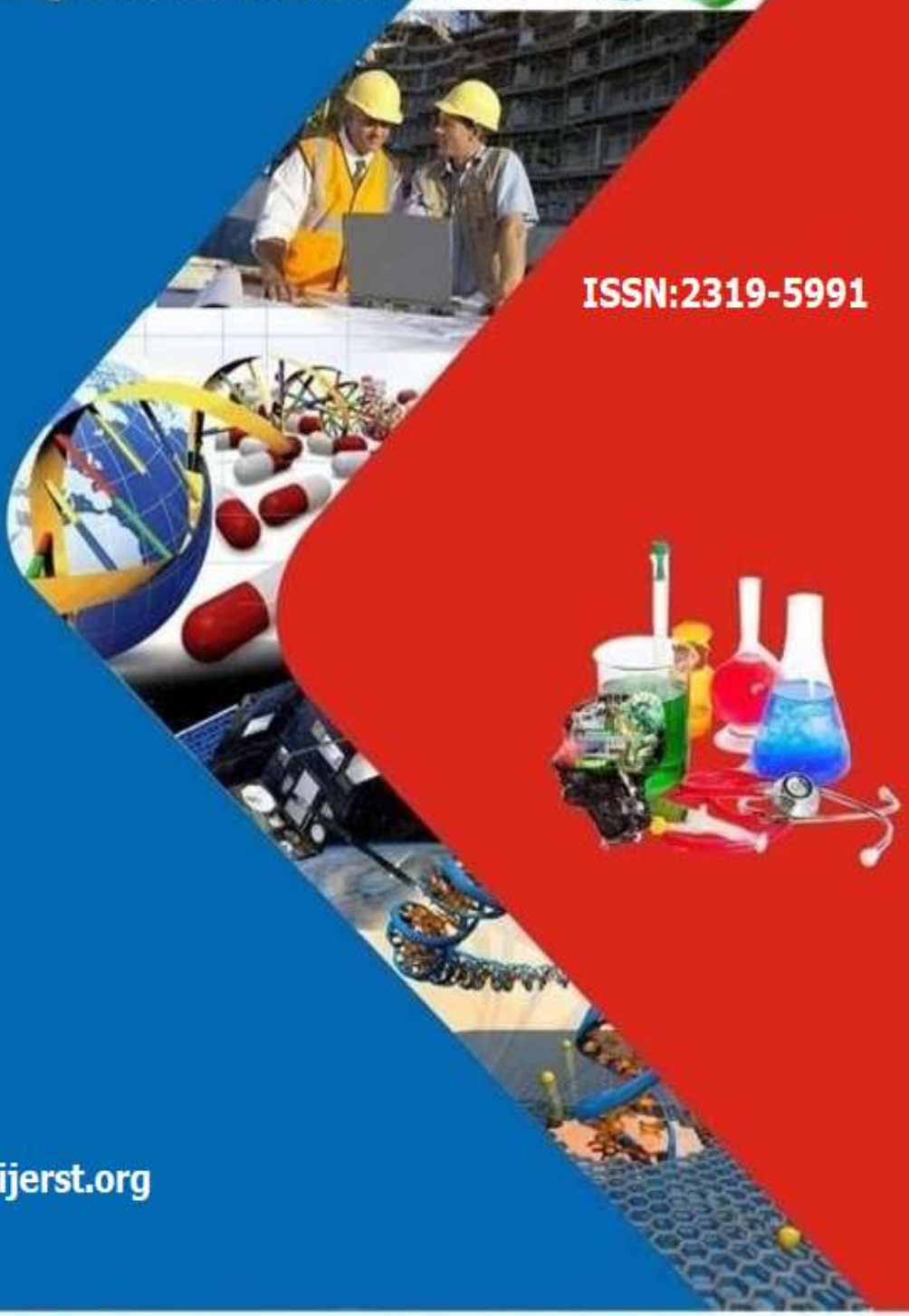
International Journal of Engineering Research and Science & Technology

IJERST

ISSN:2319-5991



www.ijerst.org

E-mail: editor@ijerst.org or ijerst.editor@gmail.com

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

PROTECTING CLOUD DATA WITH DYNAMIC SECURITY VIA NETWORK CODING

1 Ms. T. GLORY, 2 B. DIVYA, 3 E. VENKATESH

4 G. KEERTHANA, 5 S. AKSHAI KUMAR

1Assistant Professor, Department of CSIT, Sri Indu College of Engineering and Technology-Hyderabad

2345Under Graduate, Department of CSIT, Sri Indu College of Engineering and Technology-Hyderabad

ABSTRACT

In the age of cloud computing, cloud users with limited storage can outsource their data to remote servers. These servers, in lieu of monetary benefits, offer retrievability of their clients' data at any point of time. Secure cloud storage protocols enable a client to check integrity of outsourced data. In this work, we explore the possibility of constructing a secure cloud storage for dynamic data by leveraging the algorithms involved in secure network coding. We show that some of the secure network coding schemes can be used to construct efficient secure cloud storage protocols for dynamic data, and we construct such a protocol (DSCS I) based on a secure network coding protocol. To the best of our knowledge, DSCS I is the first secure cloud storage protocol for dynamic data constructed using secure network coding techniques which is secure in the standard model. Although generic dynamic data support arbitrary insertions, deletions and modifications, append-only data find numerous applications in the real world. We construct another secure cloud storage protocol (DSCS II) specific to append-only data — that overcomes some limitations of DSCS I. Finally, we provide prototype implementations for DSCS I and DSCS II in order to evaluate their perform.

Keywords: **Cloud Computing, Data Security**

I. INTRODUCTION

Cloud computing allows clients to delegate computation and data storage to cloud servers. However, malicious servers can delete infrequently accessed data. Secure cloud storage protocols, classified as static (SSCS) and dynamic (DSCS), detect untampered data storage. Clients can audit outsourced data without accessing the entire file, detecting unwanted changes by malicious servers. These protocols can be publicly verifiable or privately verifiable, depending on the third-party auditor's needs. These protocols are crucial for protecting client data and ensuring data security. For example, a client having a smart phone with a low- performance processor or limited storage cannot accomplish heavy computation or store large volume of data. Under such circumstances, she can delegate her computation/storage to the cloud server.In case of storage outsourcing, Cloud servers store massive data on behalf ofclients, but malicious servers can delete some data to save space. Secure cloudstorage protocols provide a mechanism to detect if the server stores the client's data untampered. These protocols are classified as secure cloud storageprotocols for static data (SSCS) and for dynamic data (DSCS). For static

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

data,the client cannot change their data after the initial outsourcing, while for dynamic data, the client can modify their data as often as needed. Secure cloud storage protocols are publicly verifiable if an audit can be performed by any third party auditor (TPA) using public parameters, or privately verifiable if an auditor needs secret information of the client. Network coding protocols, which combine incoming packets to output another packet, enjoy higher throughput, efficiency, and scalability than store-and-forward routing. However, they are prone to pollution attacks by malicious intermediate nodes injecting invalid packets. Secure network coding (SNC) protocols use cryptographic techniques to prevent these attacks. This work investigates theproblem of constructing a secure cloud storage protocol for dynamic data (DSCS) from a different perspective. Network coding techniques have been used to construct distributed storage systems, but they primarily aim to reducerepair bandwidth when some servers fail. The study explores whether the algorithms involved in an SNC protocol can be exploited to construct an efficient and secure cloud storage protocol for dynamic data.

Our Contribution:

Our major contributions in this work are summarized as follows

•We explore the possibility of providing a generic construction of a DSCS protocol from any SNC protocol. We discuss the challenges for a generic construction in details and identify some SNC protocols suitable for constructing efficient DSCS protocols.

•We construct a publicly verifiable DSCS protocol (DSCS I) from an SNC protocol DSCS I handles dynamic data, i.e., a client can efficiently performupdates (insertion, deletion and modification) on the outsourced data. We discuss the (asymptotic) performance and certain limitations of DSCS I.

•We provide the formal security definition of a DSCS protocol and prove thesecurity of DSCS

•We construct such a publicly verifiable secure cloud storage protocol (DSCS II) for append-only data by using an SNC protocol proposed by Boneh et al.

II. LITERATURE SURVEY

Cloud service providers offer storage outsourcing facility to their clients. In a secure cloud storage (SCS) protocol, the integrity of the client's datais maintained. In this work, we construct a publicly verifiable secure cloud storage protocol based on a secure network coding (SNC) protocol where the client can update the outsourced data as needed. To the best of our knowledge, our scheme is the first SNC-based SCS protocol for dynamic data that is securein the standard model and provides privacy-preserving audits in a publicly verifiable setting. Furthermore, we discuss, in details, about the (impossibility of providing a general construction of an efficient SCS protocol for dynamic data (DSCS protocol) from an arbitrary SNC protocol. In addition, we modify an existing DSCS scheme (DPDP I) in order to support privacy-preserving audits. We also compare our DSCS protocol with other SCS schemes (including the modified DPDP I scheme). Finally, we figure out some limitations of

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

an SCS scheme constructed using an SNC protocol.

We introduce a new class of problems called network information flow which is inspired by computer network applications. Consider a point-to- point communication network on which a number of information sources are to be multicast to certain sets of destinations. We assume that the information sources are mutually independent. The problem is to characterize the admissible coding rate region. This model subsumes all previously studied models along the same line. We study the problem with one information source, and we have obtained a simple characterization of the admissible coding rate region. Our result can be regarded as the max-flow min-cut theorem for network information flow.Contrary to one's intuition, our work reveals that it is in general not optimal to regard the information to be multicast as a "fluid" which can simply be routed orreplicated. Rather, by employing coding at the nodes, which we refer to as network coding, bandwidth can in general be saved. This finding may have significant impact on future design of switching systems

Consider a communication network in which certain source nodes multicast information to other nodes on the network in the multihop fashion where every node can pass on any of its received data to others. We are interested in how fast each node can receive the complete information, or equivalently, what the information rate arriving at each node is. Allowing a node to encode its received data before passing it on, the question involves optimization of the multicast mechanisms at the nodes. Among the simplest coding schemes is linear coding, which regards a block of data as a vector overa certain base field and allows a node to apply a linear transformation to a vectorbefore passing it on. We formulate this multicast problem and prove that linear coding suffices to achieve the optimum, which is the max-flow from the sourceto each receiving node.

III. SYSTEM ANALYSIS

EXISTING SYSTEM

We look at the problem of constructing a secure cloud storage protocol for dynamic data (DSCS) from a different perspective. We investigate whether we can construct an efficient DSCS protocol using an SNC protocol. In a previous work, Chen et al. reveal a relationship between secure cloudstorage and secure network coding. In particular, they show that one can exploit some of the algorithms involved in an SNC protocol in order to construct a secure cloud storage protocol for static data. However, their construction does not handle dynamic data that makes it insufficient in many applications where a client needs to update (insert, delete or modify) the remote data efficiently. Further investigations are needed towards an efficient DSCS construction using a secure network coding (SNC) protocol.

Network coding techniques have been used to construct distributed storage systems where the client’s data are disseminated across multiple servers. However, they primarily aim to reduce the repair bandwidth when some of the servers fail. On theother hand, we explore whether we can exploit the algorithms involved in an SNC protocol to construct an efficient and secure cloud storage protocol for dynamic data (for a single storage server).

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

DISADVANTAGES

1.A client having a smart phone with a low-performance processor or limited storage cannot accomplish heavy computation or store large volume of data. Under such circumstances, she can delegate her computation/storage to the cloud server. Secure cloud storage protocols enable a client to check integrity of outsourced data.

2.For static data, the client cannot change her data after the initial outsourcing (e.g., backup/archival data)

PROPOSED SYSTEM

We explore the possibility of providing a generic construction of a DSCS protocol from any SNC protocol. We discuss the challenges for a generic construction in details and identify some SNC protocols suitable for constructing efficient DSCS protocols. We construct a publicly verifiable DSCS protocol (DSCS I) from an SNC protocol. DSCS I handles dynamic data, i.e., a client can efficiently perform updates (insertion, deletion and modification) on the outsourced data. We discuss the (asymptotic) performance and certain limitations of DSCS I. We provide the formal security definition of a DSCS protocol and prove the security of DSCS I. As append- only data are a special case of generic dynamic data, we can use DSCSI (which is based on) for append-only data. However, we identify some SNC protocols that are not suitable for building a secure cloud storage for generic dynamic data, butefficient secure cloud storage protocols for appendonly data can be constructed from them. We construct such a publicly verifiable secure cloud storage protocol (DSCS II) for append-only data by using an SNC protocol proposed by Boneh et al..We discuss the (asymptotic) performance of DSCS II which overcomes some limitations of DSCS I.We implement DSCS I and DSCS II and evaluate their performance based on storage overhead, computational cost and communication cost.

ADVANTAGES

1.Secure network coding (SNC) protocols use cryptographic techniques to prevent these attacks: the sender authenticates each packet by attaching a small tag to it.

2.We look at the problem of constructing a secure cloud storage protocol for dynamic data (DSCS) from a different perspective. We investigate whether we can construct an efficient DSCS protocol using an SNC protocol.

IV. IMPLEMENTATION

MODULE DESCRIPTION

Data Owner:-In this application the owner is one of the main module for uploading the files and view the uploads file which are uploaded by the owner before do all these operations the owner should register with the application and the owner should be authorized by the cloud.

TPA(Trusted Third Party):-The TPA is used to generate the Auditing Task for the requested users. Here the trapdoor should login directly with the application

Cloud Server:-The cloud is the main module to operate this project in the users activations, owner activation and also the cloud can check the following operations like search permission provides to the users, can check the top-k searched keyword,top-k similarity in chart, top-k searched keyword in chart. Primarily the cloud should login. Then only the cloud can perform the abovementioned actions.

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 21, Issue 2, 2025

V. RESULTS

HOME SCREEN

PROTECTING CLOUD DATA

CUSTOMER INTERFACE

VI. CONCLUSION

In this work, we have proposed a secure cloud storage protocol for dynamic data (DSCS I) based on a secure network coding (SNC) protocol. To the best of our knowledge, this is the first SNC- based DSCS protocol that is secure in the standardmodel and enjoys public verifiability. We have discussed some challenges while constructing an efficient DSCS protocol from an SNC protocol. We have also identified some limitations of an SNC-based secure cloud storage protocol for dynamic data. However, some of these limitations follow from the underlying SNC protocol used. A more efficient SNC protocol can give us a DSCS protocol with better efficiency. We have also identified certain SNC protocols suitable for append-only data and constructed an efficient DSCS protocol (DSCS II) for appendonly data. We have shown that DSCS II overcomes some limitations of DSCS I. Finally, we have provided prototype implementations of DSCS I and DSCS II in order to show their practicality and compared the performance of DSCSI with that of an SNC-based

REFERENCES

[1] B. Sengupta and S. Ruj, “Publicly verifiable secure cloud storage for dynamic data using secure network coding,” in ACM Asia Conference on Computer and Communications Security, 2016, pp. 107– 118.

[2] G. Ateniese, R. C. Burns, R. Curtmola, J. Herring, L. Kissner, Z. N. J. Peterson, and D. X. Song, “Provable data possession at untrusted stores,” in ACM Conference on Computer and Communications Security, 2007, pp. 598–609.

[3] A. Juels and B. S. Kaliski, “PORs: Proofs of retrievability for large files,” in ACM Conference on Computer and Communications Security, 2007, pp. 584–597.

[4] H. Shacham and B. Waters, “Compact proofs of retrievability,” Journal of Cryptology, vol. 26, no. 3, pp. 442–483, 2013.

[5] C. C. Erway, A. Kupc¸ ¨ u, C. Papamanthou, and R. Tamassia, ¨ “Dynamic provable data possession,” ACM Transactions on Information and System Security, vol. 17, no. 4, pp. 15:1–15:29, 2015.

[6] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, “Enabling public auditability and data dynamics for storage security in cloud computing,” IEEE Transactions on

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

Parallel and Distributed Systems, vol. 22, no. 5, pp. 847– 859, 2011.

[7] D. Cash, A. Kupc¸ ¨ u, and D. Wichs, "Dynamic proofs of ¨ retrievability via oblivious RAM," in EUROCRYPT, 2013, pp. 279–295.

[8] E. Shi, E. Stefanov, and C. Papamanthou, "Practical dynamic proofs of retrievability," in ACM Conference on Computer and Communications Security, 2013, pp. 325–336.