International Journal of Scientific Research in Science, Engineering and Technology

Print ISSN - 2395-1990
Online ISSN : 2394-4099

OPEN ACCESS

Available Online at : www.ijsrset.com
doi : https://doi.org/10.32628/IJSRSET2411255

An Optimized Data Storage in A Secure Cloud-Edge Collaboration : A Fault-Tolerance Approach

M. Manideepsai*[1] , U. Vineeth Goud[1], CH. Vinay Goud[1] , P. Vignesh Yadav[1], D. Saidulu[2]

[1]UG Student, Department of Computer Science and Engineering(Internet of Things), Guru Nanak Institutions Technical Campus, Hyderabad, Telangana, India

[2]Associate Professor, Department of Computer Science and Engineering (Internet of Things), Guru Nanak Institutions Technical Campus, Hyderabad, Telangana, India

ARTICLEINFO

Article History:

Accepted: 05 April 2024
Published: 21April 2024

Publication Issue :
Volume 11, Issue 2
March-April-2024
Page Number :
355-362

ABSTRACT

The rise of edge smart IoT devices has led to the development of edge storage systems (ESS) for efficient access to massive edge data. ESS can reduce the load on cloud centers and improve user experience. However, ESS still faces challenges in improving fault tolerance and efficiency. Thus, there is a need for a secure and efficient fault-tolerant storage scheme. Existing schemes have drawbacks like high edge storage overhead, difficulty in protecting edge data privacy, and low data writing performance. To address these issues, we propose a Hierarchical Cloud-Edge Collaborative Fault-Tolerant Storage (HCEFT) model. This model aims to enhance system robustness, reduce edge storage overhead, and ensure edge data privacy. We also introduce an optimization method for data writing in HCEFT, called ECWSS (Erasure Code data Writing method based on Steiner tree and SDN). This method improves the trade-off between data writing time and traffic consumption. Our scheme improves data robustness, availability, and security. Additionally, the writing optimization method reduces data write time by 13%-67% and network traffic consumption by 20%-62%, enhancing network load balance performance.

Keywords : Edge storage systems (ESS), Quality of Experience (QoE), Fault Tolerance Ability, Secure Fault-Tolerant Storage Scheme, Edge Data Privacy, Data Writing Performance, Hierarchical Cloud-Edge Collaborative Fault-Tolerant Storage (HCEFT) Model, System Robustness, Data Writing Optimization Method, Data Robustness, Availability, Security

I. INTRODUCTION

We take it for granted that the data owner is reliable and that the data users have permission from them. The owner and users' communication channels are protected by established security protocols like TLS and SSL. Other secure semantic searching schemes rely on "semi-honest servers," but our scheme is resistant to a more demanding security model that goes beyond it when it comes to the cloud server. According to our model, the dishonest cloud server tries to provide false or incorrect search results and obtain private data, but it doesn't intentionally remove or alter the documents that are outsourced. Consequently, under such a security model, our secure semantic scheme ought to ensure the verifiability and confidentiality.

II. EXISTING SYSTEM

Edge storage systems (ESS) have emerged as a new paradigm to support the efficient access of massive edge data, driven by the explosive growth of edge smart IoT devices. ESS can significantly reduce cloud center load and improve user Quality of Experience (QoE)[1]. Though ESS has made great strides, it still has to figure out how to increase the efficiency and fault tolerance of the system. It is therefore vital and essential to design a safe and effective fault-tolerant storage system. Sadly, there are still a number of issues with the fault-tolerant ESS schemes that are currently in use. These issues include low data writing performance, high edge storage overhead, and difficulty protecting edge data privacy. Erasure coding specifically permits the creation of redundant parity chunks by encoding the data[2].

Existing System Disadvantages:

1. Collection of quality characteristic data, high-speed safe transmission.
2. Next-generation information technology.

III. PROPOSED SYSTEM

Inspired by this, we present a fault-tolerant, secure cloud-edge collaborative storage scheme along with an optimization method for data writing. To be more specific, we first suggest an edge data privacy security, low edge storage overhead, and system robustness using the Hierarchical Cloud-Edge Collaborative Fault
Tolerant Storage (HCEFT) model.

In order to achieve a better trade-off between the data writing time and traffic consumption, we further optimized the HCEFT writing process by developing a data writing optimization method called ECWSS (Erasure Code data Writing method based on Steiner tree and SDN)[3]. Ultimately, thorough comparison and extensive experimentation demonstrate the superior data availability, security, and robustness that our scheme can achieve. Additionally, the writing optimization method can improve network load balance performance while reducing data write times by 13%–67% and network traffic by 20%–62%[4].

Proposed System Advantages:

1. Sharing platform's real-time and orderly operation.
2. Data storage security sharing, and supplier assessment models on this foundation
3. Providing practical and intelligent sharing solutions for airlines

IV. SYSTEM ARCHITECTURE

In this research, we present a comprehensive framework designed to address the intricate challenges of secure data sharing within cloud-based collaborative environments[5]. Central to our framework is the seamless interaction between data owners, data users, and cloud servers, ensuring not only the confidentiality and integrity of shared information but

also the efficiency and ease of collaboration. At the core of our system lies a robust authentication and access control mechanism, enabling users to securely register, log in, and manage their interactions within the platform. Through a combination of encryption techniques and stringent access policies, sensitive documents uploaded by data owners are safeguarded against unauthorized access, ensuring that only authorized users can retrieve and interact with the data[6].

Moreover, our framework incorporates advanced request handling mechanisms, allowing data users to search for and request access to specific documents uploaded by data owners. Cloud servers play a pivotal role in this process, facilitating the secure exchange of encryption keys and overseeing the access approval process.

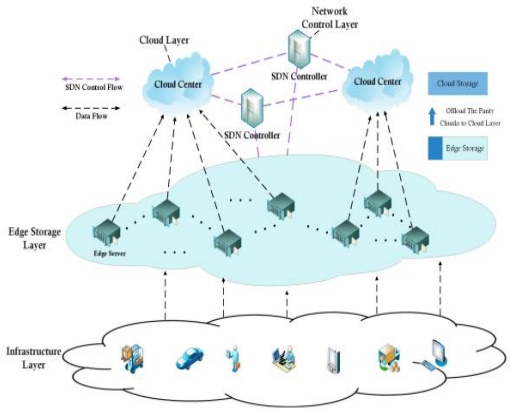

Figure 1 : System architecture

With a comprehensive view of all stored data and user information, cloud servers ensure that access requests are handled efficiently and in accordance with predefined security policies. Additionally, our framework includes provisions for handling unauthorized access attempts, with mechanisms in place to detect and block users who attempt to access data using incorrect or unauthorized keys. By proactively addressing security threats and vulnerabilities, our framework provides a robust foundation for secure data sharing in cloud-based collaborative environments, enhancing user confidence and promoting seamless collaboration.

Through extensive experimental evaluation, we demonstrate the effectiveness and efficiency of our framework in real-world scenarios. By analyzing performance metrics such as data retrieval time, access latency, and system throughput, we showcase the scalability and reliability of our solution in handling large volumes of data and concurrent user requests[7]. Furthermore, we conduct a comprehensive security analysis, identifying potential threats and vulnerabilities and proposing mitigation strategies to safeguard against them. Overall, our research contributes to the advancement of secure data sharing practices in cloud environments, providing valuable insights and solutions for organizations and individuals seeking to collaborate and exchange information securely in the digital age[8].

V. LITERATURE SURVEY

Numerous development bottlenecks have emerged as a result of the growth of the Industrial Internet of Things and the ongoing expansion of application scenarios. The problem with data security has made it difficult for it to be widely used. Both academia and business have given it a great deal of attention. The features of blockchain technology include non-tampering, openness, transparency, and decentralization. It is naturally advantageous in addressing the Industrial Internet of Things' security issue. In light of this, this paper first examines the security threats related to data storage in the Industrial Internet of Things and suggests using blockchain technology to guarantee data security in this context. Merkle hash trees are used by the data layer in conventional blockchains to store data; nevertheless. Because the Merkle hash tree cannot produce non-member proof, malicious nodes within the network cannot attack it[5]. This paper provides member proof and non-member proof by substituting

a password accumulator for the Merkle hash tree in order to solve this issue. Additionally, the current accumulators are unable to accommodate the blockchain's expansion requirements due to their trapdoors, inability to update in batches, and other issues. This paper defines the term "accumulator" and presents an improved version of the RSA accumulator. In conclusion, this paper builds a trapdoor-free batch update accumulator scheme using RSA and demonstrates the security and correctness of the scheme.

It is becoming more and more popular to offload complex virtual reality (VR) computational tasks to a network edge computation entity as a way to deliver high-quality, immersive, interactive VR services to low- end client devices wirelessly and with minimal energy consumption, anywhere in the world at any time. In this work, we use a prototype testbed for edge-assisted VR processing and streaming to conduct extensive experiments with the goal of providing an understanding of various aspects of VR computation offloading Initially, we look into how VR offloading helps a client device's computational load and power consumption when compared to standalone operation. Subsequently, we quantify VR traffic patterns, encompassing frame size, data, and packet rates, across multiple configurations, including encoding and resolution settings.

In addition, we measure a number of performance metrics with different configuration settings that are related to experience quality, such as frame rate, packet loss rate, and image quality. Next, we explore per-component latency with different settings and present studies on latency measurement. In addition, we present the results of our exhaustive experiments investigating the effects of motion patterns and latency on the black borders created by image reprojection as well as the overfilling method employed to remove these borders.

Multiple access As an extension of cloud computing, edge computing (MEC) offers network edge storage resources to allow users to retrieve data with minimal latency[9]. When functioning independently, individual edge servers are unable to store a significant amount of data due to their restricted physical sizes and storage resources. In order to serve users cooperatively, they frequently need to transfer data to other edge servers. Edge servers, which are run by various edge infrastructure providers, typically operate in a hostile environment. The two biggest obstacles to enabling collaborative edge storage are incentive and trust. This paper presents CSEdge, a novel decentralized system designed to address these issues and allow blockchain- based collaborative edge storage. Edge servers can post requests for data offloading on CSEdge for other servers to compete for.

The selection of winners is dependent on their reputations. When they successfully complete data offloading tasks, they will be rewarded and the offloaded data will be stored. Their performance will be documented on blockchain for future reputation assessment through a distributed consensus[10]. Based on Hyperledger Sawtooth, a CSEdge prototype is tested experimentally in a simulated MEC environment against two state-of-the-art systems and a baseline system. The outcomes show that CSEdge can effectively and efficiently enable edge servers to collaborate on edge storage.

We have seen a growing trend in research and development for edge computing and edge storage, which expands the capabilities of a single mobile device on the edge through on-demand collaboration among multiple geographically dispersed mobile devices. This trend is driven by the advancements in the Internet of Things and the growing capacity of smart mobile devices at the edge of the Internet[13]. This article

discusses a number of technical issues that are particular to collaborative storage at the edge because of the peculiarities of mobile devices. The collaborative storage problem is first formulated as an optimization problem. Next, we create A2CS, an Acceleration Algorithm for Collaborative Storage, which is modeled after the Alternating Direction Method of Multipliers architecture (ADMM)[11].

In particular, we update variables and calculate the ideal rate of convergence using the Nesterov's Acceleration strategy and the step size rules. To steer the entire collaborative storage lifecycle, we create a novel collaborative storage policy. In order to analyze and validate acceleration performance, we finally carry out a number of experiments. We demonstrate that, when compared to two existing approaches—the ADMM baseline and the ADMM-OR (ADMM with Over- Relaxation)—A2CS provides a better convergence performance with varying step size rules, achieving the acceleration percentage by at least 25.33 percent and at most 64.01 percent. Furthermore, by comparing the utility performance of the current Distance Preferred Distribution Strategy (DPDS) and Average Distribution Strategy (ADS), we demonstrate the benefit of A2CS over both ADS and DPDS[12].

VI. EXISTING ALGORITHM

kNN Algorithm

To encrypt relevance scores and implement a multi-keyword ranked search scheme under the vector space model, homomorphic encryption was introduced. techniques for encryption. Multi-keyword ranked searching schemes that are resilient to multiple attacks from OPE-based schemes are not supported. Safe and Secure Semantic Exploration[14].

VII. PROPOSED ALGORITHM

LP problems for linear programming to acquire the encrypted MWTC

We formulate the word transportation (WT) problem by treating the matching between queries an minimum word transportation cost (MWTC), which serves as a similarity metric between queries and documents, is computed using WT problems[15].

We present the forward indexes as document semantic information. The keywords distributions for a document are defined as each keyword and its weight in the forward index of the document. As a result, we must choose keywords for every document and determine how important each keyword is for a given document.Without loss of generality, we use TF-IDF (term frequency inverse document frequency) as a criterion to select keywords in our scheme.

VIII. RESULTS

User

Input : Enter Login name and Password

Output : If valid user name and password then directly open the home page otherwise show error message and redirect to the registration page.

Edge Node

Input : Data User Login name and Password

Output: If valid user name and password then directly open the Data user home page otherwise show error message and redirect to the data user login page.

Edge Server

Input : Enter the owner name and password

Output : If valid owner name and password then directly open the data owner home page otherwise show error message and redirect to the data owner login page.

Cloud

Input : Enter the Cloud Server name and password

Output: If valid Cloud Server name and password then directly open the Cloud Server home page

otherwise show error message and redirect to the cloud Server login page.

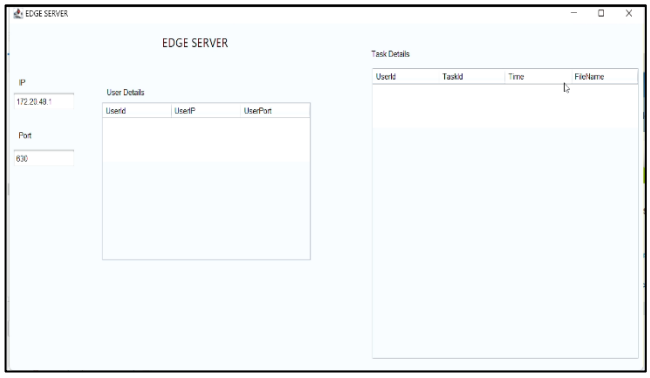

Figure 2 : Edge Server

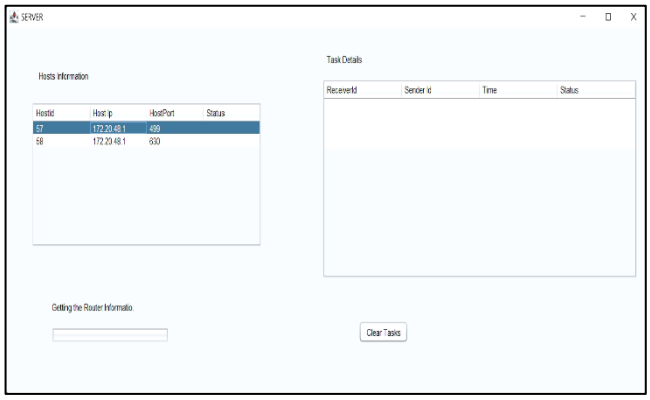

Figure 3: Server

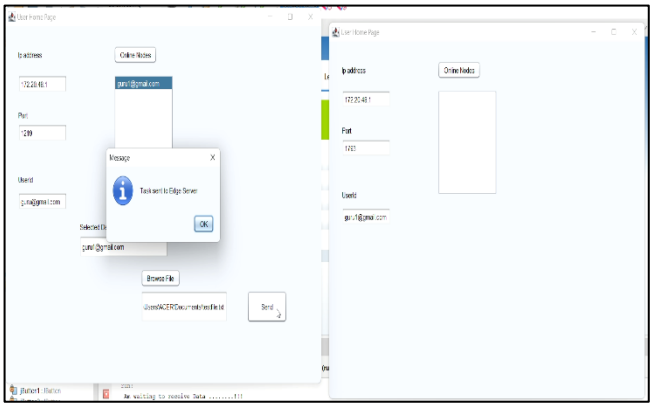

Figure 4: Edge Server Running

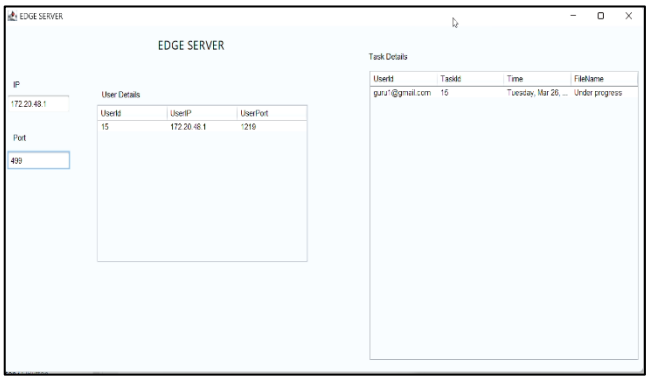

Figure 5: Task details in edge server

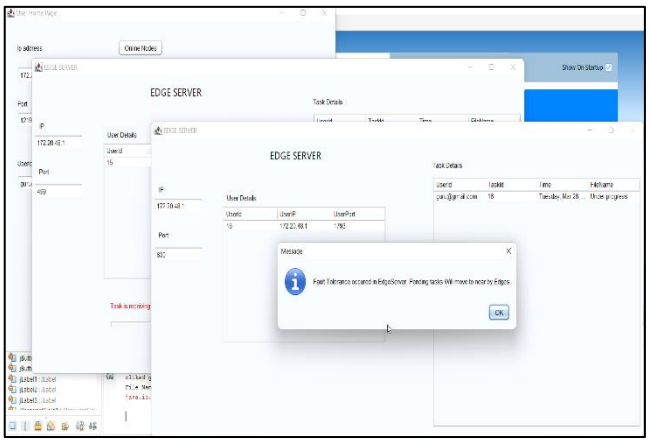

Figure 6 : Fault tolerance occured in Edge Server

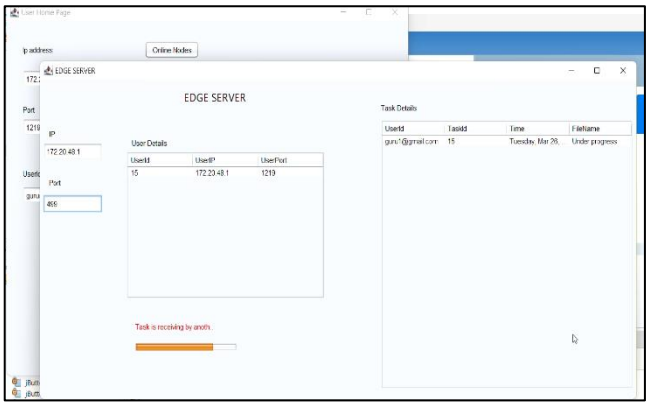

Figure 7:Task transferred to nearest edge server

IX. CONCLUSION

The secure fault-tolerant and data writing issues in ESS were covered in this paper. The goal of this work is to increase the data writing efficiency for ESS while offering a secure, fault-tolerant storage scheme. In particular, we designed our CEPPC code and proposed a novel and secure cloud-edge collaborative fault-tolerant storage scheme, named HCEFT. It can offer high availability and fault tolerance while

preserving edge node data privacy security. Subsequently, a future- proposed data writing optimization method for HCEFT was presented, which can minimize writing traffic and reduce writing time. A thorough comparative analysis along with extensive experimental results demonstrate the HCEFT scheme's effectiveness and the data writing optimization method's improvement.

Our future work will concentrate on data update and repair issues in dynamic network environments for ESS. Furthermore, the fundamental concepts offered in this work can be leveraged by researchers looking into general erasure coding data writing problems for ESS,

and modified to fit the particular needs of their contexts. Furthermore, as the edge storage network grows in size, it is imperative to research cooperative management of multiple SDN controllers in ESS, including control domain partitioning, cooperative communication, and other related techniques. All of these studies have the potential to improve the edge storage systems' scalability, effectiveness, and dependability.

X. REFERENCES

[1]. T. Wu, G. Jourjon, K. Thilakarathna, and P. L. Yeoh, "MapChainD: A distributed blockchain for IIoT data storage and communications," IEEE Trans. Ind. Informat., early access, Jan. 6, 2023, doi: 10. 1109/TII.2023.3234631.

[2]. S. H. A. Kazmi, F. Qamar, R. Hassan, and K. Nisar, "Routing-based interference mitigation in SDN enabled beyond 5G communication networks: A comprehensive survey,"IEEE Access, vol. 11, pp. 4023–4041, 2023.

[3]. B. W. Nyamtiga, A. A. Hermawan, Y. F. Luckyarno, T. Kim, D. Jung, J. S. Kwak, and J. Yun, "Edge-computing-assisted virtual reality computation offloading: An empirical study," IEEE Access, vol. 10, pp. 95892–95907, 2022.

[4]. M. Carrie and R. David, The Growth in Connected IoT Devices is Expected to generate 79.4ZB of Data in 2025, According to a New IDC Forecast. Accessed: Apr. 8, 2023.

[5]. R. van der Meulen. What Edge Computing Means for Infrastructure and Operations Leaders? Accessed: Apr. 8, 2023

[6]. L. A. Haibeh, M. C. E. Yagoub, and A. Jarray, "A survey on mobile edge computing infrastructure: Design, resource management, and optimization approaches" IEEE Access, vol. 10, pp. 27591–27610, 2022.

[7]. H. Zhang, Y. Yang, X. Huang, C. Fang, and P. Zhang, "Ultra-low latency multi-task offloading in mobile edge computing," IEEE Access, vol. 9, pp. 32569–32581, 2021.

[8]. S. Li and T. Lan, "HotDedup: Managing hot data storage at network edge through optimal distributed deduplication," in Proc. IEEE INFOCOM Conf. Comput. Commun., Jul. 2020, pp. 247–256.

[9]. L. Yuan, Q. He, F. Chen, J. Zhang, L. Qi, X. Xu, Y.Xiang, and Y. Yang, "CSEdge: Enabling collaborative edge storage for multi-access edge computing based on blockchain," IEEE Trans. Parallel Distrib. Syst., vol. 33, no. 8, pp. 1873–1887, Aug. 2022.

[10]. S. Kisseleff, S. Chatzinotas, and B. Ottersten,"Reconfigurable intelligent surfaces in challenging environments: Underwater, underground, industrial and disaster," IEEE Access, vol. 9, pp. 150214– 150233,2021.

[11]. X. Gao, W. Bao, X. Zhu, G. Wu, and L. Liu, "An edge storage acceleration service for collaborative mobile devices," IEEE Trans. Services Comput., vol. 15, no. 4, pp. 1993–2006, Jul. 2022.

[12]. A. Aral and T. Ovatman, "A decentralized replica placement algorithm for edge computing," IEEE Trans. Netw. Service Manage. vol. 15, no. 2, pp. 516–529, Jun. 2018.

[13]. M. Linaje, J. Berrocal, and A. Galan-Benitez,"Mist and edge storage: Fair storage distribution in sensor networks," IEEE Access, vol. 7, pp. 123860– 123876, 2019.

[14]. L. Liang, H. He, J. Zhao, C. Liu, Q. Luo, and X. Chu, "An erasurecoded storage system for edge computing," IEEE Access, vol. 8, pp. 96271–96283, 2020.

[15]. Y. Wu, D. Liu, X. Chen, J. Ren, R. Liu, Y. Tan, and Z. Zhang, "MobileRE: A replicas prioritized hybrid fault tolerance strategy for mobile distributed system," J. Syst. Archit., vol. 118, Sep. 2021, Art. no. 102217.