IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2320-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 7, July 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.569

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

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

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 7, July 2021 ||

| DOI:10.15680/IJIRSET.2021.1007162 |

Block Design-Based Key Agreement for Group Data Sharing In Cloud Computing

Megha Shah, Dr. Uma Godase

PG Student, Department of Information Technology, Sinhgad College of Engineering, Pune, India

Professor, Department of Information Technology, Sinhgad College of Engineering, Pune, India

ABSTRACT: Data shared in the cloud allows many numerous people exchange their data in a group that helps improve environmental work efficiency. It is a challenging task today how we can assure data security in a single group and also how to share the data with multiple group members, and for it we use a key agreement protocol to share our data in a safe group. In this article we demonstrate a new conceptual agreement protocol, which contributes to the participation of many users who may assist expand many participants in the cloud environment based on the building of the block design, by using the symmetrical block design. Based on the group data sharing of the model. For several participants, we provide a regular approach to retrieve some shared conference key. A key agreement protocol is established, which includes the key to the Conference, in order to ensure the protection of your communication and to ensure that information exchange is secured. Cluster securing plays an essential part in the essential agreement

KEYWORDS: Multi cloud storage, information leakage, system attack-ability, remote synchronization, distribution and optimization.

I.INTRODUCTION

With the undeniably number of gadgets, for example, workstations, PDAs and tablets, clients require pervasive and enormous system stockpiling to deal with their regularly developing advanced lives. To meet these requests, much cloud-based capacity and record sharing administrations, for example, Drop box, Google Drive and Amazon S3 have picked up ubiquity due to the simple to-utilize interface and low stockpiling expense. In any case, these brought together distributed storage administrations are reprimanded for snatching the control of clients' information, which enables capacity suppliers to run investigation for promoting and publicizing One conceivable answer for decrease the danger of data spillage is to utilize multi distributed storage frameworks in which no single purpose of assault can release all the information. A vindictive substance, for example, the one uncovered in ongoing assaults on protection would be required to pressure all the diverse Cloud Server Provider on which a client may put her information, so as to get an entire image of her information. Put just, as the adage goes, don't put all the investments tied up on one place. However, the circumstance isn't so basic. CSPs, for example, Drop box, among numerous others, utilize rsync-like conventions to synchronize the nearby document to remote record in their concentrated mists. Each neighborhood document is parceled into little pieces and these lumps are hashed with fingerprinting calculations, for example, SHA1, MD5 Thus, a record's substance can be remarkably recognized by this rundown of hashes. For each refresh of neighborhood record, just pieces with changed hashes will be transferred to the cloud.

1.1 Background and Motivation

Blockchain is a system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system. A blockchain is essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain. Each block in the chain contains a number of transactions, and every time a new transaction occurs on the blockchain, a record of that transaction is added to every participant's ledger. The decentralized database managed by multiple participants is known as Distributed Ledger Technology (DLT). This synchronization dependent on hashes is not quite the same as like as conventions that depend on looking at two variants of a similar record line by line and can distinguish the correct updates and just transfer these updates in a fix style. Rather, the hash based synchronization demonstrates necessities to transfer the entire lumps with changed hashes to the cloud. Subsequently, in the multi cloud condition, two pieces varying just somewhat can be conveyed to two distinct mists.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 7, July 2021 ||

| DOI:10.15680/IJIRSET.2021.1007162 |

1.1 Motivation

There are lots of user preference cloud Services for Data Storage but there is no Assurance for the secure data on cloud that why our system given some effective work to Cloud Server Provider for the purposed of Data Storing

1. In cloud computing consistent view of resources is not monitored which lacks the actual condition & hence in case of faults heavy data losses or data availability reduction occurs.
2. Centralized resource manager is not identified which shares the distributed load information for first level encryption admin is performance and accurate analysis is done by cloud services provider.
3. In cloud computing security is major factor of data and key related concepts so our application is used as concepts of KASE.
4. Dynamic and efficient key management for access hierarchies.
5. Simple and fault-tolerant key agreement for dynamic collaborative data of groups.

II.REVIEW OF LITERATURE

1. PROXY PROVABLE DATA POSSESSION IN PUBLIC CLOUDS [1]

In public cloud environment, the client moves its data to public cloud server (PCS) and cannot control its remote data. Thus, information security is an important problem in public cloud storage, such as data confidentiality, integrity, and availability. Proxy provable data possession (PPDP) system allow user to secure its data through delegated proxy. PPDP provides integrity checking, provable security, bilinear pairing. This system is feasible only for the public cloud sector.

2. MOBILE CLOUD COMPUTING SERVICE MODELS: A USER-CENTRIC APPROACH [2]

Cloud computing enables mobile devices to offload complex operations of mobile applications, which are infeasible on mobile devices alone. We first provide a classification and representative achievements of current MCC service models. Then we discuss the transformation from the traditional Internet cloud to the user-centric mobile cloud by listing the issues for current MCC and presenting user-centric MCC and its design principles. It presents a new user centric MCC Service Model. Cost is more for centralized approach.

3. CLOUD-ENABLED DATA SHARING MODEL [3]

Database-as-a-Service is becoming more and more popular for many organizations. Storing data on the cloud can significantly reduce costs in terms of maintenance costs and initial investment costs. Cloud-Enabled Data Sharing Model protects data privacy on the cloud, at the same time, allowing multiple users accessing the shared database with security assurance. Re-encryption after completion of each task is very costly.

4. ATTRIBUTE-BASED ACCESS CONTROL WITH EFFICIENT REVOCATION IN DATA OUTSOURCING SYSTEMS [4]

Cipher text-policy attribute-based encryption is a promising cryptographic solution to these issues for enforcing access control policies defined by a data owner on outsourced data. However, the problem of applying the attribute-based encryption in an outsourced architecture introduces several challenges with regard to the attribute and user revocation. In this paper, we propose an access control mechanism using ciphertext-policy attribute-based encryption to enforce access control policies with efficient attribute and user revocation capability. ABE scheme is used for user revocation with access control. If multiple users collude, they may be able to decrypt a ciphertext by combining their attributes even if each of the users cannot decrypt the ciphertext alone. These colluders should not succeed in decrypting the data.

5. ENERGY-EFFICIENT FAULT –TOLERANCE IN MOBILE [5]

The advances in hardware for hand-held portable devices, resource-intensive application still remain off bounds since they require significant computation and storage capabilities. These issues are addressed by employing remote servers, such as clouds and peer mobile devices. However, for mobile devices deployed in dynamic networks challenges of reliability and energy efficiency remain largely unaddressed. These challenges are addressed by an approach called as k-out-of-n computing. Efficient access control management. Due allowance of k times incorrect input, it is less secure system.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 7, July 2021 ||

| DOI:10.15680/IJIRSET.2021.1007162 |

6. SCALABLE AND SECURE SHARING OF PERSONAL HEALTH RECORDS IN CLOUD COMPUTING USING ATTRIBUTE-BASED ENCRYPTION [6]

To assure the patients' control over access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing. Yet, issues such as risks of privacy exposure, scalability in key management, flexible access, and efficient user revocation, have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control. Novel patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semi trusted servers. Can support multiple authorities. On-demand user revocation then user private Id & information will not change.

7. MONA: SECURE MULTI-OWNER DATA SHARING FOR DYNAMIC GROUPS IN THE CLOUD [7]

With the character of low maintenance, cloud computing provides an economical and efficient solution for sharing group resource among cloud users. Unfortunately, sharing data in a multi-owner manner while preserving data and identity privacy from an entrusted cloud is still a challenging issue, due to the frequent change of the membership. Dynamic Group are used by user & generated Bilinear Map Not centralized system.

8. PRIVACY PRESERVING POLICY BASED CONTENT SHARING IN PUBLIC CLOUDS [8]

An approach is to encrypt documents satisfying different policies with different keys using a public key cryptosystem such as attribute-based encryption (ABE), and/or proxy re-encryption (PRE). However, such an approach has some weaknesses: it cannot efficiently handle adding/revoking users or identity attributes, and policy changes; it requires keeping multiple encrypted copies of the same documents; it incurs high computational costs. New Key management scheme are called as the broadcast group key management (BGKM). User Private is without utilizing cryptography send to another user.

9. SECURE OVERLAY CLOUD STORAGE WITH ACCESS CONTROL AND ASSURED DELETION [9]

It associates outsourced files with file access policies, and assuredly deletes files to make them unrecoverable to anyone upon revocations of file access policies. To achieve such security goals, FADE is built upon a set of cryptographic key operations that are self-maintained by a quorum of key managers that are independent of third-party cloud. Backup and recovery are used and also access control is used along with assured deletion. Dynamic file management at same time not implemented.

10. STRONG KEY-EXPOSURE RESILIENT AUDITING FOR SECURE CLOUD STORAGE [10]

Client doubt whether data is stored correctly in cloud or not. Indeed, security key might be explored due to weak security sense. Once malicious cloud gets the client secret key for cloud storage auditing, it can hide the data loss incidents by forging the authentication of fake data. Key update techniques are based on binary tree structures and hence provide protection and security of authentication. When key exposure happens it often cannot be found out at once. Key exposure might be difficult to be found out because the attacker might stop intrusion at once when it gets the client security key.

11. TOWARD SECURE AND DEPENDABLE STORAGE SERVICES IN CLOUD COMPUTING [11]

Cloud storage enables users to remotely store their data and enjoy the on-demand high quality cloud applications without the burden of local hardware and software management. Auditing mechanism of cloud servers at very less communication and computation cost is proposed here. Fast data error localization and secured dynamic operations on outsourced data. Third party auditor usage is possible. Flexible storage integrity and auditing mechanism. No techniques mentioned to control fraudulent attacks.

12. COOPERATIVE PROVABLE DATA POSSESSION FOR INTEGRITY VERIFICATION IN MULTI CLOUD STORAGE [12]

Provable data possession (PDP) is a technique for ensuring the integrity of data in storage outsourcing. Here, we address the construction of an efficient PDP scheme for distributed cloud storage to support the scalability of service and data migration. Here, Homomorphic variable response and hash index hierarchy are introduced. Not dependent on a single CSP. Hash index hierarchy helps in proper integration. Dynamic scaling facility on multiple storage servers. Integrating this CPDP with existing systems is challenging. It is still a challenging problem for the generation of tags with the length irrelevant to the size of data blocks. We would explore such an issue to provide the support of variable-length block verification.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 7, July 2021 ||

| DOI:10.15680/IJIRSET.2021.1007162 |

13. ENABLING DYNAMIC DATA AND INDIRECT MUTUAL TRUST FOR CLOUD COMPUTING STORAGE SYSTEMS [13]

It allows the owner to outsource sensitive data to a CSP, and perform full block-level dynamic operations on the outsourced data, i.e., block modification, insertion, deletion, and append. It enables indirect mutual trust between the owner and the CSP, and it allows the owner to grant or revoke access to the outsourced data. Dynamic Operation performances at Block Level & indirect trust between data Owner and CSP. Security is less because direct communication between clouds & Owner.

14. CLINICAL PROCESS IN BLOCK CHAIN FOR PATIENT SECURITY IN HOME CARE [14]

It is explained here how a solution for data privacy, and specifically for cognitive security, can be enforced and guaranteed using block chain technology in SAAL (Smart Ambient Assisted Living) environments. Consensus, Provenance, Immutability, Finality. No blocking mechanism introduced if continues attack from same source is found.

15. BLOCK CLOUD: A BLOCK CHAIN-BASED SERVICE-CENTRIC NETWORK STACK [15]

Connecting hundreds of devices, the Internet of Things (IoT) usage has become a technology with large influence in people's life. However, the future is threatened by frail connectivity, poor scalability, absent trust, cracked security and broken business model. Ubiquitous service and good scalability. Protects profit of both service providers and user of the network. Low Accuracy, Less Optimization of result.

III. PROPOSED WORK

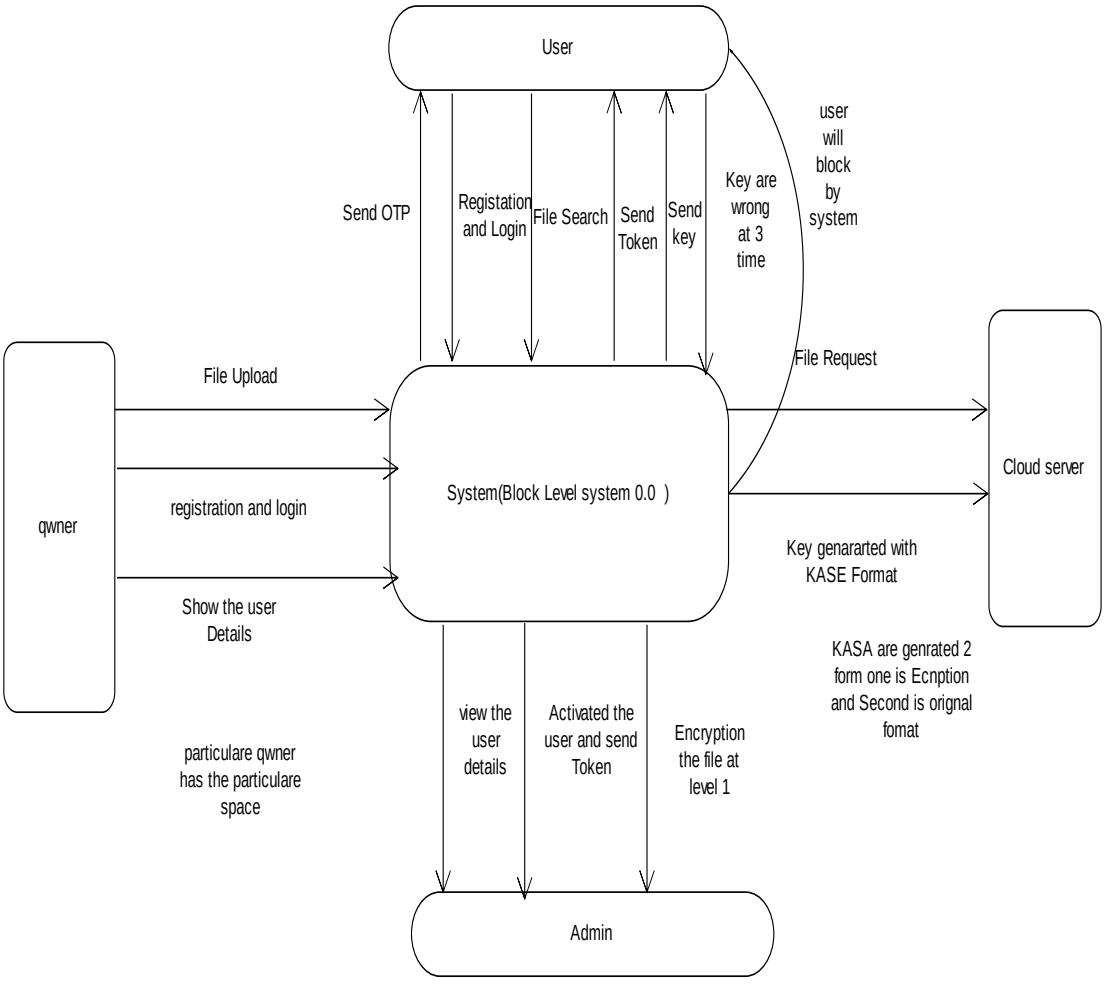

Figure 01 Proposed System Architecture

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 7, July 2021 ||

| DOI:10.15680/IJIRSET.2021.1007162 |

In Our Proposed System Our used Stored-SIM or storage planning and provide some security to user data, in that we use two layer protections such as LM Layer and CM layer all work is used in different layer. In our application de-duplication Layer and Chunking are performed in data in LM Layer and encryption and Bundling is performed in Data in CM Layer. Also we focus on access control, for the purpose for avoiding information leakage by using dynamic grouping concept's point of view also we give record monitoring to avoiding the attacker we use block chinning concept. In this project researcher used Bloom-filter Sketch for Min Hash,Generating Storage Plan Based on clustering,Idea encryption algorithms.

IV. RESULT AND DISCUSSION

In this subsection, our System evaluates the performance of the proposed scheme by several experiments. System runs these experiments on a window machine with an Intel Pentium 2.30GHz processor and 8GB memory. All these experiments use Java programming language with the many type of encryption algorithms such as Min Hash and BFS Min Hash and also using Block Chain Concepts. In our experiments, System first Install required Software. The Data are stored in the Block Chain .In Block Chain concepts the Data are stored into Sequentially block which generated by SP Chucking Algorithms .

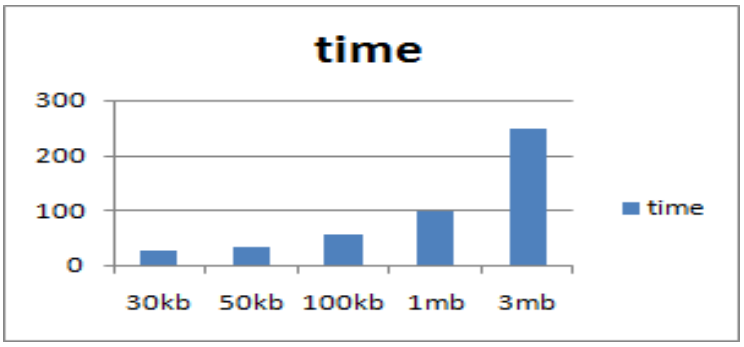

Figure 2: Shows file size on x axis and time (MS) to upload on Y-axis

Table 1: Show File Size and Time to Upload

Index Number	File size	Time (ms)
1	30kb	30
2	50kb	35
3	100kb	60
4	1mb	100
5	3mb	250

Here, In Table 1 entity Analysis of person such as Admin, Cloud which performances different role. In Our System Data Owner Upload the Data in Dynamic Group which are show to Admin Side after show the Data "Click to Encryption" when User Request to Data access of Owner than System first Check Fault Tolerances Value and Then access to User.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 7, July 2021 ||

| DOI:10.15680/IJIRSET.2021.1007162 |

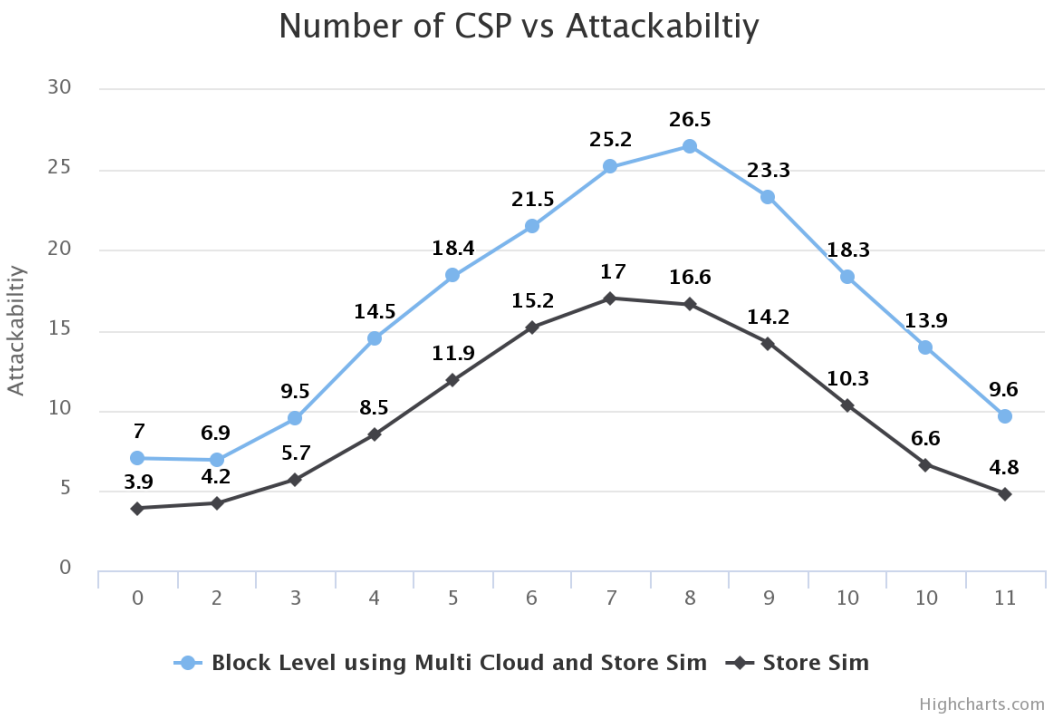

Figure 3: Graph Between Number of CSP vsAttackabiltiy

V. CONCLUSION

Cloud got many issues when it comes to security especially on Data loss, Data integrity, Data theft, and Privacy and security. According to cloud on the data loss is a very serious problem in Cloud computing. If the vendor closes due to financial or legal problems there will be a loss of data for the customers. Data Integrity is when a data is on a cloud anyone from any location can access those data from the cloud. Cloud does not differentiate between a sensitive data from a common data thus enabling anyone to access those sensitive data. Data Theft Most of the cloud Vendors instead of acquiring a server tries to lease a server from other service providers because they are cost affective and flexible for operation Data are not stored as categories in Exiting system now in our system data are stored as the as different categories. The Data are Stored in the format of Block Chain and the Main Security are not done when the data are accessibility to end User.

REFERENCES

[1] A. Bessani, M. Correia, B. Quaresma, F. Andr´e, and P. Sousa, “Depsky: dependable and secure storage in a cloud-of-clouds,” ACM Transactions on Storage (TOS), vol. 9, no. 4, p. 12, 2013.

[2] H. Chen, Y. Hu, P. Lee, and Y. Tang, “Nccloud: A network-coding-based storage system in a cloud-of-clouds,” 2013.

[3] T. G. Papaioannou, N. Bonvin, and K. Aberer, “Scalia: an adaptive scheme for efficient multi-cloud storage,” in Proceedings of the International Conference on High Performance Computing, Networking, Storage and Analysis. IEEE Computer Society Press, 2012, p. 20.

[4] Z. Wu, M. Butkiewicz, D. Perkins, E. Katz-Bassett, and H. V. Madhyastha, “Spanstore: Cost-effective geo-replicated storage spanning multiple cloud services,” in Proceedings of the Twenty-Fourth ACM Symposium on Operating Systems Principles. ACM, 2013, pp. 292–308.

[5] T. Suel and N. Memon,”Algorithms for delta compression and remote file synchronization”, 2002.

[6] ShubhangiSuryawanshi, Shubhangisuryawanshi, PramodPatil,“Email Spam Detection : An Empirical Comparative Study of Different ML and Ensemble Classifiers”, 2019 IEEE 9th International Conference on Advanced Computing (IACC).

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 7, July 2021 ||

| DOI:10.15680/IJIRSET.2021.1007162 |

[7] S.Kamara and K. Lauter, Cryptographic cloud storage, in Proc. Int. Conf. Financial Cryptography Data Security, Jan. 2010, pp. 136149.
[8] 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, Commun. ACM, vol. 53, no. 4, pp. 5058, Apr. 2010
[9] M.Kallahalla,E.Riedel,R.Swaminathan,Q.Wang,andK.Fu,Plutus: Scalablesecure file sharing on untrusted storage, in Proc. USENIX Conf. File Storage Technol., 2003, pp. 2942.
[10] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, Sirius: Securing remote untrusted storage, in Proc. Netw. Distrib. Syst. Security Symp., 2003, pp. 131145.
[11] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, Improved proxy re-encryption schemes with applications to secure distributed storage, in Proc. Netw. Distrib. Syst. Security Symp., 2005, pp. 2943.
[12] C. Delerablee, P.Paillier, andD. Pointcheval, Fully collusion secure dynamic broadcast encryption with constant-size Ciphertexts or decryption keys, in Proc. 1st Int. Conf. Pairing-Based Cryptography, 2007, pp. 3959.
[13] R. Lu, X. Lin, X. Liang, and X. Shen, Secure provenance: The essential of bread and butter of data forensics in cloud computing, in Proc. ACM Symp. Inf., Comput. Commun.Security, 2010, pp. 282292.
[14] Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud Xuefeng Liu, YuqingZhangBoyang Wang, and Jingbo Yan 2013 IEEE.
[15] B. Waters, Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization, in Proc. Int. Conf. Practice Theory Public Key Cryptography Conf. Public Key Cryptography, 2008, pp. 5370.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.569

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details