International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 6, June 2020||

Data Sharing in Cloud using Revocable Storage- Identity Based Encryption

Eyazhini. A[1], Vijayakumar .V[2]

PG Student, M.E Communication Systems, Department of Electronics and communication Engineering, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamilnadu, India[1]

Assistant Professor, Department of Electronics and communication Engineering, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamilnadu, India[2]

ABSTRACT: Cloud computing provides high performance, accessibility and low cost for data storing and sharing, provides a better consumption of resources. In cloud computing, cloud service providers compromise an abstraction of infinite storage space for clients of mass data. we outsource the storage of data, which is possibly sensitive, to cloud providers. To preserve data privacy, a mutual approach is to encrypt data files before the clients upload the encrypted data into the cloud within the organization. Unfortunately, it is hard to design In this work, an AES based encryption scheme is proposed which If the group member can be revoked means, automatically change public keys of existing group and no need encrypt again the original data. Any user in the group can use the source within the cloud and revoked users can't access the cloud once more after they are revoked. Finally implement this secure distribution scheme into group data sharing environments with AES algorithm.

KEYWORDS: Secure Data Sharing, Role with Time based access control, AES encryption,

I.INTRODUCTION

Cloud Computing Basics computing resources that are delivered as a service over a network. In cloud computing model users should provide access permission to their records for storing and performing the business operations. Hence cloud provider need to provide the trust and safety, as there's precious and sensitive information in large amount stored on the clouds. There are worries about flexible, scalable and quality grained access control inside the cloud computing .Cloud computing technology consists of the use of cuting is consistently growing and there are many main cloud computing providers including Amazon, Google, Microsoft, Yahoo and many others who are offering solutions including Software-as-a-Service (SaaS), Platform-as- a-Service (PaaS), Storage-as-a- Service and Infrastructure-as-a-Service (IaaS). In addition, considering the possibility to substantially minimizing expenses by optimization and also maximizing operating as well as economic effectiveness, cloud computing is an excellent technology. Furthermore, cloud computing can tremendously boost its cooperation, speed, and also range, thus empowering a totally worldwide computing model on the internet infrastructure. On top of that, the cloud computing has advantages in delivering additional scalable, fault tolerant services. Cloud computing handles useful resource management in a higher way for the reason that consumer not needs to be responsible for figuring out sources for storage. If a person wants to save more records they request it from the cloud provider and as soon as they may be completed they could both release the storage with the aid of virtually stopping the use of it, or move the data to a protracted-term lower-cost storage resource. This in addition lets in the consumer to use greater dynamic resources due to the data they now not want to difficulty themselves with storage and cost that accompany new and old sources.Cloud computing service models are all inside in the cloud sing and laptops, desktops, phones and tablets are acts like clients to get services from the cloud. Servers provide services to clients according to their request or pay base. Cloud computing provides a shared pool of configurable IT resources on demand, in which needs minimal effort of management to get better services. Services are based on various agreement SLA (Service Level Agreement) between service providers and consumers.

1.1 Cloud Security

The meaning of security is plentiful. Security is the combination of confidentiality, the prevention of the unauthorized disclosure of information, integrity, the prevention of the unauthorized amendment or deletion of information, and availability, the prevention of unauthorized withholding of information.The inherent problems of data security, governance, and control with control inside the cloud computing are discussed. The key protection,

privateness, and true issues in the existing environment of cloud computing and assist customers to understand the tangible and intangible threats associated with its use. According to the authors, there are three essential ability threats in cloud computing, particularly, security, privateness, and trust. Security performs a critical role inside the current technology of long dreamed vision of computing as a application. It divided into further types called protection approaches, server tracking or tracing, data confidentiality, and avoids malicious insiders' illegal operations and carrier hijacking.

A information security framework for cloud computing networks is proposed. The authors especially mentioned the security issues associated with cloud information storage. There are also some patents approximately the statistics storage safety techniques. Give a survey on secure cloud computing for essential infrastructure. A security and privacy framework for RFID in cloud computing was proposed for RFID technology integrated to the cloud computing, which will combine the cloud computing with the Internet of Things.

1.2 Data Integrity

Data integrity is one of the maximum crucial elements in any information storage. Generally, data integrity defines defensive statistics from unauthorized deletion, modification, or fabrication. Managing entity's admittance and rights to specific organization resources guarantees that precious records and services are not abused, misappropriated, or stolen. Data integrity is without difficulty executed in a standalone gadget with a single database. Data integrity in the standalone system is maintained via database constraints and transactions, which is usually finished by a database management system (DBMS). Transactions ought to observe ACID (atomicity, consistency, isolation, and durability) properties to ensure integrity of data. Most databases help ACID transactions and might maintain information integrity. Authorization is used to control the access of data. It is the mechanism through which a device determines what stage of access permission to a selected authenticated person should must comfortable resources managed by way of the system.

1.3 Data Confidentiality

Data confidentiality is crucial for customers to store their personal or private information inside the cloud. Authentication and access permission techniques are used to make certain data confidentiality. The data confidentiality, authentication, and access manipulate issues in cloud computing will be addressed with the aid of growing the cloud reliability and trustworthiness. Because the users do no longer accept as true with the cloud providers and cloud storage service carriers are absolutely not possible to remove ability insider danger, it is very risky for users to save their sensitive records in cloud storage immediately. Simple encryption is faced with the important thing management problem and cannot guide complex necessities along with query, parallel change, and fine- grained authorization.

II.RELATED WORK

Chard, et.al,.[1] Online relationships in social networks are often based on real world relationships and can therefore be used to infer a level of trust between users. Here advise leveraging those relationships to shape a dynamic “Social Cloud,” thereby permitting customers to proportion heterogeneous resources within the context of a social network. In further improvement, the inherent socially corrective mechanisms called incentives and disincentives are can be used to permit a cloud-based framework for long term sharing with decrease privacy concerns and protection overheads than are determined in traditional cloud environments. Due to the precise nature of the Social Cloud, a social market place is proposed as a method of regulating sharing. The social market is novel, as it uses each social and financial protocol to facilitate trading. The social storage cloud implementation consists of two concurrent financial markets, published price and reverses auctions. In the reverse auction (gentle) market, a consumer can specify their storage requirements and then submit a public sale request to the social garage cloud. The consumer’s buddies then bid to provide the asked storage. The auction mechanisms used are based on the DRIVE Meta scheduler. In particular, a reverse auction protocol plug-in is used, because the dominant bidding approach (reality telling) is socially centric. It also means that “antisocial” behavior such as counter speculation is fruitless. Yang, et.al,.[2] In proposed method, let the server compute the proof as an intermediate value of the verification (calculated by the challenge stamp and the linear combinations of data blocks), such that auditor could use intermediate value to verify the auditing proof. Therefore, this method can greatly reduce the computing loads of the auditor by moving it to the cloud server. To improve the performance of an auditing system, apply the Data Fragment Technique and Homomorphic Verifiable Tags in our method. The fragment technique can lessen quantity of information tags, such that it may lessen the storage overhead and enhance the storage performance. By using the homomorphic verifiable tags, no matter what number of information blocks are challenged, the server responses the sum of data blocks and the product of tags to the auditor,

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 6, June 2020||

whose length is constant and equal to other information block. Thus, it reduces the conversation cost.Wang, et.al,.[3] In this process, enhance the safety of ID-primarily based ring signature via presenting forward security: If a secret key of any person has been compromised, all previous generated signatures that include this consumer still stay valid. This belongings is particularly critical to any huge scale statistics sharing system, as it's far impossible to ask all records proprietors to re-authenticate their statistics despite the fact that a mystery key of one single user has been compromised. Motivated by means of the practical desires in data sharing, we proposed a brand new notion called Forward Secure ID-Based Ring Signature. It permits an ID-based fully ring signature scheme to have forward security. It is the primary in the literature to have this feature for ring signature in ID- primarily based setting. Our scheme gives unconditional anonymity and may be confirmed forward-relaxed unforgeable within the random oracle model, assuming RSA trouble is difficult. Our scheme could be very efficient and does no longer require any pairing operations. This scheme might be very beneficial in lots of different sensible packages, specially to the ones require person privacy and authentication, such as ad-hoc based network communication, e-commerce activities and smart grid.Huang, et.al,.[4] Data sharing with a massive number of individuals should recollect numerous problems, including performance, data integrity and privateness of data owner. Ring signature is a promising candidate to construct an anonymous and authentic data sharing device. It lets in a records owner to anonymously authenticate his records which may be put into the cloud for storage or evaluation cause. Yet the important costly certificates verification in the conventional public key infrastructure (PKI) setting will become a bottleneck for this solution to be scalable. Identity-based (ID-primarily based) ring signature, which removes the method of certificate verification, can be used rather. In this paper, also enhance the safety of ID- primarily based ring signature by way of supplying ahead security: If a secret key of any person has been compromised, all preceding generated signatures that consist of this user nevertheless stay valid. This property is particularly critical to any big scale data sharing environment, as it is not possible to invite all data owners to re- authenticate their information despite the fact that a secret key of single user has been compromised. Propose a new perception known as Forward Secure ID-based Ring Signature, that's an critical tool for building value-powerful real and nameless data sharing system: For the primary time, we offer formal definitions on ahead comfortable ID-based ring signatures; right here present a concrete layout of ahead relaxed ID based ring signature.Chu, et.al,.[5] Describe new public- key crypto systems which produce steady- length ciphertexts such that green delegation of decryption rights for any set of ciphertexts is viable. The novelty is that one can aggregate any set of secret keys and lead them to as compact as a single key, however encompassing the energy of all the keys being aggregated. In different words, the secret key holder can launch a consistent-size aggregate key for bendy alternatives of ciphertext set in cloud storage, however the different encrypted documents outdoor the set stay confidential. This compact combination key can be easily sent to others or be saved in a smart card with very limited relaxed storage. The sizes of ciphertext, public-key, and grasp-secret key and combination key in our KAC schemes are all of constant length. The public storage parameter has length linear in the number of ciphertext instructions, but most effective a small a part of it is wished on every occasion and it is able to be fetched on call for from big cloud storage. Previous solutions may get a similar assets offering a constant-size decryption key, however the lessons want to comply to some pre- described hierarchical relationship. Our work is flexible in the feel that this constraint is removed, this is, no special relation is needed between the training.

III.EXISTING METHODOLOGIES

Cloud storage is one of the most important services in cloud computing, which enables the interconnection of all types of electronic products. Group data sharing has many practical applications, such as electronic health networks, wireless body area networks, and electronic literature in libraries. There are two ways to share data in cloud storage. The first is a one-to-many pattern, which refers to the scenario where one client authorizes access to his/her data for many clients. The second refers to a many-to-many pattern, this defines a situation in which many clients in the common group should authorize access to their data for many clients at the same time. Fig 3 Identity Based Encryption In existing work, proposed a revocable-storage identity-based encryption (RS-IBE), which can provide the forward/backward security of ciphertext by introducing the functionalities of user revocation and ciphertext update simultaneously.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 6, June 2020||

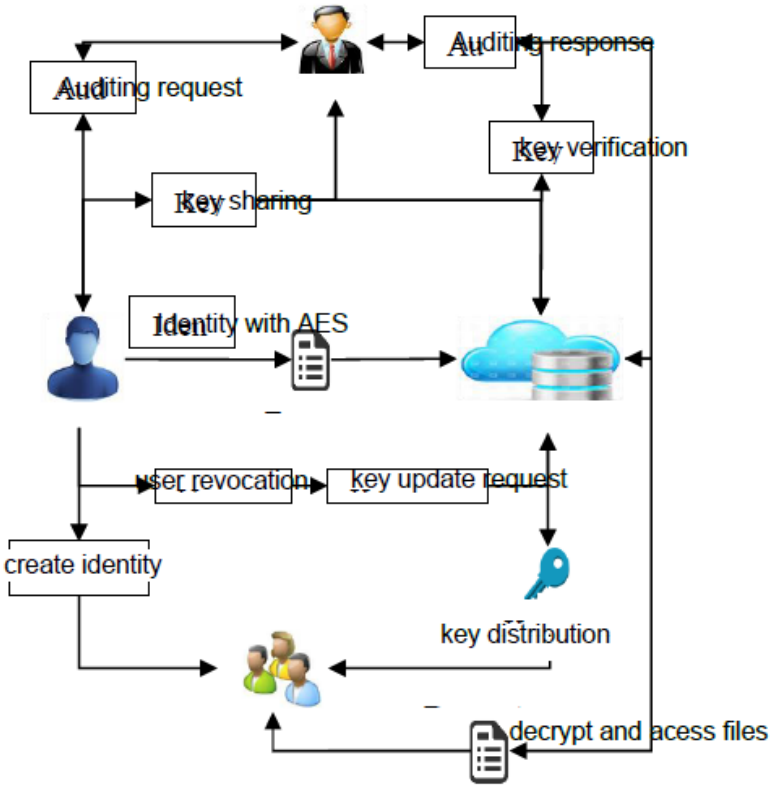

Fig 3 Architecture Diagram RS-IBE

3.1 IBE

Identity Based Encryption (IBE) takes a effective approach to the problem of encryption key management. IBE can use any string as a public key, enabling data to be protected without the need for certificates. Identity-based systems allow any user to generate a public key from a known identity value such as an ASCII string. A trusted third party is denoted by Private Key Generator (PKG) that generates the corresponding private keys. The PKG first provides a master public key, and then provide the corresponding master private key. Given the master public key, any user can compute a public key corresponding to the identity ID by combining the master public key with the identity value. To acquire a corresponding personal key, the user authorized to apply the identity ID contacts the PKG, which uses the master key to generate the personal key for Identity ID. Thus, users may additionally encrypt messages with out a earlier distribution of keys among individual contributors. This is useful in instances wherein pre-distribution of authenticated keys is inconvenient or

3.2 Architecture Diagram RS-IBE

The non-revocable data sharing system can provide confidentiality and backward secrecy. Furthermore, the method of decrypting and re-encrypting all the shared data can ensure forward secrecy. However, this brings new challenges. Note that the process of decrypt-then reencrypt necessarily involves users' secret key information, which makes the overall data sharing system vulnerable to new attacks. In general, the effect of secret key need to be restrained to best common decryption, and it is inadvisable to replace the cipher textual content periodically through the usage of secret key. Another challenge comes from efficiency. To update the cipher text of the shared data, the data provider has to frequently carry out the procedure of download-decrypt-reencrypt-upload. This process brings great communication and computation cost, and thus is cumber some and undesirable for cloud users with low capacity of computation and storage.

3.3 Secure Group Data Sharing With User Revocation

To enable data sharing in the Cloud, it is essential that only authorised users are able to get access to data stored in the

Cloud. Figure 4.1 demonstrates the Secure Group Sharing in Cloud. When the data owner desires to share their data in to a group, he/she sends the secret key used for data encryption to every member of the organization. Any of the institution participants can then get the encrypted data from the Cloud and decrypt the information using the secret key and for this reason group member does now not require the interference of the data owner. The hassle in this approach is that it's far inefficient. When the data owner receives back the access rights from a member of the institution, that member have to no longer be capable of access to the corresponding data. Since the unauthorized member of the organization now also has the data access key. So the data owner has to change the key using the process of re-encrypt the data. When the data is re-encrypted, data owner must give out the new key to the remaining customers in the group and that is computation inefficient.

IV.RESEARCH METHODOLOGY

4.1 AES Encryption

The AES cipher is also referred to as the block cipher. No a success attack has been noted on AES. Some advantages of AES are smooth to enforce on eight-bit processors and powerful implementation on 32-bit structure processors. AES encryption isperformed in multiple rounds. Each round has 4 vital steps in conjunction with sub- byte, shift row, mix column and upload round key. Sub-byte is the substitution of bytes the use of lookup-up table. Shift row is the shifting of rows consistent with byte duration. Mix column is multiplication over Galois subject matrix. Finally, inside the upload round key step, the output matrix of blend column is XORed with the round key. The wide variety of rounds used for encryption is predicated upon at the critical issue size. For a 128-bit key, these 4 steps are applied to 9 rounds, wherein the 10th round does not take into account the aggregate column step. Since all steps are recursive, decryption is the alternative of encryption.

4.2 Algorithm Procedure

The set of regulations begins with an Add round key diploma observed via the usage of 9 rounds of 4 degrees and a tenth round of 3 ranges. This applies for each encryption and decryption with the exception that each degree of spherical the decryption set of policies is the inverse of its counterpart in the encryption set of rules. The four ranges are as follows:

1. Substitute bytes
2. Shift rows
3. Mix Columns
4. Add Round Key

The 10th spherical in reality leaves out the Mix Columns stage. The first nine rounds of the decryption algorithm include the following:

1. Inverse Shift rows
2. Inverse Substitute bytes
3. Inverse Add Round Key
4. Inverse Mix Columns

Again, the tenth round leaves out the Inverse Mix Columns degree. Each of those degrees will now be taken into consideration in extra element.

4.3 Data Sharing Framework

In this module, create a local Cloud and provide priced abundant storage services. The users can add their data within the cloud, wherein the cloud storage can be made at ease. However, the cloud is not fully depended on by users for the reason that CSPs are very probably to be outside of the cloud customers' depended on area. Proposed secure data sharing framework provides communication between group owner and group members. Group Owner takes charge of followings,

1. System parameters generation
2. User registration
3. User revocation
4. Revealing the original identity of outsourced data owner.

Therefore, the group owner is fully trusted by the other parties. The Group owner is the admin. The group owner has

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 6, June 2020||

the logs of each and every process in the cloud. The group owner is responsible for user registration and also user revocation too.

4.4 Key Generation and Distribution

Key Generation is the process of generating secret key for group owner and group members. After completion of registration secret key is generated using random key generation process and send to the corresponding user through email. During login user should enter their secret key that will be verify with database. If user does not have valid user id they will not allowed accessing application. The concept of group signatures was performed by PKG (Public Key Generation). In formally, a group signature scheme permits any member of the group to sign messages even as retaining the identity secret from verifiers. Besides,the certain institution manager can reveal the identity of the signature's originator when a dispute happens, that is denoted as traceability. In this paper, a variant of the group signature updation scheme will be used to achieve anonymous access control, as it supports efficient membership revocation.

V.CONCLUSION

Data sharing in the Cloud is available in the future as demands for data sharing continue to grow rapidly. Proposed work, presented a review on secure data sharing in cloud computing environment. To reduce the cost data owner outsource the data. Data owner is unable to control over their data, because cloud service provider is a third party provider. The problem with data sharing in the cloud is the privacy and security issues. Various techniques are discussed in this paper to support privacy and secure data sharing such as AES encryption, Group data sharing and User revocation. The study concludes that secure anti collision data sharing scheme for groups provides more efficiency, supports access control mechanism and data confidentiality to implement privacy and security in group sharing.

REFERENCES

[1]Chard, Kyle, Kris Bubendorfer, Simon Caton, and Omer F. Rana. "Social cloud computing: A vision for socially motivated resource sharing." IEEE Transactions on Services Computing5, no. 4 (2011): 551- 563.
[2]Yang, Kan, and Xiaohua Jia. "An efficient and secure dynamic auditing protocol for data storage in cloud computing." IEEE transactions on parallel and distributed systems 24, no. 9 (2012): 1717-1726.
[3]Wang, Boyang, Baochun Li, and Hui Li. "Panda: Public auditing for shared data with efficient user revocation in the cloud." IEEE Transactions on services computing 8, no. 1 (2013): 92-106.
[4]Huang, Xinyi, Joseph K. Liu, Shaohua Tang, Yang Xiang, Kaitai Liang, Li Xu, and Jianying Zhou. "Cost-effective authentic and anonymous data sharing with forward security." IEEE Transactions on computers 64, no. 4 (2014): 971-983.
[5]Chu, Cheng-Kang, Sherman SM Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng. "Key-aggregate
[6]Yao, Danfeng, Nelly Fazio, Yevgeniy Dodis, and Anna Lysyanskaya. "ID-based encryption for complex hierarchies with applications to forward security and broadcast encryption." In Proceedings of the 11th ACM conference on Computer and communications security, pp. 354-363. ACM, 2004.
[7]Sahai, Amit, Hakan Seyalioglu, and Brent Waters. "Dynamic credentials and ciphertext delegation for attribute-based encryption." In Annual Cryptology Conference, pp. 199-217. Springer, Berlin, Heidelberg, 2012.
[8]Seo, Jae Hong, and Keita Emura. "Revocable identity-based encryption revisited: Security model and construction." In International Workshop on Public Key Cryptography, pp. 216-234. Springer, Berlin, Heidelberg, 2013.
[9]Krishna, Ch M. Siva Rama, and G. John Samuel. "Decentralized access control with Anonymous authentication of data stored in cloud." (2016): 2052-2060.
[10]Chen, Jie, Hoon Wei Lim, San Ling, Huaxiong Wang, and Khoa Nguyen. "Revocable identity-based encryption from lattices." In Australasian Conference on Information Security and Privacy, pp. 390-403. Springer, Berlin, Heidelberg, 2012.