Secure Cloud Converges With Secure Network Coding

[1]MOHAMMED ASADULLAH KHAN, [2]S MD ISMAIL

[1]PG Scholar, Department of CSE, Al Habeeb College Of Engineering And Technology, Village Damergidda, Mandal Chevella , District Ranga Reddy, Telangana, India

[2]Associate Professor, Department of CSE, Al Habeeb College Of Engineering And Technology, Village Damergidda, Mandal Chevella , District Ranga Reddy, Telangana, India

Abstract—In cloud storage environment, information owners host their data on cloud servers and users will access the information from cloud servers. owing to the info outsourcing, this method of information hosting service introduces new security challenges, which needs associate independent auditing service to visualize the information integrity within the cloud as a result of owner must be convinced that the info are properly hold on within the cloud. Two-Party storage auditing system could not be sure to provide proper auditing result so Third-Party Auditing is that the more sensible choice for the storage auditing in cloud computing. In this, we tend to try and evaluate HASH function algorithmic rule for encoding and decoding. A Third-Party Auditor is capable of doing a additional economical work and convinces each the cloud service providers and also the owner. There are possibilities of information being lost or get misplaced in cloud storage surroundings. For this, we have a tendency to propose replication mechanism to third-party auditing such it will enhance the info accessibility. We have a tendency to divide a data file into fragments and replicate the fragmented data over the cloud nodes. every of the nodes stores only one fragment of a selected file that ensures that even within the case of a productive attack, no significant data is disclosed to the assaulter. What is more, the nodes storing the fragments square measure separated by sure distance to ban an aggressor of estimation the locations of the fragments. Thus user can get the idea that his knowledge is safely hold on within the cloud and will retrieve information without any modification.

Index Terms—Secure Cloud Storage, Network Coding, Security, Third-Party Public Auditing;

I. INTRODUCTION

Cloud storage refers to saving data to an off-site storage system that is maintained by the third party. The data is holding on computer's hard drive or another local storage device, and it's the saved to the remote information through internet association between your computer and also the information. Cloud storage has many benefits over traditional data storage. As an example, if we tend to store the information on a cloud storage system, it is simple to induce that data from any location that has web access. We will not carry any physical storage device or use an equivalent pc to save and retrieve your data. With the correct storage system, we tend to might even enable others to access the information, turning a private project into a cooperative effort. Cloud storage is convenient and offers additional flexibility. Cloud storage provides edges of larger accessibility and reliability, speedy readying, robust protection for knowledge backup and disaster recovery and conjointly reduces the value as no purchase is needed to manage and maintain the valuable hardware. Data Integrity is that the basic demand of the data technology. As information Integrity is an important in databases equally integrity of information Storages is an important within the cloud, it is a serious issue moving the performance of the cloud. The information integrity provides the validity of the information, assuring the consistency or regularity of the information. It is the complete mechanism of the writing of the data during a reliable manner to the persistent data storages which might be retrieved within the same format with none changes. As described higher than, within the cloud, the whole storage of data provided by the end-user is completed at the information centres or data storages, and also the security and integrity of the information like on the vendor storing data within the data centres however not the cloud hosts. Cloud Storage is gaining quality for the outsourcing of the day-to-day management of information. So integrity monitoring of data in cloud storages is as essential for any data centred, to avoid any data corruption or data crash data corruption or data failure will occur at any storage level. so simply storing data at cloud knowledge storages or data centres doesn't make sure the integrity of information, however some mechanisms got to be enforced at every storage level to confirm the information integrity. data Integrity is most important of all the security problems in cloud data storages as a result of it not only ensures completeness of data however additionally ensures that the information is correct, accessible, and consistent and of high quality. To higher defend data security, secure cloud storage was foremost studied by Juels and Kaliski and Ateniese et al. In cloud computing, data owners host their data on cloud servers and users will access these data from cloud servers. Which means data moves or source from its local computing system to the cloud this data outsourcing introduces new security challenges. The Figure one shows the Secure Cloud Storage System. This technique consists of two entities Cloud and its user. Cloud can be any Cloud Service supplier like Amazon's S3, Dropbox, Google Drive, etc. and user can be several individual or company or a company that uses computer or portable. To increase this model, a third-party auditor can be introduced to shift the auditing task from the user to the third-party auditor. The auditing protocol should have the following properties: Confidentiality: The auditing protocol ought to keep owner's data confidential against the auditor. Dynamic Auditing: The auditing protocol ought to support the dynamic updates of the information within the cloud. Batch auditing: The auditing protocol should also be able to support the batch auditing for multiple house owners and multiple clouds. There is some existing remote integrity checking strategies which might only serve for static archive data and so they cannot be applied to the auditing service as a result of the data within the cloud will be dynamically updated. Thus, an economical and secure auditing protocol is desired to win over data house owners that the data area unit properly hold on within the cloud. To verify whether or not the cloud lies to an audit question, the user must have some secret data on its aspect that is computed in keeping with exact security level parameter victimization the likelihood of productive cheating. A secure cloud storage (SCS) protocol, a keyed protocol used for the user to generate data to be outsourced and later on query for auditing.

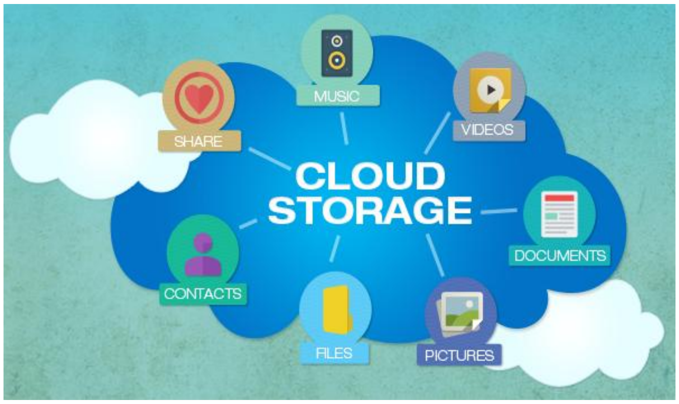


Figure 1: Architecture of Cloud Storage

II. RELATED WORK

In 2014 K. Yang and X. Jia, an efficient and secure dynamic auditing protocol for knowledge storage in cloud computing, this paper projected an efficient auditing framework for cloud storage systems and privacy protective auditing protocol for information storage in cloud computing. Then this protocol is extended to support dynamic operations. This new paradigm additionally introduces new security challenges. Data owners would worry that the info may be lost within the cloud. Therefore, owners need to be convinced that the info is properly kept within the cloud. In 2014 Danan Thilakanathan, Shiping subgenus Chen, Surya Nepal and Rafael A. Calvo, Secure data Sharing within the Cloud, Springer-Verlag Berlin Heidelberg. This paper planned a model and protocol which provides the information owner larger management once sharing data via the Cloud. The planned algorithmic program incorporating TPM devices that prevent misappropriated distribution of data once sharing information with dishonest users within the distributed computing surroundings this paper planned a secure data sharing model within the cloud. In 2007 A. Juels and B. Kaliski Jr, Pors: Proofs of retrievability for giant files, during this paper the proofs of retrievability is outlined and explored. A POR theme permits or backup service to provide a elliptic proof that a user will retrieve a target file F that's that the archive retains and faithfully transmits file information sufficient for the user to recover F in its completeness. The goal of a POR is to accomplish these checks while not users having to transfer the files themselves. It additionally provides quality of service guarantees. During this variations on basic POR theme with totally different sets of tradeoffs is explored. Obvious information possession at un-trusted stores, in this paper a model for obvious information possession is introduced that permits a consumer that has stored data at AN un-trusted server to verify that the server possesses the initial information while not retrieving it. The representation generates probabilistic proofs of ownership by variety accidental sets of blocks from the server that drastically reduces I/O prices. The consumer maintains a constant amount of information to verify the proof. Two demonstrably secure PDP schemes that area unit additional economical than previous solutions, even compared with schemes that bring home the bacon weaker guarantees.

III. FRAME WORK

In this paper, for the first time, we tend to reveal a relationship between these two different areas, i.e., secure cloud storage and secure network coding. Our main result is that we are able to construct an in public verifiable secure cloud storage protocol given any in public verifiable secure linear network secret writing protocol. The association instantly implies that a lot of previous protocols for secure network coding may be remodelled for securing cloud storage. With our generic construction, we will mechanically have several secure cloud storage constructions from existing secure network coding protocols. In contrast, secure cloud storage protocols are currently designed during a rather ad-hoc method and there are only few winning protocols. To demonstrate the ability of our construction, we tend to propose two increased secure cloud storage protocols that may satisfy the requirements of various applications. These new protocols derived from our generic construction additionally sheds insights on private-key secure cloud storage protocols, though this paper in the main focuses on public-key protocols. Notably, we tend to design the primary in public verifiable secure cloud storage protocol that is secure within the customary model, i.e., while not modelling a hash operate may be a random perform once asserting the security of the protocol. Moreover, we tend to extend our generic construction to support advanced functionalities, especially, user anonymity, and third-party public auditing. These options have received considerable attention recently. The safety of our generic construction is established under a security definition that modelling use scenarios. We tend to additionally implement and open-source a paradigm of the new publicly-verifiable secure cloud storage protocol and any valuate its performance. The paradigm makes a step forward for the protocol to be adopted in follow. We tend to hope our work will bring the knowledge behind existing solutions of secure cloud storage to possibly contribute to and provide new perspective to the network coding community. We tend to model a secure cloud storage system as shown in Figure 2.

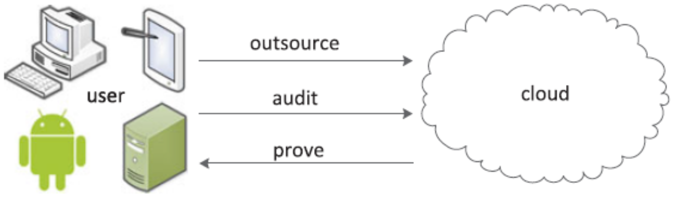


Figure 2: Architecture of Secure Cloud Storage System

There are two entities: user and cloud. In observe, a user Could be a private, a company, or an organization using a laptop or a mobile, etc.; a cloud might be any CSP, for instance Amazon S3, Drop-box, Google Drive, etc. The user first outsources its information to the cloud. Later, the user periodically performs an audit on the integrity of outsourced information. The user will then check whether or not the proof returned from the cloud is valid or not, that means that the info remains intact, or obtaining an evidence that the data has been tampered which is able to probably incur some more action (which is out of our scope), like action or data recovery. Almost like previous work and as impelled earlier during this paper, we tend to model the cloud as potentially malicious. We tend to assume the communication between the user and also the cloud is documented, which might be done by standard techniques. Thus, we will focus our attention on the user and also the cloud however not communication. A secure cloud storage system that allows a user to ascertain the integrity of the outsourced data is predicted to be Correct. If the cloud so stores the total outsourced data, the cloud will continuously sway the user that the info remains intact. Secure. If the user's data is damaged, the user will discover with high likelihood within the audit question, even though the cloud tries to hide the event. Efficient the computation, storage, and communication value of each the user and also the cloud ought to be as little as attainable. First, we need to know the aptitude of a malicious cloud. In practice, the cloud has the processed information. Besides that, the cloud will see lots of audit queries and its proof responses. it is additionally affordable that the cloud will understand whether or not the user accepts an indication response or not. This is often as a result of if the user rejects the proof, the user could sue the cloud or follows another remedy actions; if the user accepts the proof, there are not any such actions. Another necessary issue is what number audit queries and verification results the cloud will get. Our definition allows the malicious cloud to check polynomial several (in security parameter) such queries and verification results; which might cowl the user's periodical audit in observe.

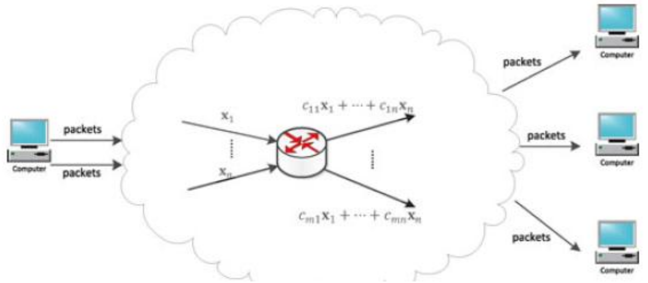
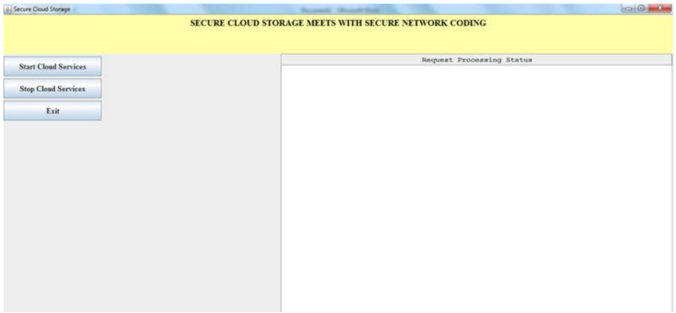
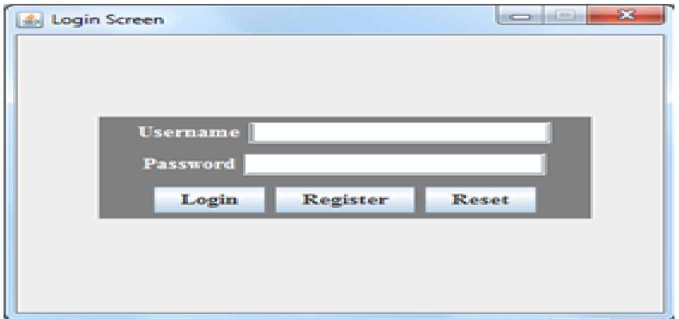


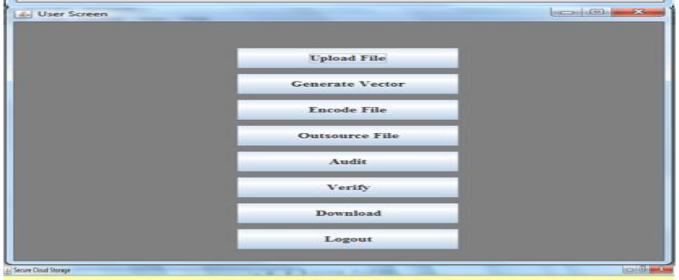
Figure 3: Architecture of Secure Network Coding System

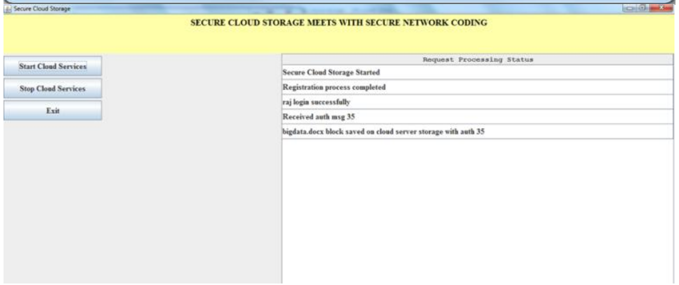
IV. EXPERIMENTAL RESULTS

In our experiments, first we need the start the secure cloud storage server after starting the secure cloud storage server then authorized user need to register in that system after registration then authorized user login into the system authorized user upload the file into the system after that click on Vector generator then the file will be store in blocks format all blocks are divided in fixed size and each block is stored encoded format after that generate the user authentication message from cloud storage server. Cloud storage server verify that authentication message then after storing file and authentication message after the audit the storage files we can also verify the each file damaged or not we can also download the file into the system after that authorized user logout into the system to shown in below screens


Secure Cloud Storage
SECURE CLOUD STORAGE MEETS WITH SECURE NETWORK CODING
Start Cloud Services
Stop Cloud Services
Exit
Request Processing Status






Secure Cloud Storage
SECURE CLOUD STORAGE MEETS WITH SECURE NETWORK CODING
Start Cloud Services
Stop Cloud Services
Exit
Request Processing Status

```
Secure Cloud Storage Started
Registration process completed
raj login successfully
Received auth msg 35
bigdata.docx block saved on cloud server storage with auth 35
```

Through our implementation we can authorized user upload the file the uploaded file can be divided into blocks format and store into encoded format and we can also audit the block and verify the block is damage or not based on that we can store and audit the data in efficient and secure manner at lower cost then compare to current methods.

V.CONCLUSION

In this work, we tend to project an efficient and secure storage auditing protocol. It protects the information privacy against the varied security issues. It additionally assures the data integrity as we tend to are taking backup of this data into slave cloud server. As most of the computation is processed on auditing server, the load on cloud server gets reduced. It presents the replication mechanism to the third party auditing that it will enhance the information accessibility. The data file was fragmented and therefore the fragments are distributed over multiple nodes. The nodes were separated by bound distance. The fragmentation and ensured that no important data was obtainable by an adversary within the case of a successful attack. Hence, the owner would remain unaware concerning such data loss things and obtain his original data. So it helps to realize data integrity, data convenience additionally its confidentiality. It is strategic to develop associate automatic update mechanism which will determine and update the required fragments only. The future work can save the time and resources used in downloading, updating, and uploading the file again.

REFERENCES

[1] J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine, "Maxprop:Routing for vehicle-based disruption tolerant networks," in *Proc.IEEE INFOCOM*, 2006, pp. 1–11.

[2] R. Gennaro, J. Katz, H. Krawczyk, and T. Rabin, "Secure network coding over the integers," in Proc. Int. Conf. Practice Theory Public Key Cryptography, 2010, pp. 142–160.

[3] D. Catalano, D. Fiore, and B. Warinschi, "Efficient network coding signatures in the standard model," in Proc. Int. Conf. Practice Theory Public-Key Cryptography, 2012, pp. 680–696.

[4] A.G.Dimakis, P.B.Godfrey, Y.Wu, M.J.Wainwright, and K. Ramchandran, "Network coding for distributed storage systems," IEEE Trans. Inf. Theory, vol. 56, no. 9, pp. 4539–4551, Sep. 2010.

[5] A. Bessani, M. Correia, B. Quaresma, F. Andr_e, and P. Sousa," Depsky: Dependable and secure storage in a cloud-of-clouds," ACM Trans. Storage, vol. 9, no. 4, p. 12, 2013.

[6] H. Chen, Y. Hu, P. Lee, and Y. Tang, "NCCloud: A network coding- based storage system in a cloud-of-clouds," IEEE Trans. Comput., vol. 63, no. 1, pp. 31–44, Jan. 2014.

[7] B. Chen, R. Curtmola, G. Ateniese, and R. Burns, "Remote data checking for network coding-based distributed storage systems," in Proc. ACM Workshop Cloud Comput. Security, 2010, pp. 3142.

[8] A. Le and A. Markopoulou, "NC-Audit: Auditing for network coding storage," in Proc. Int. Symp. Netw. Coding, 2012, pp. 155– 160.

[9] H.Chen and P.Lee, "Enabling data integrity protection in regenerating- coding-based cloud storage: Theory and implementation," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 2, pp. 407–416, Feb. 2014.

[10] B. Wang, B. Li, and H. Li, "Public auditing for shared data with efficient user revocation in the cloud," in Proc. IEEE INFOCOM, 2904–2912.

[11] B. Wang, S. S. M. Chow, M. Li, and H. Li, "Storing shared data on the cloud via security-mediator," in Proc. IEEE 33rd Int. Conf. Distrib.Comput. Syst., 2013, pp. 124–133.

[12] S. S. M. Chow, Y. J. He, L. C. K. Hui, and S. Yiu, "SPICE - simple privacy-preserving identity-management for cloud environment," inProc. Int. Conf. Appl. Cryptography Netw. Security, 2012, pp. 526–543.

[13] Wikipedia dump service [Online]. Available:http://dumps.wikimedia.org/simplewiki/20130608/

[14] Source code for secure cloud storage based securenetwork coding [Online]. Available: https://sites.google.com/site/chenfeiorange/secure cloud-storage-and-secure-networkcoding