International Journal of Computing Communication and Information System(IJCCIS)
Vol 6. No.3 – July-September 2014 Pp. 106-117
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0976–1349

AN INVESTIGATION ON THE ISSUES IN CLOUD DATA STORAGE SYSTEM WITH SECURE DATA FORWARDING

[1]S.Kalaivany, [2]Dr.T.Nalini
[1]Research Scholar, [2]Professor & HEAD
[1]Department of Computer Science / [2]Department of Computer Science & Engineering
[1]Vels University, Pallavaram, Chennai 600117, [2]Bharath University ,Chennai 600 073
email id : [1]kalaivany23@gmail.com, [2]drnalinichidambaram@gmail.com

ABSTRACT

Cloud data storage system enables enterprises and government sectors with flexible, integrated, real-time decision support and eliminates economy overhead of data management. The files storage and backup maintenance can be achieved remotely by a third-party cloud storage system. The cloud provider maintains data centers with authenticated identity. Security and identity of data is a major issue when data stored remotely in third party cloud storage. Stored data in the cloud may be accidentally revealed in the future due to malicious attempts on the cloud or careless management of cloud operators.Secure data transfer is needed to maintain the data security between authorized users. The significance of maintaining a secure data sharing can be achieved by re-encrypting the data rather than normal encryption process. So that effective governance of data identity can be achieved. The re-encryption scheme enables encoding process on encrypted messages with secure data forwarding. The re-encoding process thus ultimately provides secure management and monitoring servives with data confidentiality and data robustness.

Index Terms- Re-encryption, Cloud Storage, Verifiability, Attribute based encryption.

1. INTRODUCTION

CLOUD computing has generated significant interest in the market place in which it technically treats the resource on the internet as a unified entity, a cloud. Clients simply use services without concerning about data management using virtualization. Many Recent cloud computing technologies are used to create access, manage, and maintain cloud computing environment. Cloud computing offers smooth and seamless flow of information with remotely cloud storage system. Several encryptions technique provides data confidentiality but restricts the functionality of the storage system because a few operations are supported over encrypted data, increased usage of cloud resources faces various malicious threats.To reduce threat attacks, cloud computing stakeholders must invest heavily in risk assessment to be certain that the system encrypts to safeguard data; and builds higher assurance of auditing to reinforce compliance.

In this paper, we intend to address cloud storage system [8] for maximum bandwidth utilization, confidentiality, and practicality. There is a unit numerous underlying challenges and risks in cloud computing that upsurge the threat of knowledge being negotiated. Security considerations should be self-addressed so as to absorb trust in cloud computing technology. Distributed networked storage systems [9] give storage service on the net. We indend to address privacy issue of the distributed network servers within the system area unit compromised.

2. LITERATURE REVIEW

Ateniese et al.[16] proposed precise proxy re-encryption schemes and applied them to the sharing function of protected storage systems. Here the data are encrypted by the proprietor and then stashed away in a storage server. When a user shares his messages, he directly sends a re-encryption key to the storage server. The cloud data storage proxy re-encrypts the encrypted messages for the legal user. Thus data confidentiality supports secure data forwarding

Lin et al. [12] defined Decentralized Erasure Codes are linear codes with exact randomized structure stimulated by network coding on random bipartite graphs, they are optimally sparse, and leads to minimized communication, storage and utilization cost over random linear coding.

Kallahalla et al. [11] defined the usage of cryptographic primitives to sentinel and share files. Plautus features focus highly scalable key management allowing individual users to retain direct control of access the files. The mechanisms in Plautus reduces the number of cryptographic keys exchanged between users by using file groups, with distinguished file read and write access, handling user revocation resourcefully, and permit an untrusted server to sanction file writes.

Lin et al.[10] defined a work “A Secure Erasure Code-Based Cloud Storage System With Secure Data Forwarding” in which a cloud storage system consists of storage servers and key servers integrated with a newly proposed threshold proxy re-encrytion scheme. Each storage server independently performs encoding and re-encrytion and eack key server independently performs partial decryption.

Amritha et al. [1] proposed a work entitled as “Threshold Proxy Re-Encryption Scheme and Decentralized Erasure Code in Cloud Storage with Secure DataForwarding” proxy re-encryption supports encoding operation and forwarding operation over encrypted message. It increases security and reduces the time and cost for a particular operation. This method is completely integrated encrypting, encoding and forwarding.

Priyadharshini et al. [14] proposed “A Secure Code Based Cloud Storage System Using Proxy Re-Encryption Scheme in Cloud Computing” The threshold proxy re-encryption scheme supports encryption, forwarding, and partial decryption operations in a dispersed way.

It is completely decentralized with the storage server performing encoding and re-encryption process and each key server perform independent decryption. Integrity of data is a significant functionality in cloud storage system. Whenever a user stores data in cloud storage, he/she no longer possess the data at hand. Encryption technique is used to translate plain text into cipher text. Proxy re-encryption provides data privacy in the cloud storage system.The decentralized erasure code is used to compute codeword for each message symbol.

Ateniese et al. [2] proposed a novel work "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage" that presents new encryption scheme to realize a stronger notion of security, and demonstrates the practicality of proxy re-encryption as a method of adding access control to a secure file system. Performance measurements of the experimental file system prove that proxy re-encryption can work successfully in practice.

3. SYSTEM MODEL

a. Proxy re-encryption in privacy scheme

Proxy re-encryption plays significant role in the privacy scheme. Here the request from different user will be accepted by cloud server, in addition the cloud service server will make another request to the data owner. After authorizing the request from the data owner a 64 bit key will be generated for data visualization. Here proxy re encryption will be successfully implemented using privacy technique. The encrypted key remains in the awaiting request, until another user accesses the key to view the data of the data owner. Proxy reencryption keys are one use key. So that keys cannot able to replicate, furthermore, in case of hacking the key it will take nearly 18 days to 45 days. But the new user will use the key within the time. Else the key request will be deleted.

Data proprietor stores the encryted data into the cloud storage server. Cloud user's can view the uploaded data.But the identity of data is maintained. Any users can send requests to the cloud server to view the data. Cloud server will forward the request from the user to the data owner. Data owner decides to accept the request from the cloud server.If accepted, Cloud server will forward the encoded key to the client. Also concurrently cloud server will generate a virtual server and decrypts the data from the cloud storage server. User can enter the encrypted key to the proxy server to view the original data. The key will be legal for one time only. After the data viewed from the proxy server, the computer-generated data will be deleted automatically.

b. Secure Forwarding for virtual preservation scheme (VPS)

Virtualization is achieved by decryption of the encrypted data in the virtual proxy server. This can be achieved by proxy re encryption. As soon as the encrypted key used by the user, a virtual server will be created for the data virtualization purpose. Once the key is used, the VPS will be removed. So that both data integrity and data confidentiality can be implemented successfully. Once data owner certifies the sender request. The key will be generated from the cloud server and sent to the user. The proxy server will be created after the user request.Decrypted data will be sent to the proxy server. The proxy server will be deleted after data visualization.

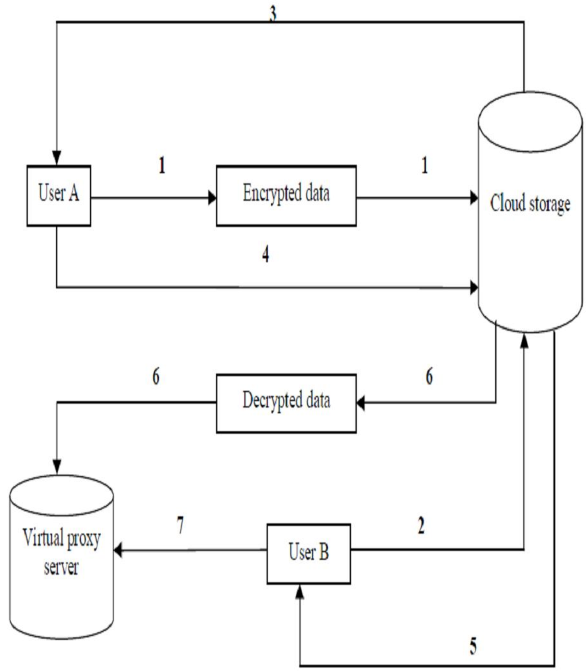

Figure 1. Illustration of Secure Forwarding for preservation scheme

c. Decentralized erasure code

Decentralized erasure code is used to split up the messages or text data into n number of blocks. The result n=akc allows more number of storage server to be superior than the number of blocks for splitting process.Decentralized erasure code acts as a first stage that autonomously computes each codeword symbol for a message. Thus, the encoding method for a message can be split into n similar tasks of generating codeword symbols. A decentralized erasure code is used in a distributed storage system. The n blocked message is stored in for the integration process.

3.1 Integration

In an integration process, the splitted message is linked into a m number of blocks, and stored in the larger storage server. User A encrypts his message M which is decomposed into k number of blocks as m1, m2, . . ., mk using an identifier ID. User A encodes corresponding block mi into a cipher text Ci and sends it to v randomly chosen storage servers. In receipt of cipher texts from a client, every cloud storage server linearly combines them with randomly chosen coefficients into a codeword symbol and stores it.Integration is used to aggregate messages into m number of blocks, which is encrypted and stored in a large number of storage server. Data is encrypted using a single key by applying hash key algorithm and forward to user B.

3.2 Encryption

Encryption is the process of conversion of plain text into a cipher text. An exclusive key is used to create cipher text.The encrypted key is used to change the cipher text again into plain text.The information is encrypted with single key using random key generation algorithm. Storage of data in third party cloud storage system does not provide confidentiality. Proxy re-encryption scheme preserves confidentiality of Data

3.3 Data forwarding

In data forwarding phase, user A forwards his encrypted message with an identifier ID stored in storage servers. User B decrypts the forwarded message by his secret key. A uses his secret key SKA and B’s public key PKB to compute a re-encryption key RKID A->B and then sends RKID A->B to every cloud storage servers. All cloud storage server employs the re encryption key to re-encrypt its codeword symbol for later retrieval needed by B. The re-encrypted codeword symbol is the grouping of cipher texts under B’s public key. In order to differentiate re-encrypted codeword symbols from intact ones, we call them unique codeword symbols and re-encrypted codeword symbols

3.4 Data Retrieval

Date retrieval is the final stage. Here Users download data using proxy re-encryption method and partially decryption. A proxy server can transfer a cipher text under a public key PKA to a new one with another public key PKB by using the re-encryption key RKA->B.In the data recovery phase, user A retrieves a message from storage servers.The message is either stored by user A or forwarded to user A. User A sends a retrieval request to central servers.A verification process is done on the request of data access.Each key server KSi needs u randomly chosen storage servers to obtain code symbols for partially decryption by using the key share SKA, I.

Finally, user A combine the partially decrypted codeword symbols to obtain the original message M. There are two situations for the data recovery phase. The first situation is User A retrieves his own message from the cloud storage system.When user A needs to retrieve the message with an identifier ID, he indicates every key servers with the identity token The key server first retrieves original code symbols from u randomly chosen storage servers and then performs partial decryption.The result of partial decryption is called a partially decrypted code symbol. The key server propels the moderately decrypted codeword symbols and the coefficients to user A. After user A collects replies from t key servers the partial decrypted codeword symbols are recovered as the chunk m1, m2, . . ., mk.

The second situation is that a user B retrieves a message forwarded to user B.The collection and combining process are as same as the first case except that key servers retrieve re-encrypted codeword symbols and perform partial decryption

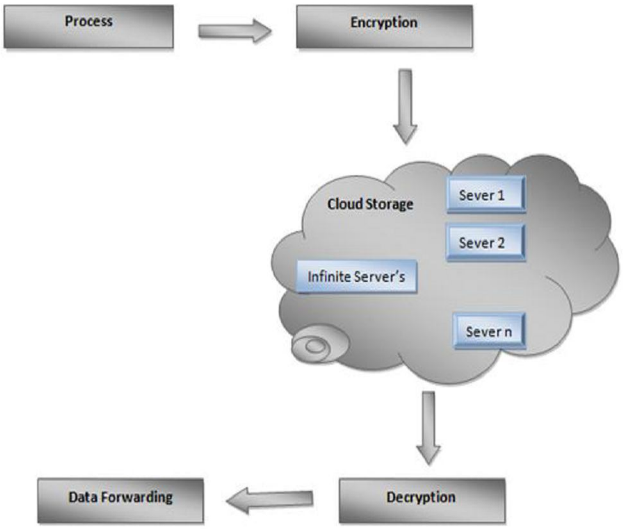

Figure2: Overview architecture

Existing System

Every existing system employs a straightforward integration method. Data stored in a third party cloud system causes serious concern on data privacy by straightforward integration method. To facilitate strong privacy of messages in storage servers, user's can encrypt messages by a cryptographic method before applying an erasure code method to encode and save messages. To make use of a message, he needs to recover the Codeword symbols from cloud storage servers. Additionally performs decryption repeatedly by using cryptographic keys. General encryption schemes protect data privacy. Cloud storage system limits the functionality of the storage system. Efficient scalability is achieved by a decentralized architecture, since a cloud storage server can fix or separate without control of a central authority.

1. Encoding Techniques
2. Centralized Erasure Code Technique
3. Proxy Re-encryption Schemes

3.5 Disadvantages of the existing system

- The user can perform more computation and communication traffic between the user and storage servers is high.
- The user has to manage his cryptographic keys
- High computation cost
- High computation time
- High communication traffic
- Less data confidentiality
- Forwarding data consumes more time
- Static data storage

4. EXISTING APPROACHES

4.1 A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding (2012)

A cloud storage system is considered here with storage servers and key servers. To remove codes above exponents the author uses a threshold proxy re-encryption technique. The threshold proxy re-encryption assistance with various processes like encoding, forwarding and fractional decryption functions in a distributed way. To decrypt a message of k blocks, each key server has to partially decrypt two codeword symbols in the system [10]. These approaches present a secure cloud storage system that gives secure data storage and secure data forwarding operation in a decentralized structure. Furthermore, every storage server independently performs encoding and re-encryption and each key server separately carry out partial decryption. The storage servers take action as storage nodes in a satisfied addressable storage system for storing comfortable addressable blocks. At the same time the key servers act as access nodes for giving a front-end layer such as a conventional file system interface.

4.2 Enabling Public Auditability and Data Dynamics for Storage Security in CloudComputing (2011)

This work facilitates the integrity of data storage in Cloud Computing. Specifically, the main purpose of Third Party Auditor (TPA) is to authenticate the integrity of the dynamic data stored in the cloud behalf of cloud clients. TPA removes the association of the client through auditing of whether his data stored in the cloud are indeed intact, which intern attains economies for Cloud Computing. This work investigated the issue of providing simultaneous public audit capability and data dynamics for remote data integrity check in Cloud Computing. The construction is purposefully developed to meet these two essential goals while attaining high efficiency [29]. For supporting efficient handling of multiple auditing works, the technique of bilinear aggregate signature is further investigated to extend main result into a multiuser setting. Performance analysis and extensive security shows that the proposed scheme is highly secure and efficient.

4.3 Key Policy-Attribute Based Encryption

A new encryption scheme namely Attribute Based Encryption (ABE) was discovered in a fine grained manner [33]. Storing data in the form of cipher-text at the third party storage is essential. The limitation of using encrypted message is that it could be distributed at coarse-grained level only. To overcome this limitation, a fine grained level is proposed by KPABE.This system engages cipher-texts and private keys. Cipher texts are tagged using attributes. Private keys associated with access structures administer the cipher-texts needed for decryption. The authors admit HIBE for assigning confidential keys.

Information stored in the server has a Fine grained access control. Also security distress involves insider attackers and a hierarchy. Hierarchy acts as a mediator and decrypts the data for the third party or gives the private decryption key to the third party. These security concerns are solved by encrypting data and allowing users to decrypt as per the security. In Secret Sharing Schemes (SSS), secret is divided and shared with the associates. SSS is represented as a tree with an access structure. ABE comprises of four steps as Setup, Encryption, Key Generation and Decryption. Access trees are created using attributes in which the intermediate nodes are the threshold gates and the child nodes are connected with the attributes. Private keys are generated and delegated to lower level users using attribute. The producer of the private key acts like a local key authority. Audit log is a complicated application in which encryption makes it more complex. Providing the entire audit log to a single analyst results in uncertainty. The presence of attribute based access structures in audit log, unauthorized access is prevented and collusion by different users is also avoided. A broadcast encryption named Targeted Broadcast works well with the help of attributes.

4.4 Cipher text Policy - Attribute Based Encryption

CP-ABE, an alternative to KP-ABE was discussed. The alternate to KP-ABE is CP-ABE. The KP-ABE attributes denote the cipher-texts while access policies are built based on the user’s keys. However, the limitation in KP-ABE system is that encryptions are not allowed to create the access policies. This in turn leads to development of CP-ABE [31]. The key provider is responsible for granting the keys and creating access policies. Altogether, the entire KP-ABE system is subject to expectation. CP-ABE is utilized to identify the complex access control in cipher-texts even in case of unknown servers. The user credentials are represented by the system using attributes. The person responsible for encryption of data assigns the access policy to a person for decryption of data. Role Based Access Control (RBAC) implements the same feature. Collusion attack is eliminated efficiently by CP-ABE other than KP-ABE. If the cipher-text is combined high chance of collusion attack is possible. Keys in Private key CPABE is obtained by randomization technique. CP-ABE is found to be more efficient than KP-ABE.

4.5 Enhancing Security by CP-ABE

A scheme which ensures data integrity and security in data outsourcing using CP-ABE was suggested [32]. The owner of the data is responsible for defining and enforcing the policies for attributes and not for users. Thus, unauthorized access is avoided. The cloud storage privacy architecture comprises of the Key Generator, Data Storage Centre, Data proprietor and the User. The Data Storage system and the Key Generator are assumed to be partially-confident. The attribute sets are recognized by private keys. The key using protocol involves key generation and data storing centers. This is followed by generation of secret keys using the secure protocol. Users possess the correct attributes using key. The key using protocol comprises two authorities to generate the secret keys for the user.

5. COMPARATIVE ANALYSIS OF THE EXISTING APPROACHES

The performance evaluation of the above discussed approaches is based on certain performance metrics. The security of the data outsourcing in the cloud is evaluated using three metrics like Decryption and Re-Encryption time, Time cost and the Space cost.

Table 2: Methods to Secure Data Outsourcing in the Cloud

Approaches	Decryption & Reencryption `	Time Cost	Space Cost
V.Goyal et.al., 2006	0.2854	10.589	4.190
J.Bethencourt et.al., 2007	0.1345	8.450	3.350
Hsiao-Ying Lin et.al., (2010)	0.0899	8.200	3.120
Guojun Wang et.al., 2010	0.0856	7.980	3.050
B.Raja Sekhar et.al.,2012	0.0498	7.160	2.450

5.1 Performance Comparison

Figure 3 shows the comparison of the Decryption and Re-Encryption time values of various approaches.

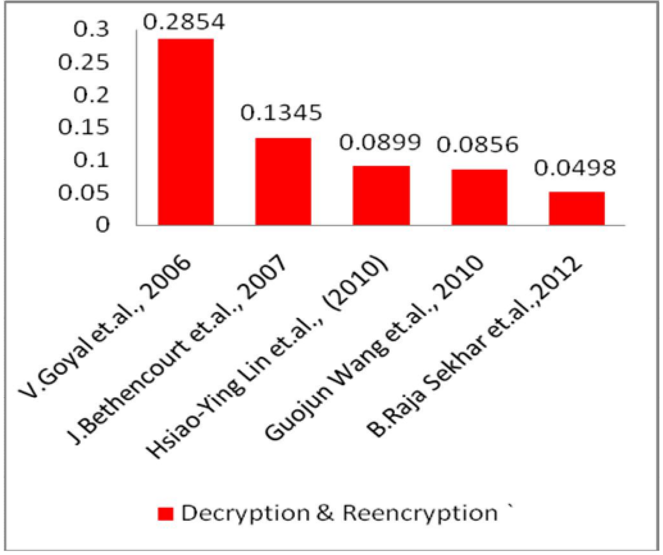

Figure 3: Comparison of Decryption and Re-Encryption time values

It is observed from the figure that the approach by B. Rajasekhar et.al.,(2012) and Guojun et al., (2010) outperformed the other approaches in terms of Decryption and Re-Encryption time values. For instance, the Decryption and Re-Encryption time obtained by the V.Goyal et al., (2007) is 0.2854, B.Rajasekhar., et al., (2012) is 0.098, Guojun et al., (2010) is 0.08, where as it is very high for the other approaches taken for consideration.

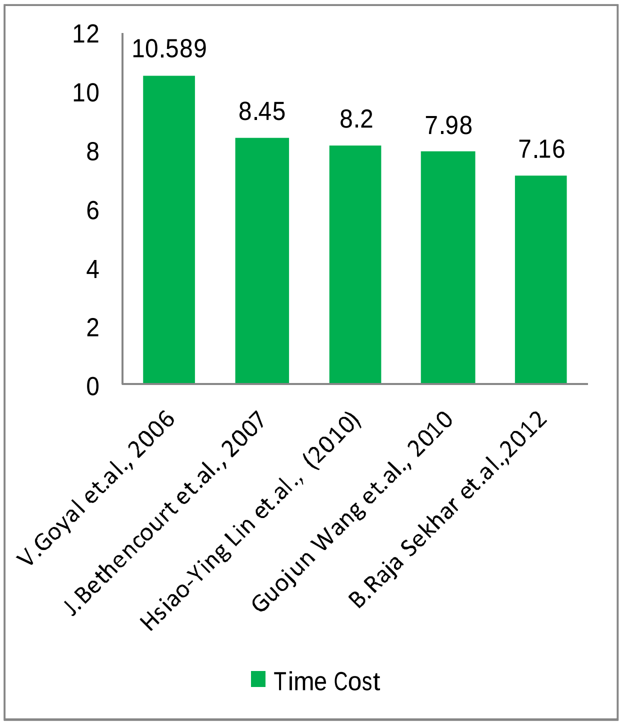

Figure 4 Comparison of Time Cost Values

Figure 4 shows the comparison of time cost values for various existing approaches. It is observed from the graph that the B. Rajasekar, et al., (2012), Guojun., et al., (2010) and Hsiao-Ying, et al., (2010) approach outperformed the other approaches in terms of time cost.

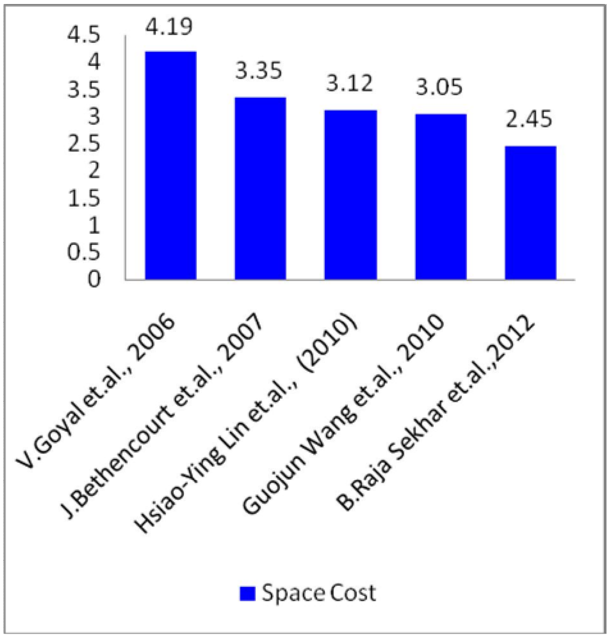

Figure 5 Comparison of Space Cost Values

Figure 5 shows the space cost of various existing approaches. The space cost of the B. Rajasekar, et al., (2012), Guojun., et al., (2010) and Hsiao-Ying, et al., (2010) approach outperformed the other approaches in terms of Time cost, where as the other approaches is observed to provide high space cost.

It is inferred from the above results that the B. Rajasekar, et al., (2012), Guojun., et al., (2010) and Hsiao-Ying, et al., (2010) approach outperformed the other approaches and gives significant results. Thus, also to increase the security of the data several other key management schemes and the new encryption algorithms should be developed.

6. CONCLUSION

This paper clearly discusses the various available cloud data security techniques and also analysis various security issues, characteristics features and working of the existing techniques. This investigation would be a motivation for research scholars to carry out their research work in cloud data security. It has been observed that, a number of cryptographic techniques have been presented to provide security and authentication to the cloud data. But, still there is space available for improvement. Key management system is observed to provide significant performance in the cloud data security. Novel encryption algorithms have to be utilized for providing cloud security. Thus, more efficient encryption techniques have to be developed which reduce the time needed for encryption and decryption.

7. FUTURE WORK

Several disadvantages are there in all existing approaches, so we have try to invent a new and modified approach with the following advantages.

- Data confidentiality, data robustness is achieved by efficient integration of encoding, encryption, and forwarding for cloud storage system.
- The storage servers independently perform encoding and re-encryption process and the key servers independently perform a partial decryption process.
- More flexible adjustment between the number of storage servers and robustness.
- To reduce the computation cost
- To reduce computation time
- To reduce communication traffic
- To increase data confidentiality
- Efficient forwarding data
- Efficient dynamic data storage

REFERENCE

[1] S.Amritha, S. Saravana Kumar, “Threshold Proxy Re-Encryption Scheme and Decentralized Erasure Code in Cloud Storage with Secure DataForwarding” Vol 9, Issue 5 (Mar. - Apr. 2013), PP 27-31.

[2] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, “Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage,”ACM Trans. Information and System Security, vol. 9, no. 1, pp. 1-30, 2006.

[3] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable Data Possession at Untrusted Stores,”Proc. 14thACM Conf. Computer and Comm. Security (CCS), pp. 598-609, 2007.

[4] G. Ateniese, R.D. Pietro, L.V. Mancini, and G. Tsudik, “Scalable and Efficient Provable Data Possession,” Proc. Fourth Int’l Conf. Security andPrivacy in Comm. Netowrks (SecureComm),pp. 1-10, 2008.

[5] G. Ateniese, K. Benson, and S. Hohenberger, “Key-Private Proxy Re-Encryption, ”Proc. Topics in Cryptology (CT-RSA),pp. 279-294, 2009.

[6] R. Bhagwan, K. Tati, Y.-C. Cheng, S. Savage, and G.M. Voelker, “Total Recall: System Support for Automated Availability Management,” Proc.First Symp. Networked Systems Design and Implementation (NSDI),pp. 337-350, 2004.

[7] M. Blaze, G. Bleumer, and M. Strauss, “Divertible Protocols and Atomic Proxy Cryptography,”Proc. Int’l Conf. Theory and Application ofCryptographic Techniques (EUROCRYPT),pp. 127-144, 1998.

[8] A.G. Dimakis, V. Prabhakaran, and K. Ramchandran, “Ubiqui-tous Access to Distributed Data in Large Scale Sensor Networks throughDecentralized Erasure Codes,” Proc. Fourth Int’l Symp. Information Processing in Sensor Networks (IPSN),pp. 111-117, 2005.

[9] A.G. Dimakis, V. Prabhakaran, and K. Ramchandran, “Decentralized Erasure Codes for Distributed Networked Storage,” IEEE Trans.Information Theory, vol. 52, no. 6 pp. 2809-2816, June 2006.

[10] Hsiao-Ying Lin, Member, IEEE, and Wen-Guey Tzeng, Member “A Secure Erasure Code-Based Cloud Storage System with Secure DataForwarding” vol. 23, no. 6, June 2012.

[11] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, “Plautus: Scalable Secure File Sharing on Untrusted Storage, ”Proc. SecondUSENIX Conf. File and Storage Technologies (FAST),pp. 29-42, 2003.

[12] H.-Y. Lin and W.-G. Tzeng, “A Secure Decentralized Erasure Code for Distributed Network Storage,” IEEE Trans. Parallel and DistributedSystems, vol. 21, no. 11, pp. 1586-1594, Nov. 2010.

[13] M. Mambo and E. Okamoto, "Proxy Cryptosystems: Delegation of the Power to Decrypt Cipher texts," IEICE Trans. Fundamentals ofElectronics, Comm. and Computer Sciences, vol. E80-A, no. 1, pp. 54-63, 1997.

[14] Priyadharshini. B, Mrs. Carmel Mary Belinda, M. Ramesh Kumar, "A Secure Code Based Cloud Storage System Using Proxy Re-EncryptionScheme in Cloud Computing" Vol.9, Issue 2 (Jan. - Feb. 2013), PP 22-27.

[15] Q.Tang, "Type-Based Proxy Re-Encryption and Its Construction," Proc. Ninth Int'l Conf. Cryptology in India: Progress in Cryptology(INDOCRYPT), pp. 130-144, 2008.

[16] J.Shao and Z. Cao, "CCA-Secure Proxy Re-Encryption without Pairings,"Proc. 12th Int'l Conf. Practice and Theory in Public KeyCryptography (PKC),pp. 357-376, 2009.

[17] G.Ateniese, K. Fu, M. Green, and S.Hohenberger, "Improved Proxy Re-EncryptionSchemes with Applications to Secure DistributedStorage," ACM Trans. Information and SystemSecurity, vol. 9, no. 1, pp. 1-30, 2006.

[18] Q.Tang, "Type-Based Proxy Re-Encryptionand Its Construction," Proc. Ninth Int'l Conf.Cryptology in India: Progress in Cryptology(INDOCRYPT), pp. 130-144, 2008.

[19] G.Ateniese, K. Benson, and S. Hohenberger,"Key-Private Proxy Re-Encryption," Proc. Topics inCryptology (CT-RSA), pp. 279-294, 2009.

[20] J.Shao and Z. Cao, "CCA-Secure Proxy Re-Encryption without Pairings," Proc. 12th Int'l Conf.Practice and Theory in Public Key Cryptography(PKC), pp. 357-376, 2009.

[21] Lidong Zhou ; Schneider, F.B. ; Marsh, M.A.; Redz A. Distributed Blinding for Distributed ElGamal Re-encryption, 25th IEEE International Conference on Distributed Computing Systems, 2005.

[22] M. Jakobsson. On quorum controlled asymmetric proxy re-encryption.In Proceedings of Public Key Cryptography. pp. 112-121.

[23] M. Mambo and E. Okamoto. Proxy Cryptosystems: Delegation of the Power to Decrypt Ciphertexts. In TFECCS, 1997.

[24] Giuseppe Ateniese, Kevin Fu, Matthew Green and S. Hohenberger Improved Proxy Re-encryption Schemes with Applications to Secure Distributed Storage, ACM Transactions on Information and System Security, Vol. 9, No. 1, February 2006.

[25] Zhidong Shen, Qiang Tong "The Security of Cloud Computing System enabled by Trusted Computing Technology" 2nd International Conference on Signal Processing Systems (ICSPS), 2010.

[26] Sayi, T.J.V.R.K. ; Krishna, R.K.N.S. ; Mukkamala, R. ; Baruah, P.K., "Data Outsourcing in Cloud Environments: A Privacy Preserving Approach", Ninth International Conference on Information Technology: New Generations (ITNG), Page(s): 361 – 366, 2012.

[27] Miao Zhou , Yimu, Willy Susilo , Junyan , Lijudong “privacy enhanced data outsourcing in the cloud” Journal of Network and Computer Applications, 2012.

[28] Wallner, HarderE.Agee,Rfc2627: key management for multicast: issues and architectures; 1999.

[29] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, Jin Li, “Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing” IEEE Transactions On Parallel And Distributed Systems, Vol. 22, No 5 May 2011.

[30] Guojun Wang, Qin Liu and Jie Wu, “ Hierarchical attribute-based encryption for fine-grained access control in cloud storage services,”CCS Proceedings of the 17th ACM conference on Computer and communications security., 735-737, 2010.

[31] J.Bethencourt, A.Sahai, B.Waters, “Ciphertext-policy attribute-based encryption,” IEEE S&P., 321–334, 2007.

[32] B.Raja Sekhar, Sunil Kumar, L.Swathi Reddy and V.PoornaChandar, “CP-ABE Based Encryption for Secured Cloud Storage Acces,” International Journal of Scientific & Engineering Research, Volume 3, Issue 9, 2012.

[33] V.Goyal, O.Pandey, A.Sahai, B.Waters, “Attribute-based encryption for fine grained access control of encrypted data,” CCS., 89–98,2006.

Author Profile

S.Kalaivany Working as Assistant Professor in Mailam Engineering College, Mailam, Tamilnadu. She has 2 years of experience in Industry and 8 years of experience in academic fields. She completed her Bachelor of Technology (IT) in Pondicherry University and Master of Engineering (CSE) in Anna University Now, doing as Research Scholar in Vels University, Pallavaram, Chennai in the field of Computer Science. Her area of interest includes computer networks, Cloud Security etc. She has also life member for several association and society.

Dr.T.Nalini Working as a professor in Bharath University. She did her M.Tech (computer Science and Engineering) and PhD in Bharath University. She has received Master degree in Computer applications (MCA) in Madras University and also she has received M.Sc degree in Information Technology in Karnataka University. She has presented more than 75 papers in various national and international conferences. And she also published 70 papers in Scopus index and referred index journals. She is having Life member of many professional bodies like ISTE, CSI and IEEE, IAENG. She is also Technical advisor and Technical committee member for various international conferences. And she is also reviewer in WASET (World Applied Science in Engineering Technology) WASJ (World Applied Science Journal).