ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 9, April 2017

A Network Coding Approach for Enhanced Storage Security in Cloud Computing

[1]B.Bhargavi [2]B.Ravinder Reddy[3]G.Vishnu Murthy

[1]M.Tech Student, Software Engineering,Anurag Group of Institutions,Ghatkesar,Medchal District,Telangana.
Mail id: bhargaviemireddy@gmail.com
[2]Assistant Professor,CSE Dept,Anurag Group of Institutions, Ghatkesar,Medchal District, Telangana.
Mailid :ravinderreddycse@cvsr.ac.in
[3]Head of Dept.CSE Dept,Anurag Group of Institutions, Ghatkesar,Medchal District, Telangana.
Maid id:hodcse@cvsr.ac.in

ABSTRACT:

By making use of Cloud storage platform, varioususers can remotely save their data from any place and experience the on-demand high essence applications and offerings from a shared pool of configurable computing sources, without the overhead of neighborhood data storage and protection. However, the reality that users will no longer have physical ownership of the outsourced information makes the information integrity safety in Cloud computing a formidable challenge, mainly for customers with limited computing sources.The principle in the back of network coding is to permit intermediate nodes to re-encode packets. Compared to other conventional methods, coding makes most appropriate use of the available network sources and computing a scheme that achieves such rate is computationally simple.Despite the fact that the two areas are quite unique of their nature and are studied independently, we prove the way to construct a comfortable cloud storage protocol given any secure network coding protocol. This gives a direction to a scientific way to construct comfortable cloud data storage protocols. Our creation is strong and secure under a definition which captures the real world usage of the cloud storage space. Moreover, we advise particular secure cloud storage protocols primarily based on two latest secure network coding protocols. Mainly, we acquire very first publicly verifiable secure cloud data storage protocol in the well known model.

I. INTRODUCTION

cloud computing has been estimated as the next era information technology architecture for organizations due to its long listing of remarkable benefits within the IT history: on-demand self-service, ubiquitous network accessibility, location independent useful

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 9, April 2017

resource pooling, fast resource elasticity, usage-primarily based pricing and transference of hazard. As a disruptive era with profound implications, Cloud Computing is reworking the very nature of how organizations use data technology. One fundamental aspect of this paradigm transferring is that data is being centralized or outsourced to the Cloud. From users' perspective, such as both individuals and IT organizations, storing information remotely to the cloud in a flexible on-demand manner brings attractive advantages: relief of the load for storage control, everyday data get admission to with unbiased geographical locations, and avoidance of capital expenditure on hardware, software program, and personnel maintenances, and many others.

However previous reports suggest that information loss can arise cloud storage providers. Therefore, the trouble of checking the integrity of the data records in cloud storage, which we referred to as secure cloud storage (SCS), has attracted plenty of interest. On the other side hand, networking coding, which become proposed to enhance the network capability, additionally faces the problem of integrity checking. An intermediate router may deliberately pollute codewords, which leads to deciphering failures on the endpoints. Checking the integrity of codewords is referred to as the secure network coding problem. Various researchers have studied comfortable cloud storage and secure network coding independently.

The inspiration of data integrity checking lies in several elements. First, because of the poor control of the cloud, the user's data records will be lost due to device failures (hardware or software program). To hide the problem, the cloud might also choose to misinform the user. The second point is, the cloud has a massive economic incentive to discard the information that is not often accessed through the data users. Ignoring some part of the records helps the cloud to reduce its price. Third, a cloud can also be hacked and the records may be changed. Fourth, a cloud can also behave maliciously because of numerous feasible government pressures. Without a comfortable cloud storing protocol, the prevalence of those incidents can be hidden by cloud and gone neglected.The primary characteristic of a secure cloud storage protocol is that the user can test the data integrity with out owningthe actual records. Conventional strategies based on hash, message authentication codes (MACs), and digital signatures would require the user to save the data regionally.

In context of this paper, for the first time, we study a relationship among those special areas, i.e., secure cloud storage and secure network

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 9, April 2017

coding. Our essential end result is that we are able to construct a publicly verifiable strong and secure cloud storage protocol given any publicly verifiable comfortable and secure linear network coding protocol.

II. RELATED WORK

Network coding is a unique mechanism proposed in the few past years to enhance the throughput utilization of a given network topology. The principle behind network coding is to permit intermediate nodes to re-encode packets. In comparison to different conventional strategies, network coding makes most suitable use of the available networking resources and computing a scheduling scheme that achieves such data rate is computationally clean. An evaluation of network coding and a discussion of viable internet programs are given in the past. With network coding, on every occasion a user desires to send a packet to every other client, the source user generates and sends a linear combination of all (or part) of the data accessible to it (in addition to XORing a couple of packets). After clients receive enough linearly impartial mixtures of packets, they are able to reconstruct the unique facts. The gain we assume to get with the aid of the use of community coding is due to the randomization introduced every time we generate a new encoded block. If at least one of the mixed blocks is of use to different nodes down the direction, then the linear combination will additionally be beneficial. Network coding minimizes the reaction time in the absence of a centralized scheduler that makes a decision which node wills ahead which part of the content.

Some of previous works constructed on the proof of retrievability.A POR allows detection of tampering or deletion of a remotely positioned document—or relegation of the document to storage with unsure provider quality. A POR does no longer itself, however, protection against loss of document contents. Document robustness requires a few form of storage redundancy and, within the face of capable system failures, needs the distribution of a report throughout more than one system. Even though a POR best aims at detection of record corruption or loss, and no longer prevention, it is able to work hand-in-hand with strategies for document robustness. For example, a consumer may also select to disperse a file throughout more than one service vendors. By executing PORs with those carriers, the user can come across faults or lapses in service essence. She will be able to consequently re-distribute her file throughout service providers to reinforce its robustness and availability. In peer-to-peer environments, wherein provider service quality

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 9, April 2017

may be unreliable, such dynamic reallocation of sources may be especially essential.

Ateniese et al. proposed the concept of provable data ownership which uses homomorphic authentication information. More or less, computation can be finished on a collection of facts blocks, such that a brand new authenticator can be computed from the same computation on their authentications. The consumer can then audits the cloud storage by asking the cloud to send back some computation of the randomly chosen records blocks and an authentication of the computed result. If the authentication is accurate, the cloud stores the consumer's records intact. [6] discussed about a method, End-to-end inference to diagnose and repair the data-forwarding failures, our optimization goal to minimize the faults at minimum expected cost of correcting all faulty nodes that cannot properly deliver data. First checking the nodes that has the least checking cost does not minimize the expected costin fault localization. We construct a potential function for identifying the candidate nodes, one of which should be first checked by an optimal strategy. We proposes efficient inferring approach to the node to be checked in large-scale networks.

III. FRAMEWORK

In our proposed model we construct a secure cloud storage system by integrating the strong encoding technology called secure network coding to protect the data security in cloud storage systems.

A. Secure Cloud Storage Model

In our secure storage system, there will be two entities called, user and cloud. A User can be an individual, or an organization using a personal computer or a mobile device, etc.; a cloud may be any CSP like Amazon, Google Drive, IBM cloud etc. A user initially outsources its data to the cloud server. Later, the user will periodically perform audit on integrity of outsourced data in cloud. The user can then verify whether the proof which is sent from the cloud is generic and valid or not, i.e. the data remains perfect, or obtaining proof that a data has been tampered or corrupted which will possibly lead some later action (out of our scope), such as legal action or data recovery from storage devices.

Our secure cloud storage model that allows a user to verify the integrity of the storage data is to be perfect, highly secure and efficient.

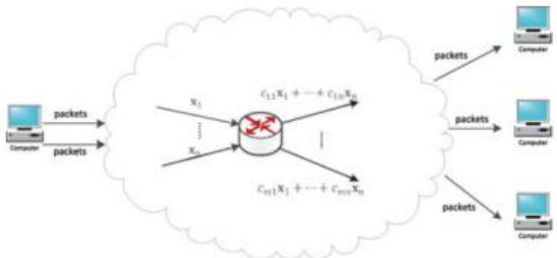


Fig.1. SNC Model

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 9, April 2017

B. Our Proposed Secure Network Coding Model:

In our SNC model there will be three involving entities called sender, router and a receiver. A sender desires to broadcast a few data packets to a institution of receivers. The sender divides the data file into packets and sends a linear aggregate of the packets via the network path. A router inside the network additionally sends a linear collection of the received data packets to its next hops. Whilst a receiver obtains enough encoded information packets, it could decode them to get better the unique data through solving a device of linear equations. To avoid a malicious router from editing a packet, the sender attaches a few authentication data with every information packet. When a router gets a sequence of packets, the router first checks their correctness, then combines the obtained accurate packets, and subsequently sends out the blended packet collectively with the combined authentication statistics. The grouped authentication data is computed in keeping with the details of a specific protocol.

SNC protocol has four efficient algorithms.

Those are:

i. Key Generation Algorithm
ii. Authentication Algorithm
iii. Combine Algorithm and
iv. Verify Algorithm.

Key Generation Algorithm:

This algorithm takes a security parameter value α and this algorithm run by a sender in order to generate a secret key SK and also a public key PK to allow authentication of packets in the network.

Authentication Algorithm:

This algorithm takes input as a data packet which is totransferred in the network. This algorithm is being run by sender to create the authentication information and then sends the packets in the network.

Combine Algorithm:

It takes input as group of data packets and the authentication information, this algorithm is executed in router to construct a combined packet with series of multiple coefficients and combined authentication information.

Verify Algorithm:

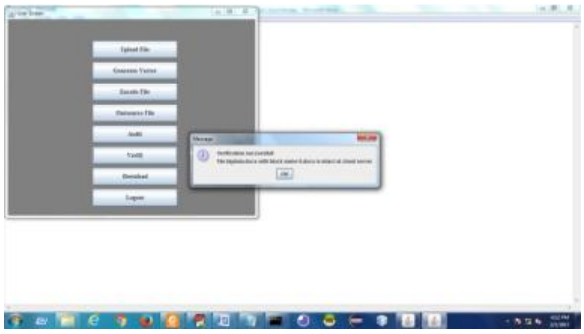
Takes input packet and the corresponding authentication information, it is being run by router or receiver to inspect if the data packet is edited maliciously. If the packet is not modified, this algorithm returns confirmation as μ=1 otherwise μ=0.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

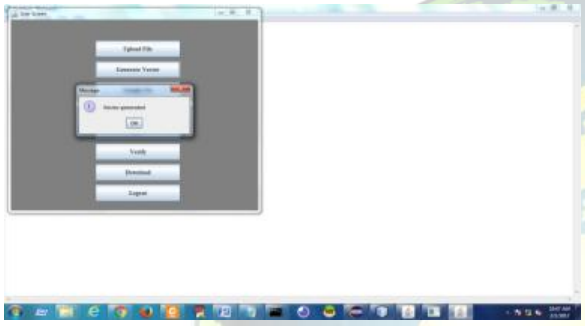
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 9, April 2017

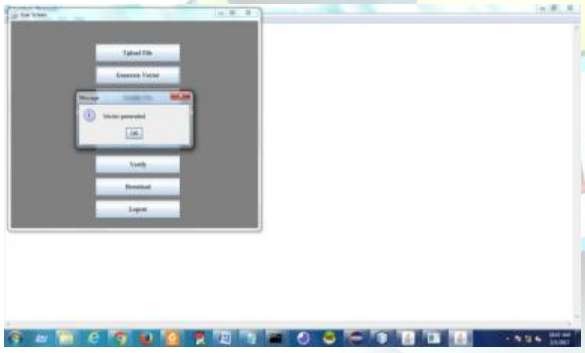
IV. EXPERIMENTAL RESULTS

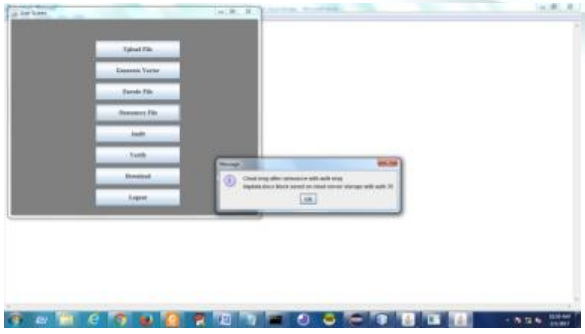
In this paper for the first time we integrate network coding and secure cloud storage. Our protocol can provide the strong security and high data throughput in order to achieve goal of our model and system.



The experimental results are shown below:







V. CONCLUSION

We monitor a relationship among secure cloud storage and secure network coding for the first time. Primarily based on the relationship, we endorse a scientific way to assemble a popular secure cloud data storage protocol primarily based on any secure network coding protocol. As a result, we achieve the first publicly verifiable and highly secure cloud storage protocol that is comfortable with out the usage of the random oracle heuristic. in addition, we improve our widespread construction to guide consumer anonymity and third-party public auditing. We are hoping our open sourced prototype could make a step toward realistic use of relaxed cloud storage protocols.

REFERENCES:

[1] Y. News. (2013). Cloud computing users are losing data, symantec finds [Online]. Available: http://finance.yahoo.com/news/

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 9, April 2017

cloud-computing-users-losing-data 205500612.html

[2] P. Hernande. (2013). Byod, data loss top list of cloud computing challenges [Online]. Available: http://www.datamation.com/ cloud-computing/byod-data-loss-top-list-of-cloud-computingchallenges.html

[3] A. Juels and B. KaliskiJr, "PORs: Proofs of retrievability for large files," in Proc. ACM Conf. Comput. Commun. Security, 2007, pp. 584–597.

[4] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proc. ACM Conf. Comput. Commun. Security, 2007, pp. 598–609.

[5] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacypreserving public auditing for secure cloud storage," IEEE Trans. Comput., vol. 62, no. 2, pp. 362–375, Feb. 2013.

[6] Christo Ananth, Mary Varsha Peter, Priya.M., Rajalakshmi.R., Muthu Bharathi.R., Pramila.E., "Network Fault Correction in Overlay Network through Optimality", International Journal of Advanced Research Trends in Engineering and Technology (IJARTET), Volume 2, Issue 8, August 2015, pp: 19-22.

[7] C. Gkantsidis and P. R. Rodriguez, "Cooperative security for network coding file distribution," in Proc. IEEE Int. Conf. Comput.Commun., 2006, pp. 1–13.

[8] H. Shacham and B. Waters, "Compact proofs of retrievability," in Proc. Int. Conf. Theory Appl. Cryptol. Inf. Security, 2008, pp. 90–107.

[9] J. Xu and E.-C.Chang, "Towards efficient proofs of retrievability," in Proc. ACM Symp.Inf., Comput.Commun. Security, 2012, pp. 79–80.

[10] K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 9, pp. 1717–1726, Sep. 2013.

[11] R. Ahlswede, N. Cai, S.-Y. Li, and R. W. Yeung, "Network information flow," IEEE Trans. Inf. Theory, vol. 46, no. 4, pp. 1204–1216, Jul. 2000.

[12] S.-Y. Li, R. W. Yeung, and N. Cai, "Linear network coding," IEEE Trans. Inf. Theory, vol. 49, no. 2, pp. 371–381, Feb. 2003.