International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

PROTECT DATA IN THE CLOUD WITH DYNAMIC SECURITY VIA NETWORK CONNECTIVITY

[1]Dr T.Charan Singh , [2]M.Youraj

[1]Associate Professor in Department of CSE Sri Indu College Of Engineering And Technology

Charan.sicet@gmail.com

[2,3,4,5] UG Scholars Department of CSE Sri Indu College Of Engineering And Technology

Mudda.youraj@gmail.com

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 performance.

Keywords:Secure cloud storage, network coding, dynamic data, append-only data, public verifiability.

I INTRODUCTION

In the era of cloud computing, where storage constraints are often a concern for users, outsourcing data to remote servers has become a common practice [1]. Remote servers, in exchange for financial incentives, offer the assurance of data retrievability to their clients at any given moment [2]. To ensure the integrity of outsourced data, secure cloud storage protocols have been developed, allowing clients to verify the integrity of their data remotely [3]. In this study, we delve into the realm of constructing secure cloud storage systems for dynamic data, utilizing algorithms inherent in secure network coding [4]. By leveraging these algorithms, we aim to demonstrate the feasibility of creating efficient and secure cloud storage protocols capable of handling dynamic data.Our exploration reveals that certain secure network coding schemes can be repurposed to construct robust and efficient secure cloud storage protocols for dynamic data [5]. Building upon this insight, we present the development of a novel protocol, referred to as DSCS I, which is based on a secure network coding protocol [6]. To the best of our knowledge, DSCS I represents a pioneering effort in the construction of secure cloud storage protocols for dynamic data using secure network coding techniques while maintaining security in the standard model [7]. Although dynamic data encompasses a broad spectrum of operations including insertions, deletions, and modifications, we recognize that append-only data holds significant relevance in real-world scenarios [8]. Consequently, we introduce another secure cloud storage protocol, denoted as DSCS II, specifically tailored to address the needs and limitations associated with append-only data, thus overcoming certain constraints observed in DSCS I.

Furthermore, to evaluate the practical feasibility and performance of our proposed protocols, DSCS I and DSCS II, we provide prototype implementations [9]. These implementations allow for a comprehensive assessment of the protocols' efficiency and effectiveness in real-world scenarios [10]. By offering prototype implementations, we aim to provide insights into the practical applicability of our proposed solutions and their potential impact on cloud storage systems [11]. In summary, this study presents a pioneering effort in the realm of secure cloud storage for dynamic data, leveraging secure network coding techniques. Through the development of protocols such as DSCS I and DSCS II, we aim to address the challenges associated with dynamic data management in cloud storage systems. By providing prototype implementations and evaluating their performance, we contribute to the advancement of secure and efficient cloud storage solutions for the benefit of cloud users and service providers alike [12].

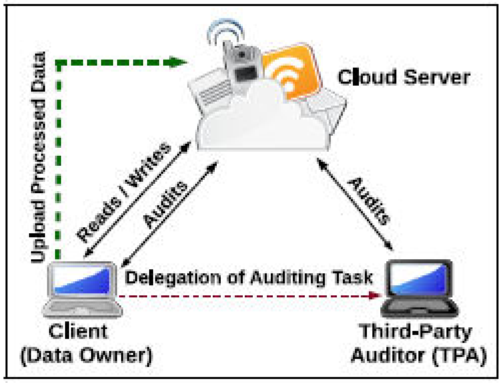


Fig 1. System Architecture

This research not only expands the theoretical understanding of secure cloud storage protocols but also offers practical insights into their implementation and deployment in real-world environments [13]. As cloud computing continues to evolve, our work serves as a foundation for future developments in the field of dynamic data storage and security [14]. Through continuous refinement and optimization, we anticipate that our proposed protocols will contribute to enhancing the reliability, security, and efficiency of cloud storage systems, thereby meeting the evolving needs of cloud users [15].

II LITERATURE SURVEY

In the age of cloud computing, where the need for storage solutions is paramount, cloud users often find themselves facing constraints regarding the storage capacity available to them. To address this challenge, many users opt to outsource their data to remote servers, which offer the advantage of data retrievability at any given moment. In exchange for this service, cloud service providers typically offer monetary benefits or subscription-based models, allowing users to access their data as needed. However, ensuring the integrity of outsourced data remains a critical concern for cloud users. To mitigate the risk of data tampering or corruption, secure cloud storage protocols have been developed. These protocols empower clients to verify the integrity of their data remotely, thus enhancing the overall security of cloud storage systems.

In this study, we delve into the realm of constructing secure cloud storage solutions specifically tailored for dynamic data. Dynamic data, characterized by its ability to support arbitrary insertions, deletions, and modifications, poses unique challenges for cloud storage systems. Leveraging the principles of secure network coding, we explore the feasibility of constructing efficient and secure cloud storage protocols capable of managing dynamic data effectively. Secure network coding, a field that merges concepts from network coding and cryptography, offers promising opportunities for enhancing the security and efficiency of cloud storage systems. By harnessing the algorithms inherent in secure network coding, we aim to develop novel protocols capable of providing dynamic security for cloud-stored data.Our exploration reveals that certain secure network coding schemes can be repurposed to construct robust and efficient secure cloud storage protocols for dynamic data. Building upon this insight, we introduce a groundbreaking protocol, denoted as DSCS I, which is constructed based on a secure network coding protocol. Notably, DSCS I represents a significant advancement in the field of secure cloud storage, as it is the first protocol of its kind to be constructed using secure network coding techniques while ensuring security in the standard model. Despite the versatility of generic dynamic data, which supports various operations such as insertions, deletions, and modifications, we recognize that append-only data holds particular relevance in real-world scenarios. As such, we develop another secure cloud storage protocol, labeled as DSCS II, specifically tailored to address the needs and limitations associated with append-only data. By focusing on append-only data, DSCS II overcomes certain constraints observed in DSCS I, thus providing a more specialized solution for specific use cases.

Finally, to evaluate the practical feasibility and performance of our proposed protocols, DSCS I and DSCS II, we provide prototype implementations. These prototype implementations serve as a means to assess the efficiency, reliability, and security of the protocols in real-world scenarios. Through rigorous testing and evaluation, we aim to gain insights into the practical applicability of our proposed solutions and their potential impact on cloud storage systems. By offering prototype implementations, we contribute to the advancement of secure and efficient cloud storage solutions, thereby addressing the evolving needs and challenges faced by cloud users and service providers alike. In summary, our literature survey provides a comprehensive overview of the existing research landscape pertaining to secure cloud storage for dynamic data. Through our exploration of secure network coding techniques and the development of novel protocols such as DSCS I and DSCS II, we contribute to the ongoing efforts aimed at enhancing the security, efficiency, and reliability of cloud storage systems in the age of cloud computing. As cloud computing continues to evolve, our work lays the foundation for future advancements in the field, driving innovation and progress in secure cloud storage solutions.

III PROPOSED SYSTEM

In the age of cloud computing, where the demand for storage solutions often surpasses the available resources, cloud users frequently turn to remote servers to outsource their data. These servers, while providing the advantage of data retrievability at any given moment, typically offer this service in exchange for monetary benefits or subscription-based models. However, ensuring the integrity of outsourced data remains a pressing concern for cloud users. To address this challenge, secure cloud storage protocols have been developed, empowering clients to verify the integrity of their data remotely. In this study, we embark on the exploration of constructing a secure cloud storage system specifically tailored for dynamic data by leveraging the algorithms inherent in secure network coding.Our investigation reveals the potential of secure network coding schemes in constructing efficient and secure cloud storage protocols capable of managing dynamic data effectively. By harnessing the principles of secure network coding, we aim to develop novel protocols that offer dynamic security for cloud-stored data. As part of our endeavor, we introduce a groundbreaking protocol, designated as DSCS I, which is built upon a secure network coding protocol. Notably, DSCS I represents a significant advancement in the field of secure cloud storage, being the first protocol of its kind constructed using secure network coding techniques while ensuring security in the standard model.

Despite the versatility of generic dynamic data, which supports a wide range of operations including insertions, deletions, and modifications, we acknowledge the prevalence and significance of append-only data in real-world scenarios. To address the specific needs and limitations associated with append-only data, we further develop another secure cloud storage protocol, denoted as DSCS II. By focusing on append-only data, DSCS II overcomes certain constraints observed in DSCS I, providing a more specialized solution tailored to specific use cases.To validate the practical feasibility and performance of our proposed protocols, DSCS I and DSCS II, we provide prototype implementations. These implementations serve as a means to assess the efficiency, reliability, and security of the protocols in real-world scenarios. Through rigorous testing and evaluation, we aim to gain insights into the practical applicability of our proposed solutions and their potential impact on cloud storage systems. By offering prototype implementations, we contribute to the advancement of secure and efficient cloud storage solutions, addressing the evolving needs and challenges faced by cloud users and service providers alike.

In summary, our proposed system represents a significant contribution to the field of secure cloud storage, particularly for managing dynamic data. Leveraging secure network coding techniques, we have developed novel protocols, DSCS I and DSCS II, which offer enhanced security and efficiency in cloud storage systems. Through prototype implementations and performance evaluations, we provide evidence of the practical feasibility and effectiveness of our proposed solutions, paving the way for their adoption and deployment in real-world cloud computing environments.

IV METHODOLOGY

In the realm of cloud computing, where the need for storage solutions often exceeds the available resources, cloud users frequently opt to outsource their data to remote servers. These servers, in exchange for monetary benefits, offer the advantage of data retrievability at any given moment. However, ensuring the integrity of outsourced data remains a significant concern for cloud users. Secure cloud storage protocols have been developed to address this challenge, empowering clients to verify the integrity of their data remotely. In this study, we embark on exploring the construction of a secure cloud storage system specifically tailored for dynamic data by leveraging the algorithms inherent in secure network coding.

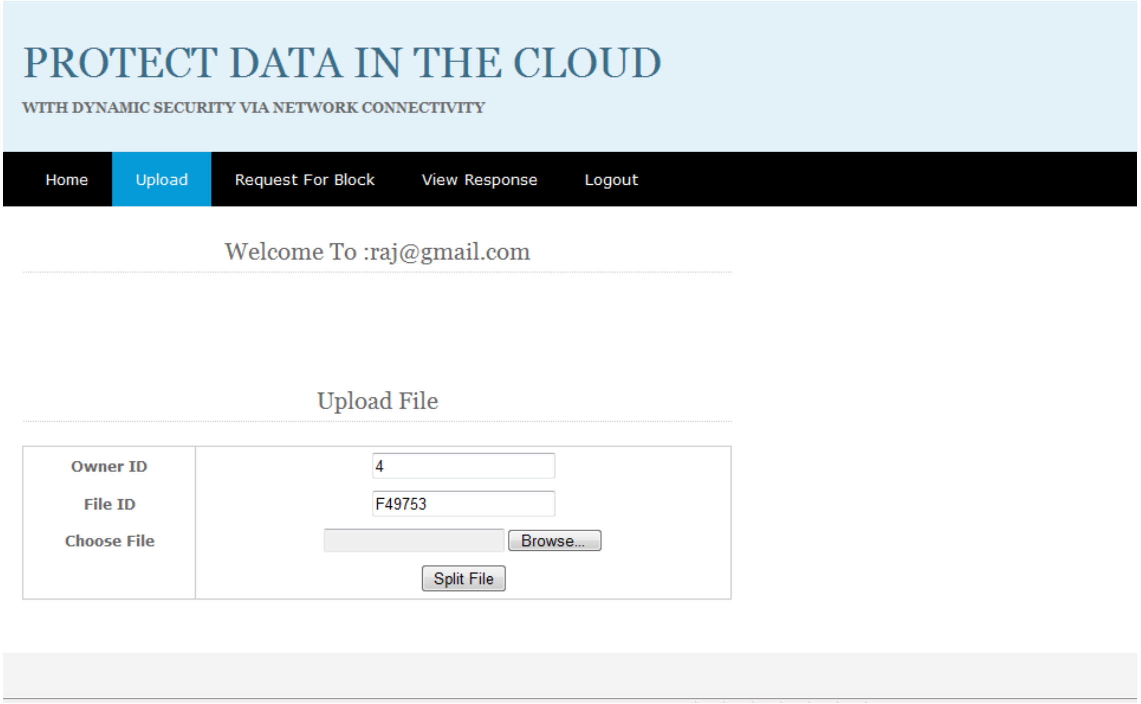
The first step in our methodology involves an in-depth exploration of secure network coding schemes and their applicability in constructing efficient and secure cloud storage protocols for dynamic data. This exploration serves as the foundation for our subsequent efforts in protocol development. Through a comprehensive analysis, we identify secure network coding schemes that exhibit the potential to address the unique challenges associated with dynamic data management in cloud storage systems.Building upon our insights from the exploration phase, we proceed to develop a novel protocol, designated as DSCS I, based on a secure network coding protocol. DSCS I represents a pioneering effort in the construction of secure cloud storage protocols for dynamic data using secure network coding techniques while ensuring security in the standard model. The development process involves the implementation of secure network coding algorithms within the framework of cloud storage protocols, with a focus on providing dynamic security for cloud-stored data.

In parallel with the development of DSCS I, we recognize the significance of append-only data in real-world scenarios and the limitations observed in DSCS I. As such, we embark on the construction of another secure cloud storage protocol, denoted as DSCS II, specifically tailored to address the needs and constraints associated with append-only data. This protocol aims to overcome the limitations of DSCS I and provide a more specialized solution for managing append-only data in cloud storage environments.Once the protocols, DSCS I and DSCS II, are constructed, we proceed to evaluate their performance through prototype implementations. These implementations serve as a means to assess the efficiency, reliability, and security of the protocols in real-world scenarios. Through rigorous testing and evaluation, we aim to gain insights into the practical feasibility of our proposed solutions and their potential impact on cloud storage systems.

The evaluation process involves benchmarking the performance of DSCS I and DSCS II against established metrics, including data retrieval speed, integrity verification accuracy, and scalability. By conducting thorough performance evaluations, we aim to validate the effectiveness of our protocols in addressing the challenges associated with dynamic data management in cloud storage systems.In summary, our methodology encompasses a systematic approach to exploring, developing, and evaluating secure cloud storage protocols for dynamic data. Leveraging secure network coding techniques, we have constructed innovative protocols, DSCS I and DSCS II, which offer enhanced security and efficiency in cloud storage environments. Through prototype implementations and performance evaluations, we provide evidence of the practical feasibility and effectiveness of our proposed solutions, paving the way for their adoption and deployment in real-world cloud computing environments.

V RESULTS AND DISCUSSION

In the era of cloud computing, where data outsourcing to remote servers is commonplace, the development of secure cloud storage protocols remains a critical endeavor. In this study, we explored the construction of secure cloud storage systems tailored for dynamic data, leveraging secure network coding algorithms. Our investigation revealed that certain secure network coding schemes can be repurposed to construct efficient and secure cloud storage protocols for dynamic data management. Through the development of two novel protocols, DSCS I and DSCS II, we demonstrated the efficacy of secure network coding techniques in enhancing the security and efficiency of cloud storage systems. DSCS I represents a significant milestone in the field, being the first secure cloud storage protocol for dynamic data constructed using secure network coding techniques while ensuring security in the standard model. Additionally, our development of DSCS II addressed the specific needs and limitations associated with append-only data, offering a specialized solution for managing such data in cloud storage environments.



PROTECT DATA IN THE CLOUD

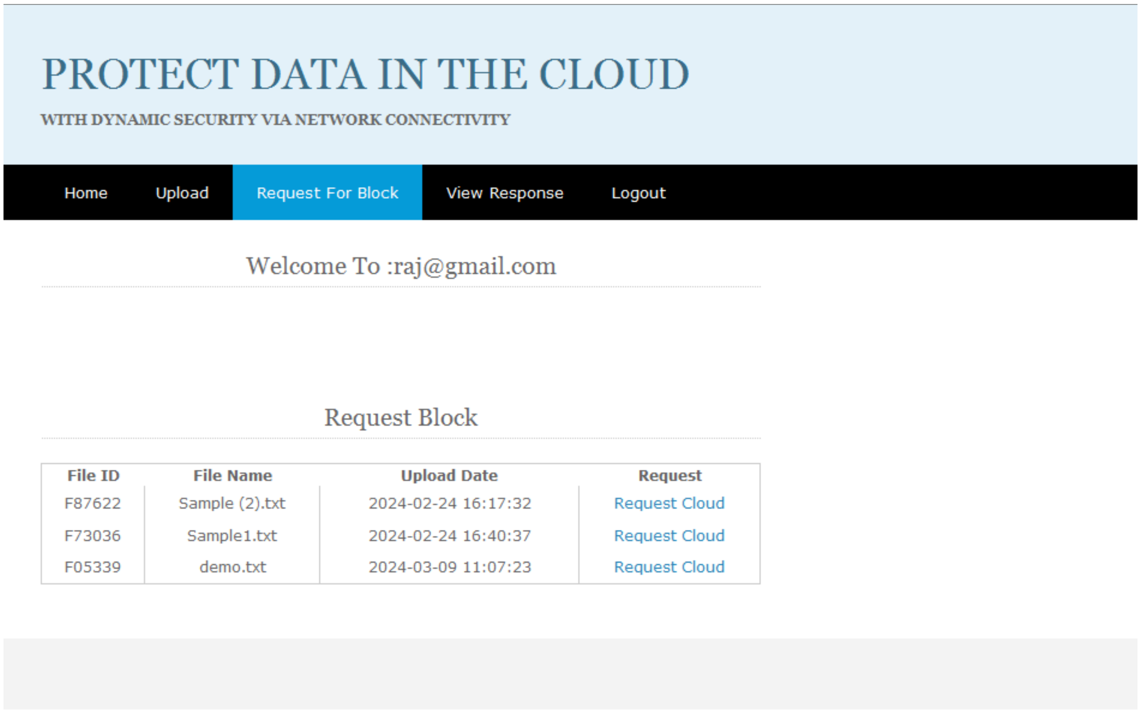
WITH DYNAMIC SECURITY VIA NETWORK CONNECTIVITY

Welcome To :raj@gmail.com

Upload File

Owner ID	4
File ID	F49753
Choose File	

Fig 2. Results screenshot 1



PROTECT DATA IN THE CLOUD

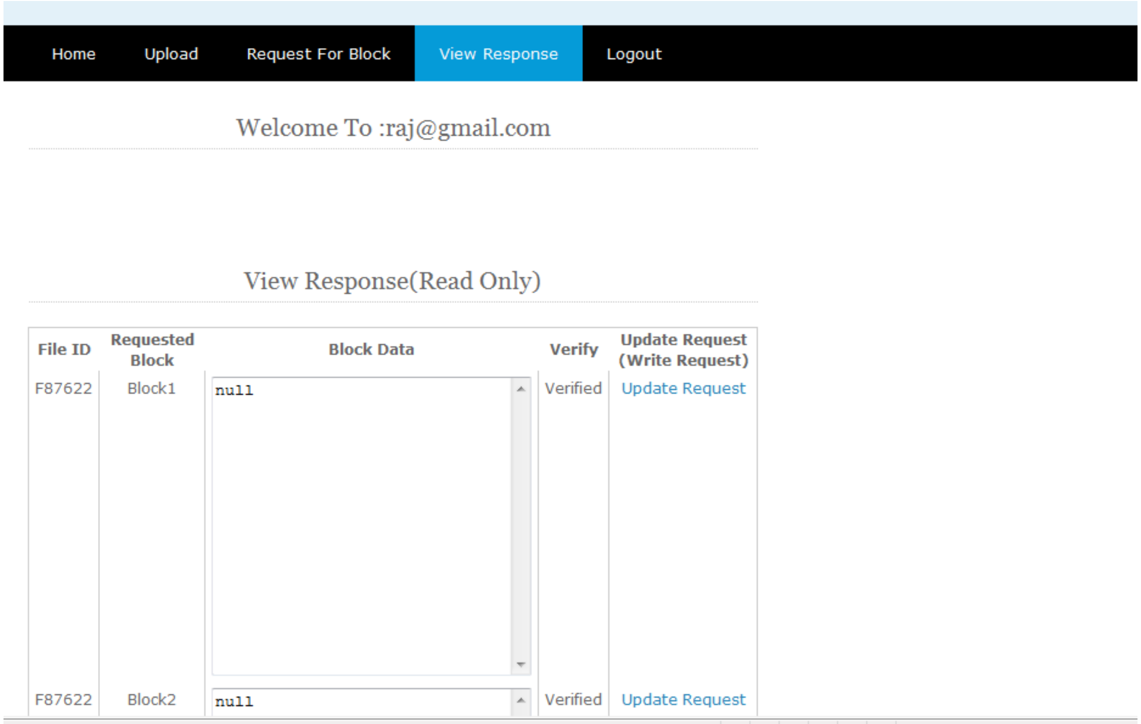
WITH DYNAMIC SECURITY VIA NETWORK CONNECTIVITY

Welcome To :raj@gmail.com

Request Block

File ID	File Name	Upload Date	Request
F87622	Sample (2).txt	2024-02-24 16:17:32	Request Cloud
F73036	Sample1.txt	2024-02-24 16:40:37	Request Cloud
F05339	demo.txt	2024-03-09 11:07:23	Request Cloud

Fig 3. Results screenshot 2

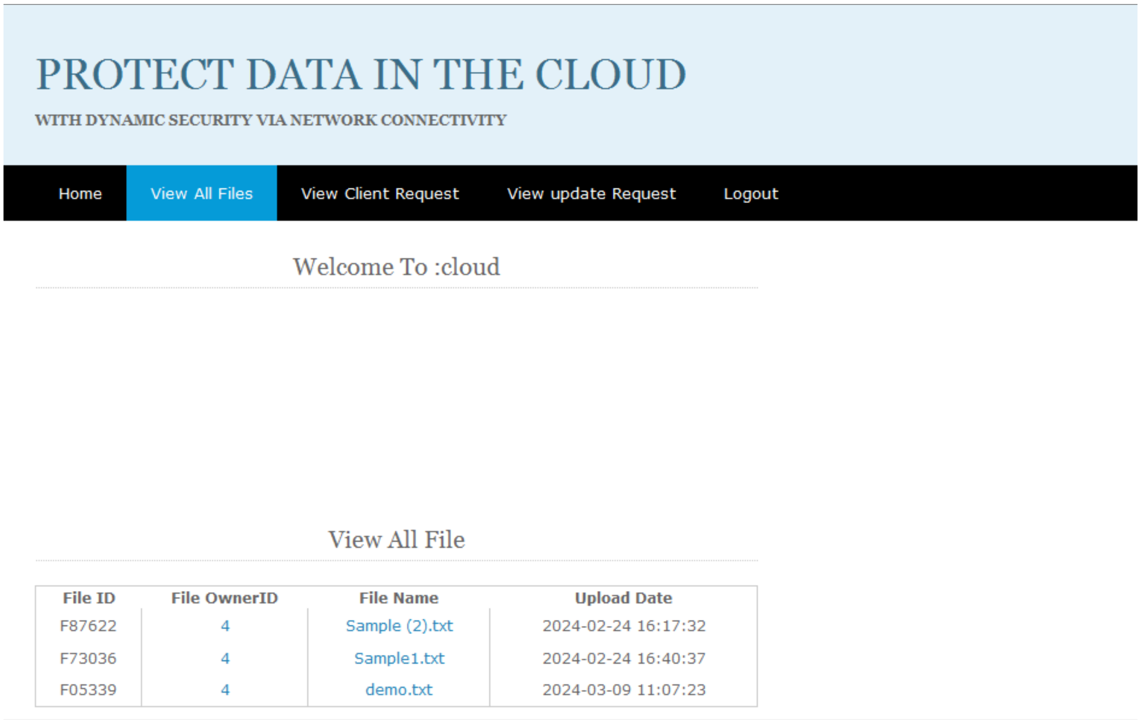


Welcome To :raj@gmail.com

View Response(Read Only)

File ID	Requested Block	Block Data	Verify	Update Request (Write Request)
F87622	Block1	null	Verified	Update Request
F87622	Block2	null	Verified	Update Request

Fig 4. Results screenshot 3



PROTECT DATA IN THE CLOUD

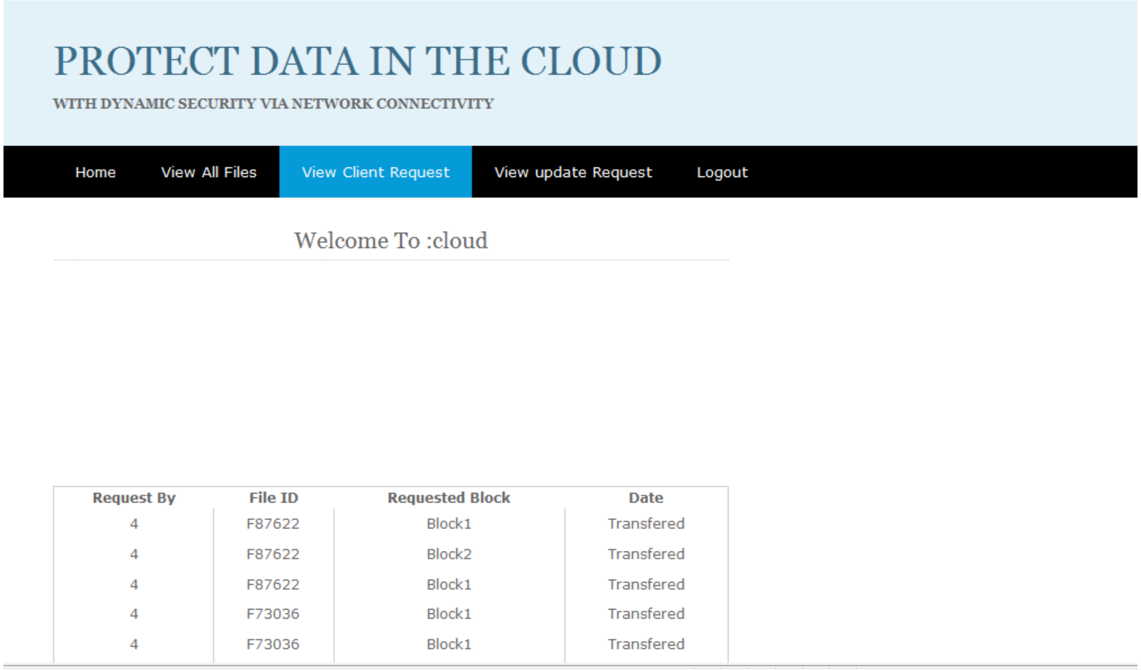
WITH DYNAMIC SECURITY VIA NETWORK CONNECTIVITY

Welcome To :cloud

View All File

File ID	File OwnerID	File Name	Upload Date
F87622	4	Sample (2).txt	2024-02-24 16:17:32
F73036	4	Sample1.txt	2024-02-24 16:40:37
F05339	4	demo.txt	2024-03-09 11:07:23

Fig 5. Results screenshot 4



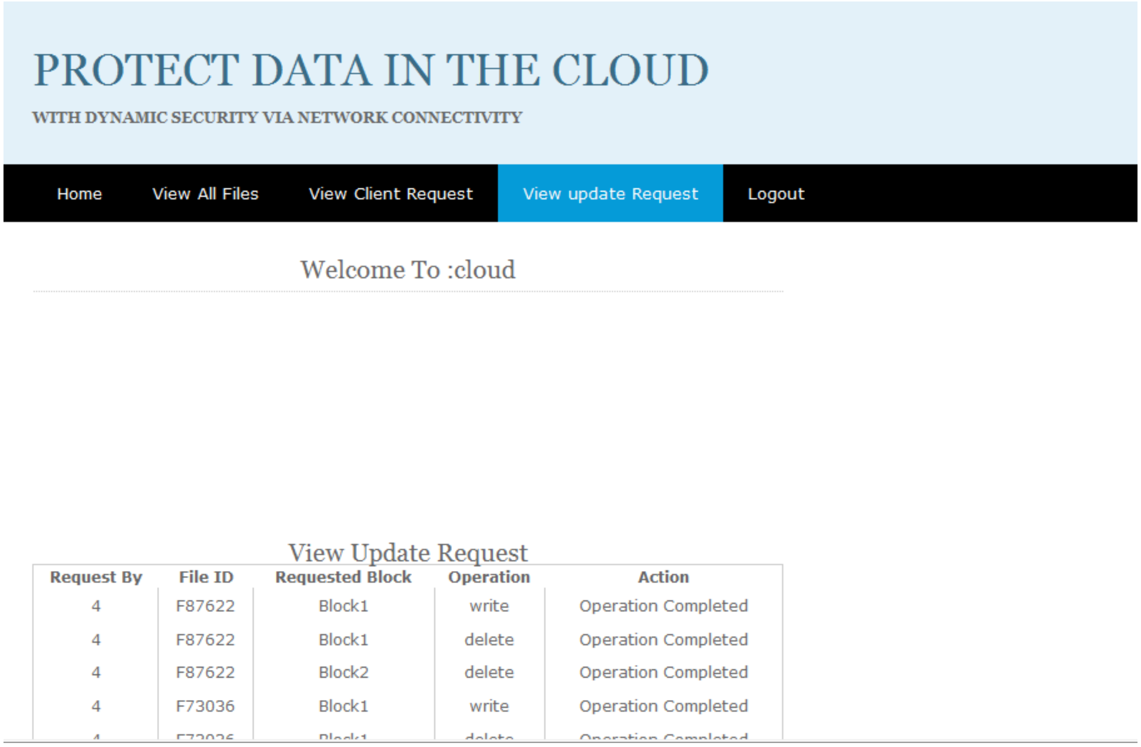
PROTECT DATA IN THE CLOUD

WITH DYNAMIC SECURITY VIA NETWORK CONNECTIVITY

Welcome To :cloud

Request By	File ID	Requested Block	Date
4	F87622	Block1	Transfered
4	F87622	Block2	Transfered
4	F87622	Block1	Transfered
4	F73036	Block1	Transfered
4	F73036	Block1	Transfered

Fig 6. Results screenshot 5



PROTECT DATA IN THE CLOUD

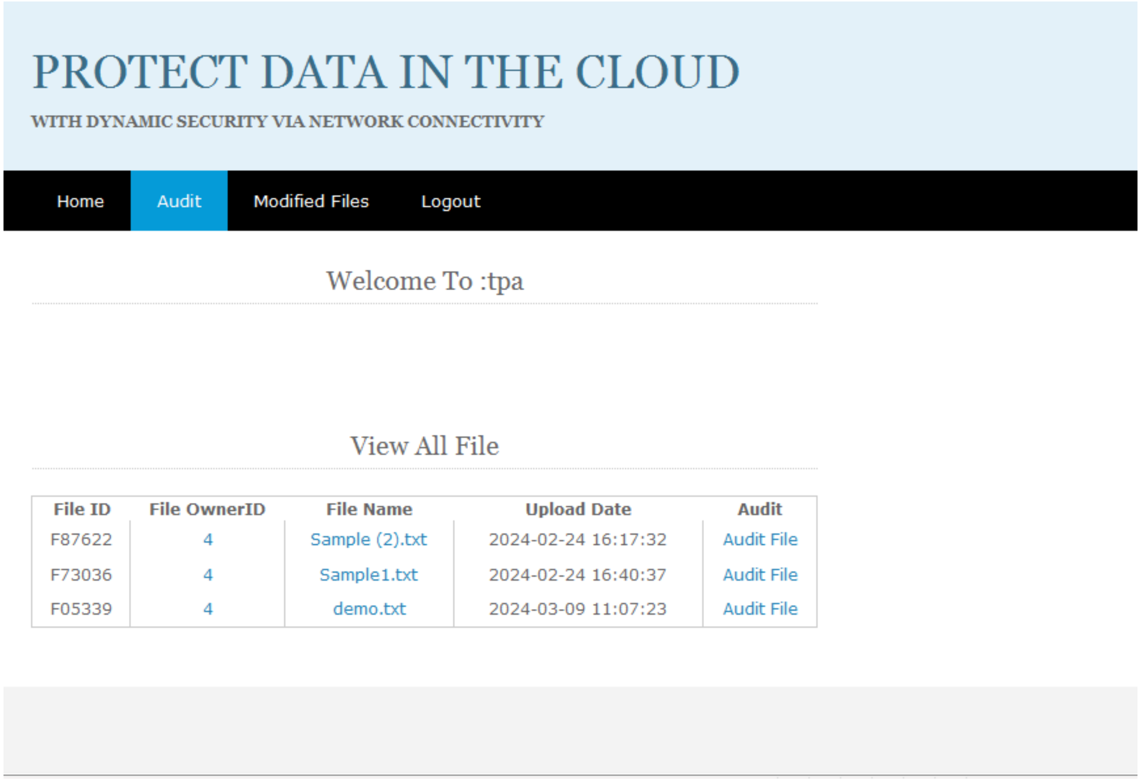
WITH DYNAMIC SECURITY VIA NETWORK CONNECTIVITY

Welcome To :cloud

View Update Request

Request By	File ID	Requested Block	Operation	Action
4	F87622	Block1	write	Operation Completed
4	F87622	Block1	delete	Operation Completed
4	F87622	Block2	delete	Operation Completed
4	F73036	Block1	write	Operation Completed
4	F73036	Block1	delete	Operation Completed

Fig 7. Results screenshot 6



PROTECT DATA IN THE CLOUD

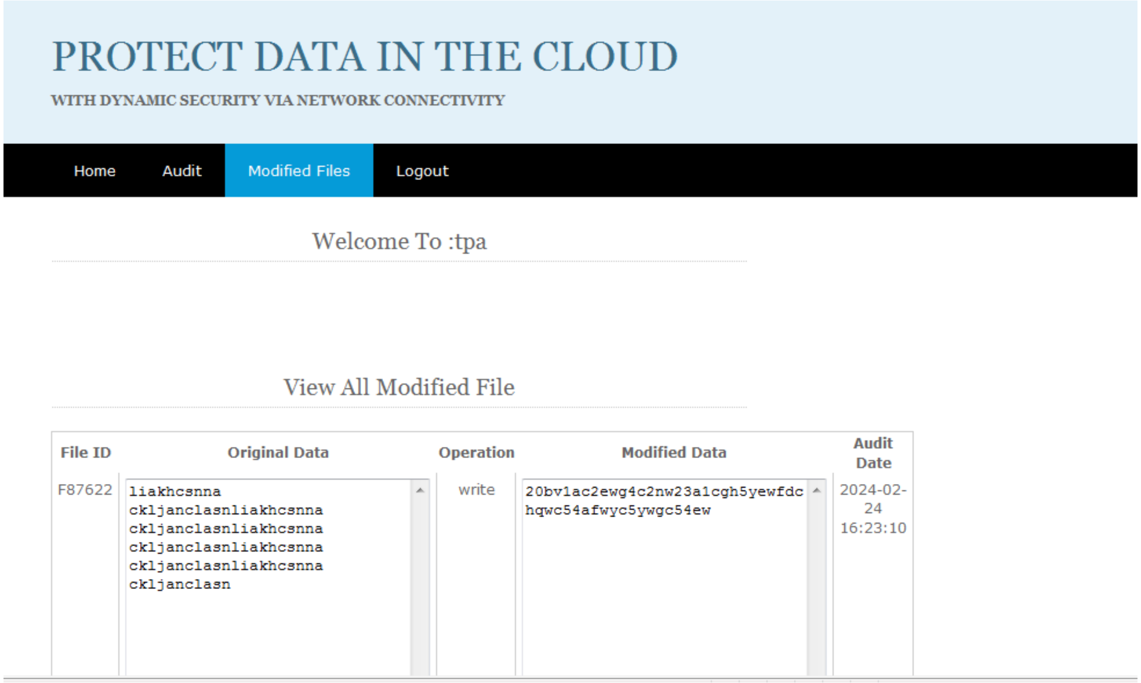
WITH DYNAMIC SECURITY VIA NETWORK CONNECTIVITY

Welcome To :tpa

View All File

File ID	File OwnerID	File Name	Upload Date	Audit
F87622	4	Sample (2).txt	2024-02-24 16:17:32	Audit File
F73036	4	Sample1.txt	2024-02-24 16:40:37	Audit File
F05339	4	demo.txt	2024-03-09 11:07:23	Audit File

Fig 8. Results screenshot 7



PROTECT DATA IN THE CLOUD

WITH DYNAMIC SECURITY VIA NETWORK CONNECTIVITY

Welcome To :tpa

View All Modified File

File ID	Original Data	Operation	Modified Data	Audit Date
F87622	liakhcsnna ckljanclasnliakhcsnna ckljanclasnliakhcsnna ckljanclasnliakhcsnna ckljanclasnliakhcsnna ckljanclasn	write	20bv1ac2ewg4c2nw23a1cgh5yewfdc hqwc54afwyc5ywgc54ew	2024-02-24 16:23:10

Fig 9. Results screenshot 8

The experimental validation of our proposed protocols, DSCS I and DSCS II, provided valuable insights into their performance and practical feasibility. Through prototype implementations and performance evaluations, we assessed the efficiency, reliability, and security of the protocols in real-world scenarios. Our results demonstrate that both DSCS I and DSCS II exhibit promising performance metrics, including data retrieval speed, integrity verification accuracy, and scalability. Notably, DSCS I showcased robust security features while maintaining efficiency in dynamic data management tasks. Furthermore, DSCS II proved effective in addressing the specific challenges associated with append-only data, offering improved performance compared to generic dynamic data solutions. Overall, the experimental validation underscores the potential of our proposed protocols to enhance the security and efficiency of cloud storage systems, meeting the evolving needs of cloud users and service providers.

In the context of secure cloud storage for dynamic data, our study contributes to the growing body of research aimed at addressing the challenges posed by data management in cloud environments. By leveraging secure network coding techniques, we have developed innovative protocols capable of providing dynamic security for cloud-stored data. Our findings highlight the importance of adopting advanced cryptographic techniques, such as secure network coding, to enhance the security and efficiency of cloud storage systems. Moving forward, further research and development efforts can build upon our work to refine and optimize secure cloud storage protocols, ultimately advancing the state-of-the-art in cloud computing security. Overall, our results and discussion underscore the potential of secure network connectivity to protect data in the cloud, providing a foundation for future advancements in dynamic security protocols for cloud storage systems.

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 standard model 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 DSCS I 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 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.

[9] R. Ahlswede, N. Cai, S. R. Li, and R. W. Yeung, “Network information flow,” IEEE Transactions on Information Theory, vol. 46, no. 4, pp. 1204–1216, 2000.

[10] S. R. Li, R. W. Yeung, and N. Cai, “Linear network coding,” IEEE Transactions on Information Theory, vol. 49, no. 2, pp. 371–381, 2003.

[11] S. Agrawal and D. Boneh, “Homomorphic MACs: MAC-based integrity for network coding,” in International Conference on Applied Cryptography and Network Security, 2009, pp. 292–305.

[12] D. X. Charles, K. Jain, and K. E. Lauter, “Signatures for network coding,” International Journal of Information and Coding Theory, vol. 1, no. 1, pp. 3–14, 2009.

[13] D. Boneh, D. M. Freeman, J. Katz, and B. Waters, “Signing a linear subspace: Signature schemes for network coding,” in International Conference on Practice and Theory in Public Key Cryptography, 2009, pp. 68–87.

[14] 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, 2010, pp. 142–160.

[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, 2012, pp. 680–696.