web, 15(4):409–428, 2012.
[3] S. Subashini and V. Kavitha. A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1):1 – 11, 2011.
[4] K. Yang and X. Jia. Expressive, efficient and revocable data access control for multi-authority cloud storage. IEEE Transactions on Parallel and Distributed Systems, 25(7):1735–1744, 2014.
[5] S. Kamara and K. Lauter, “Cryptographic cloud storage,” in Proceedings of the 14th Financial
[6] Cryptography and Data Security. Springer, 2010, pp. 136–149.
[7] K. Ren, C. Wang, and Q. Wang, “Security challenges for the public cloud,” IEEE Internet Computing, vol. 16, no. 1, pp. 69–73, 2012.
[8] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” Proc. EUROCRYPT, 2005, pp. 457-473.
[9] X. Chen, J. Li, X. Huang, J. Li, Y. Xiang and D. S.Wong, “Secure outsourced attribute-based signatures”, IEEE Transactions on Parallel and Distributed Systems, 25(12), 2014, pp. 3285-3294.
[10] M. Chase, “Multi-authority attribute based encryption”, Theory of Cryptography, 2007, pp. 515-534.
[11] H. Qian, J. Li, Y. Zhang, J. Han,“Privacy-preserving personal health record using multi-authority attribute-based encryption with revocation”, International Journal of Information Security, 14(6),
[12] 2015, pp. 487-497.
[13] S. M¨uller, S. Katzenbeisser, and C. Eckert, “Distributed attribute-based encryption”, ICISC 2008, pp. 20-36.
[14] [12] K. Yang, and X. Jia, “Expressive, efficient, and revocable data access control for multi-authority cloud storage”, IEEE Transactions on Parallel and Distributed Systems, 25(7), 2014, pp. 1735-1744.
[15] J. Li, X. Huang, J. Li, X. Chen and Y. Xiang, “Securely outsourcing attribute-based encryption with checkability”, IEEE Transactions on Parallel and Distributed Systems, 25(8), 2014, pp. 2201-2210.

[16] T. Jung, X. Li, Z. Wan, and M. Wan, "Control cloud data access privilege and anonymity with fully anonymous attribute based encryption", IEEE Transactions on Information Forensics and Security, 10(1), 2014, pp. 190-199.
[17] M. Green, S. Hohenberger, and B.Waters, "Outsourcing the decryption of ABE ciphertexts," Proc. USENIX Security Symp., 2011, 34-34.
[18] J. Lai, R. H. Deng, C. Guan, and J. Weng, "Attribute-based encryption with verifiable outsourced decryption", IEEE Trans-actions on Information Forensics and Security, 8(8), 2013, pp. 1343-1354.
[19] B. Qin, R. Deng, S. Liu S, and S. Ma, "Attribute-based encryption with efficient verifiable outsourced decryption", IEEE Transactions on Information Forensics and Security, 10(7), 2015, pp. 1384-1393.
[20] Z. Zhou, D. Huang, and Z. Wang, "Efficient privacy preserving ciphertext-policy attribute based encryption and broadcast encryption", IEEE Transactions on Computers, 64(1), 2015, pp. 126-138.
[21] J. Han, W. Susilo, Y. Mu, J. Zhou, and M. Au, "PPDCP-ABE: Privacy-preserving decentralized ciphertext-policy attribute based encryption", ESORICS 2014, pp. 73-90.
[22] J. Li, W Yao, Y Zhang, H Qian, J Han, "Flexible and fine-grained attribute-based data storage in cloud computing", IEEE Transactions on Services Computing, DOI: 10.1109/TSC.2016.2520932
[23] J Li, F Sha, Y Zhang, X Huang, J. Shen, "Verifiable outsourced decryption of attribute-based encryption with constant ciphertext length", Security and Communication Networks, DOI: 10.1155/2017/3596205.
[24] A. Pfitzmann, M. Kohntopp," Anonymity, un observability, and pseudonymityła proposal for terminology", Designing privacy enhancing technologies, LNCS 2009, 2001, pp. 1-9.
[25] L. Chen, R. Urian, "DAA-A: Direct anonymous attestation with attributes", Trust and Trustworthy Computing, LNCS 9229, 2015, pp. 228-245.