Scientific Journal of Impact Factor(SJIF): 3.134
e-ISSN(O): 2348-4470
p-ISSN(P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 2,Issue 5, May -2015

Network Coding Technique for Secure Cloud Storage

Dinesh B Tikyani[1], Rajiv Kumar Gurjwar[2]

[1]Computer Science and Engineering, Parul Institute of Engineering
[2]Computer Science and Engineering, Parul Institute of Engineering

Abstract— *as the cloud computing is growing tremendously, but there is some issue such as lack of trust, data loss/corrupt, malicious cloud, pollution attack. But out of these issues data loss/corrupt is main issue. Many organizations don't rely on public cloud because they have fear of data loss/corrupt. Means there is low reliability on public cloud. So, we are using network coding technique to recover the data which is loss/corrupt and provide reliability in cloud. For security purpose we are going to do encryption and at second level we do network coding. In traditional system if one server or node gets fail or destroyed, the data on that node will get loss but by using network coding technique we can preserve the data. So, by Encryption we are providing security and by use of network coding we will make it more reliable means its throughput is raised*

Keywords- *Cloud Storage, Network Coding, Security, Data loss, reliability.*

I. INTRODUCTION

In this paper, we study the connection between: secure cloud storage and network coding, which seem not related to each other at the first glance. One is concerned with the problem of checking whether the data outsourced to the cloud remains unharmed as it was before being outsourced, while the other focuses on protecting a network code from being polluted during the routing. Solutions for the problem, which include proof of retrievability (PoR) and provable data possession (PDP), were proposed only recently. On the other hand, the NC has been examined for more than ten years.

Cloud computing is the delivery of computing services over the Internet. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. Examples of cloud services include online file storage, social networking sites, webmail, and online business applications. The cloud computing model allows access to information and computer resources from anywhere that a network connection is available. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications.

The following definition of cloud computing [1] has been developed by the U.S. National Institute of Standards and Technology (NIST):

"**Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction**."

Network coding is refer to coding at a node in a network, where coding is an arbitrary, casual mapping of inputs to outputs. Another possible definition of network coding, is coding at a node in a network with error-free links. This distinguishes the function of network coding from that of channel coding for noisy links; we can similarly distinguish the function of network coding from that of source coding by considering the former in the context of independent incompressible source processes. This definition is frequently used and, under it, the study of network coding reduces to a special case of network information theory. A third definition of network coding, then, is coding at a node in a packet network (where data is divided into packets and network coding is applied to the contents of packets), or more generally, coding above the physical layer. Network coding can improve: - **Throughput**, **Robustness, Complexity and Security.**

II. RELATED WORK

Cloud storage auditing was first formally studied by juels and kaliski [1] and[Ateniese et al. [2].Juels and Kaliski proposed a protocol called POR which can verify whether the cloud stores the user's whole data based on some random authentication information. One drawback is that auditing can only be done a finite number of times. The work of Ateniese et al. also addresses the cloud storage auditing problem by creating some authentication information which is related to the data. Later, researchers worked out more protocols. Shacham and Waters [3] proposed two protocols based on message authentication codes (MAC) and digital signatures. Wang et al. proposed an extension based on bilinear maps. Yang and Jia [6] also gave a similar protocol. Xu and Chang [5] proposed a secure cloud storage protocol based on a special commitment protocol. There is also some interesting work based on number-theoretic-related hash functions M. A. Shah et.al. [16]. The drawback is that there lacks a convincing security argument in the hash function based protocols.

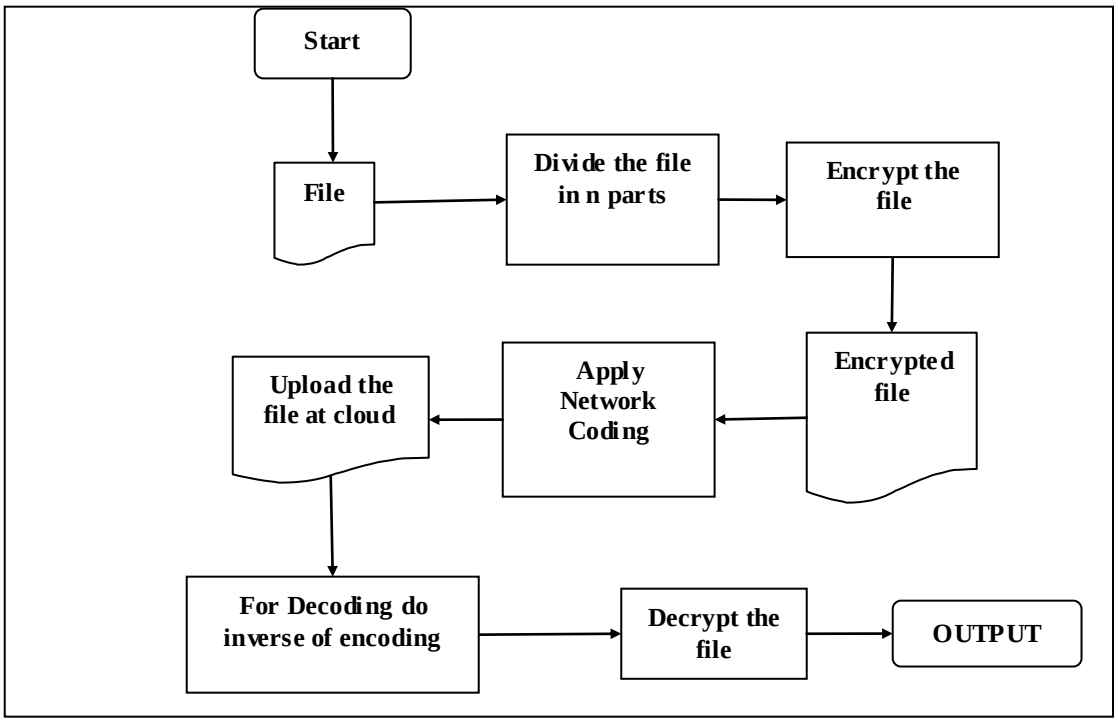
Network coding was first proposed by Ahlswede et al. [9] as a technique to increase the throughput of a multicast network. Its security issue was first studied by Cai and Yeung [7] and Gkantsidis and Rodriguez [8]. Cai and

Yeung 2002 [7] considers a positive impact of data security. Gkantsidis and Rodriguez [8] found that network coding is quite weak in front of pollution attacks. To prevent this attack, researchers proposed various protocols, e.g., employing a hash functions to protect the integrity of a codeword Gkantsidis and Rodriguez [8]. A different hash function based protocol was also proposed Q. Li et.al. [11]. There is also protocol based on digital signatures from bilinear map D. Charles et.al. [14]. More recent work focuses on constructing protocols which are secure in the standard model, i.e., without assuming the cryptographic hash functions is a truly random function R. Gennaro et.al. [17] D. Catalano et.al. [15]. There is also another line of work that employs the idea of network coding to construct reliable and distributed storage system A. G. Dimakis et.al. [18] A. G. Dimakis, P. B. Godfrey et.al. [19] Y. Hu et.al. [20], which are orthogonal to our work here. These work focus on how to construct a distributed system using network coding techniques for fast repairing damaged data with multiple clouds; while our work here focus on how to detect whether the outsourced data on a single cloud is modified using the technique that is applied for checking whether a network code is polluted.

III. PROPOSED WORK

In this section the proposed model of our system is shown in figure1. Our goal is to construct a secure cloud storage protocol given a well-designed secure network coding protocol. The basic idea lying behind the general construction is intuitive. We treat the user as a sender who wants to send the data to some receivers; however, we also treat the user as a data receiver or a router in the network. The cloud plays as a router in the network. When the user outsources the data, it first divides the data into packets which can be seen as a vector over some finite fields. Then, it authenticates the data packets by attaching some authentication information. The authenticated data is outsourced to the cloud. The steps of our model are as follow:-

Step1. Select the file to upload.
Step2. Divide the file in to n parts.
Step3. Encrypt the selected File by encrytion algorithm.
Step4. Network Encode (E (File), Key), Where E(File) = Encrypted_file
Step5. Get the m packets of a particular file from cloud.
Step6. Apply inverse of Network coding using corresponding co-efficient Stored in database.
Step7. Decrypt the encoded file.
Step8. Retrieve the file back.
Step9. Return Decoded_File.



"Figure1 Proposed Model"

IV CONCLUSION

In this paper, we have designed a general construction of secure cloud storage protocol based on any secure network coding protocol. However, it is not known if a secure network coding protocol can be constructed from a secure cloud storage protocol. Our technique is based on hybrid model for data security and reliability. For data security we are using RSA algorithm for encryption/decryption of file. The data blocks which is generated by encryption are then applied the network coding technique for the reliability purpose. RSA is an asymmetric key algorithm and it use 256 bit, so it is feasible for our technique. It is an interesting future work to consider under what condition this can be done.

REFERENCES

[1] A. Juels and B. Kaliski Jr, "Pors: Proofs of retrievability for large files," in *ACM Conference on Computer and Communications Security (SP)*, 2007, pp. 584–597.
[2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in *ACM Conference on Computer and Communications Security (CCS)*, 2007, pp. 598–609.
[3] H. Shacham and B. Waters, "Compact proofs of retrievability," in *International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT)*, 2008, pp. 90–107.
[4] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy preserving public auditing for secure cloud storage," *IEEE Transactions on Computers*, vol. 62, no. 2, pp. 362–375, 2013.
[5] J. Xu and E.-C. Chang, "Towards efficient proofs of retrievability," in *ACM Symposium on Information, Computer and Communications Security (ASIACCS)*, 2012, pp. 79–80.
[6] K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 9, pp. 1717–1726, 2013.
[7] N. Cai and R.W. Yeung, "Secure network coding," in *IEEE International Symposium on Information Theory (ISIT)*, 2002, p. 323.
[8] C. Gkantsidis and P. R. Rodriguez, "Cooperative security for network coding file distribution," in *IEEE International Conference on Computer Communications (INFOCOM)*, 2006.
[9] R. Ahlswede, N. Cai, S.-Y. Li, and R. W. Yeung, "Network information flow," *IEEE Transactions on Information Theory*, vol. 46, no. 4, pp. 1204–1216, 2000.
[10] S.-Y. Li, R. W. Yeung, and N. Cai, "Linear network coding," *IEEE Transactions on Information Theory*, vol. 49, no. 2, pp. 371–381, 2003.
[11] Q. Li, J. C. Lui, and D.-M. Chiu, "On the security and efficiency of content distribution via network coding," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 2, pp. 211–221, 2012.
[12] S. Agrawal and D. Boneh, "Homomorphic macs: Mac-based integrity for network coding," in *International Conference on Applied Cryptography and Network Security (ACNS)*, 2009, pp. 292–305.
[13] F. Zhao, T. Kalker, M. M´edard, and K. J. Han, "Signatures for content distribution with network coding," in *IEEE International Symposium on Information Theory (ISIT)*, 2007, pp. 556–560.
[14] D. Charles, K. Jain, and K. Lauter, "Signatures for network coding," *International Journal of Information and Coding Theory*, vol. 1, no. 1, pp. 3–14, 2009.
[15] D. Catalano, D. Fiore, and B. Warinschi, "Efficient network coding signatures in the standard model," in *International Conference on Practice and Theory in Public-Key Cryptography (PKC)*, 2012, pp. 680– 696.
[16] M. A. Shah, R. Swaminathan, and M. Baker, "Privacy-preserving audit and extraction of digital contents," *IACR Cryptology ePrint Archive*, vol. 2008, p. 186, 2008.
[17] R. Gennaro, J. Katz, H. Krawczyk, and T. Rabin, "Secure network coding over the integers," in *International Conference on Practice and Theory in Public-Key Cryptography (PKC)*, 2010, pp. 142–160.
[18] A. G. Dimakis, K. Ramchandran, Y. Wu, and C. Suh, "A survey on network codes for distributed storage," *Proceedings of the IEEE*, vol. 99, no. 3, pp. 476–489, 2011.
[19] A. G. Dimakis, P. B. Godfrey, Y. Wu, M. J. Wainwright, and K. Ramchandran, "Network coding for distributed storage systems," *IEEE Transactions on Information Theory*, vol. 56, no. 9, pp. 4539–4551, 2010.
[20] Y. Hu, P. P. Lee, and K. W. Shum, "Analysis and construction of functional regenerating codes with uncoded repair for distributed storage systems," *IEEE International Conference on Computer Communications (INFOCOM)*, 2013.

