Journal of Science and Technology
ISSN: 2456-5660 Volume 8, Issue 04 (April -2023)
www.jst.org.in *DOI:https://doi.org/10.46243/jst.2023.v8.i04.pp80 - 86*

DROPSTORE - A SECURE BACKUP SYSTEM USING MULTI CLOUD AND FOG COMPUTING

Dr. S. SARADA, [1],Bandaru Pranava Sai Vamsi [2],Markonda Jay Aditya Ramyendra Santhosh [3],Mutyala Pavani Sai [4],Yalla Priya Susmitha [5],Bangaru Sai Lohitha [6]
ASSOCIATE PROFESSOR
DEPT OF COMPUTER SCIENCE AND ENGINEERING
PRAGATI ENGINEERING COLLEGE(A),SURAMPALEM(EAST GODAVARI)A.P,INDIA

To Cite this Article

DR. S. SARADA, ,BANDARU PRANAVA SAI VAMSI ,MARKONDA JAY ADITYA RAMYENDRA SANTHOSH ,MUTYALA PAVANI SAI [4],YALLA PRIYA SUSMITHA ,BANGARU SAI LOHITHA**, "DROPSTORE - A SECURE BACKUP SYSTEM USING MULTI CLOUD AND FOG COMPUTING "** *JOURNAL OF SCIENCE AND TECHNOLOGY, VOL. 08, ISSUE 04,-APRIL 2023, PP80-86*

Article Info
Received: 25-02-2023 *Revised: 18-03-2023* *Accepted: 26-03-2023* *Published: 20-04-2023*

Abstract:

Data backup is essential for disaster recovery. Current cloud-based solutions offer a secure infrastructure. However, there is no guarantee of data privacy while hosting the data on a single cloud. Another solution is using multi-Cloud technologies. Although using multiple clouds to save smaller pieces of the data can enhance data privacy, it comes at the cost of the need for the edge device to manage different accounts and manage communication with different clouds.

These drawbacks made this technology rare to use technology. In this paper, we propose DropStore to provide an easy-to-use, highly secure, and reliable backup system using state-of-the-art multi-Cloud and encryption techniques. DropStore adds an abstraction layer for the end-user to hide all system complexities using a locally hosted device, ''the Droplet'', that is fully managed by the user. Hence, the user does not rely on any untrusted third party. This was achieved using Fog Computing technology. The uniqueness of DropStore comes from the convergence of Multi-Cloud and Fog Computing principles. The system implementation is open-source and available online. Performance results show that the proposed system improves data protection in terms of reliability, security, and privacy preservation while maintaining a simple and easy interface with edge devices.

I. Introduction

The widespread use of digital storage in networking and computing has led to an increase in the importance of data backup. However, digital storage also poses several threats, including security attacks, hardware failure, and operation errors. To prevent these threats, data backup is crucial, and cloud backup systems offer protection and disaster recovery.

With the increased use of cloud computing technology, it has become challenging to ensure data protection. Although many cloud service providers offer their services at low costs or even for free, they often lack uniform policies for data protection and privacy preservation. This poses a significant risk to organizations and individuals who rely on cloud services to store their data.

To address this issue, researchers have developed the multi-Cloud concept, which uses a heterogeneous architecture with various cloud computing and storage facilities. This architecture offers increased data protection, flexibility, and cost optimization. When using multi-Cloud architecture, users can either manage resources and services themselves or enlist the help of a third-party service provider. By doing so, they can ensure that their data is protected from various threats while taking advantage of the benefits of cloud computing technology.

The Number of rounds Nr is based on key length of Nk and words. Nb is steady for all forms. Cryptography is the portion of science which bargains with data security which has gotten to be exceptionally basic in present day computing framework to secure information transmission and capacity. The significance of security has gotten to be a major need as broad utilize of individual communication gadgets. The trade of advanced information in cryptography comes about completely different calculation classified into two cryptographic components: symmetric key in which same key issue for encryption and decoding which are quick and less demanding to actualize than topsy-turvy key calculation.

II. LITERATURE SURVEY

1. "Scientific cloud computing: Early definition and experience,"

Cloud computing emerges as a new computing paradigm which aims to provide reliable, customized and QoS guaranteed dynamic computing environments for end-users. This paper
reviews recent advances of Cloud computing, identifies the concepts and characters of scientific Clouds, and finally presents an example of scientific Cloud for data centers

2.''A secured cost-effective multi-cloud storage in cloud computing,''

The end of this decade is marked by a paradigm shift of industrial information technology
towards a pay-per-use service business model known as cloud computing. Cloud data storage redefines the security issues targeted at customers & outsourced data (data that is not stored/retrieved from the
customers' own servers). In this work we observed that, from a customer's point of view, relying upon a solo SP for his outsourced data is not very promising. In addition, providing better privacy as well as ensuring data availability, can be achieved by dividing the user data block into data pieces and distributing them among the available SPs in such a way that no less than a threshold number of SPs can take part in successful retrieval of the whole data block. In this paper, we propose a secured cost-effective multi-cloud storage (SCMCS) model in cloud computing which holds an economical distribution of data among the available SPs in the market, to provide customers with data availability as
well as secure storage. Our results show that, our proposed model provides better decision for customers according to their available budgets.

3.''Fog computing: A comprehensive architectural survey,''

Fog computing is a new technology for IoT applications, tackling computing and networking problems. It is a complement to cloud computing with multi-tier, distributed, cooperative deployment of computing, storage, and networking at the edge and network layers. This offers a "computing everywhere" approach, using virtualized computing functions at edge devices or network elements on demand. The paper provides an inclusive taxonomy for fog computing's architectural, algorithmic, and technological aspects, including cloud, edge and fog computing. Deployment requires system and application design, software implementation, security, resource management, and networking. The paper explores reference and application- specific architectures, and their distinctions in the context of fog computing. Base architectures for computing, software, security, resource management, and networking are evaluated using proposed maturity model.

4.''Fog computing: Survey of trends, architectures, requirements, and research directions,'

Emerging technologies like the Internet of Things (IoT) require latency-aware computation for real-time application processing. In IoT environments, connected things generate a huge amount of data, which are generally referred to as big data. Data generated from IoT devices are generally processed in a cloud infrastructure because of the on-demand services and scalability features of the cloud computing
paradigm. However, processing IoT application requests on the cloud exclusively is not an efficient solution for some IoT applications, especially time-sensitive ones. To address this issue, Fog computing, which resides in between cloud and IoT devices, was proposed. In general, in the Fog computing environment,

IoT devices are connected to Fog devices. These Fog devices are close to users and are responsible for intermediate computation and storage. Fog computing research is still in its infancy, and taxonomy-based investigation into the requirements of Fog infrastructure, platform, and applications mapped to current research is still required. This paper starts with an overview of Fog computing in which the definition of Fog computing, research trends, and the technical differences between Fog and cloud are reviewed. Then, we investigate numerous proposed Fog computing architecture and describe the components of these architectures in detail. From this, the role of each component will be defined, which will help in the deployment of Fog computing. Next, a taxonomy of Fog computing is proposed by considering the requirements of the Fog computing paradigm. We also discuss existing research works and gaps in resource allocation and scheduling, fault tolerance, simulation tools, and Fog-based microservices. Finally, by addressing the limitations of current research works, we present some open issues, which will determine the future research direction.

5.''A survey of fog computing: Concepts, applications, and issues,''

Despite the increasing usage of cloud computing, there are still issues unsolved due to inherent problems of cloud computing such as unreliable latency, lack of mobility support and location- awareness. Fog computing can address those problems by providing elastic resources and services to end users at the edge of network, while cloud computing is more about providing resources distributed in the core network. This survey discusses the definition of fog computing and similar concepts, introduces representative application scenarios, and identifies various aspects of issues we may encounter when designing and implementing fog computing systems. It also highlights some opportunities and challenges, as direction of potential future work, in related techniques that need to be considered in the context of fog computing.

III.SYSTEM ANALYSIS

3.1. EXISTING SYSTEM

Multi-Cloud Storage has been gaining a lot of attention in recent years due to its potential benefits, such as high availability, strong security, and prevention of service provider lockouts. One example of such a system was designed by Zaman et al. (2019), which is a distributed multi-Cloud storage system that uses hybrid encryption to ensure data security. The system works by encrypting user data offline, dividing it into chunks, and then distributing it to multiple cloud servers. The chunk sequence and addresses are managed by a third-party cloud service provider, and a separate key management server takes care of the encrypted keys.

However, despite its potential advantages, the system has some limitations. First, it does not implement any redundancy technique to ensure data reliability. This means that if any one of the cloud servers fails, the data stored in that server will be lost. Second, there is no explicit versioning in the system, which increases storage needs over time. Third, the third-party cloud service provider that deploys the system is a single point of failure and a vulnerable bottleneck. If this provider fails or is compromised, the entire system will be at risk.

To overcome these limitations, future research on Multi-Cloud Storage systems should focus on implementing redundancy techniques to ensure data reliability, adopting explicit versioning to reduce storage needs, and reducing reliance on a single point of failure by distributing the responsibilities of the third-party cloud service provider among multiple providers. Additionally, it is important to consider the potential security risks associated with the use of third-party providers, and to design appropriate security measures to mitigate these risks. By addressing these issues, Multi-Cloud Storage systems can become even more reliable, secure, and beneficial for users.

3.2. PROPOSED SYSTEM

Singh et al. presented a secure data deduplication technique that uses secret sharing schemes. In this technique, data is sliced based on the Permutation Ordered Binary (POB) numbering system and stored on multiple cloud

servers. The key information is divided into multiple random shares based on the Chinese Remainder Theorem (CRT) and saved to multiple servers. However, data can be restored only if all the shares are available, while the key can be restored from k servers out of n servers, where k is less than n. Therefore, the system will not be able to survive in the event of cloud service provider lockouts.

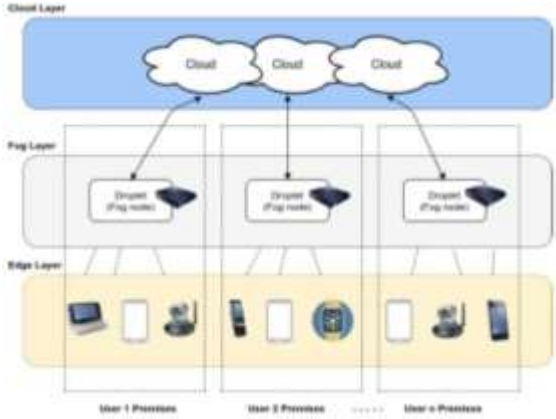
Trivia is a chunking-based backup system that minimizes storage needs by using the sec-cs data structure for deduplication of flat contents. This system offers multi-Cloud storage for the
generated backups, making storage efficient. However, this comes at the expense of data reliability and immunity against lockouts.

Trusty Drive is a document storage system that utilizes multiple cloud providers to store documents while preserving user anonymity and document anonymity. The focus of the system is to save and secure document files only. However, the system does not provide an interactive or easy way to share and view saved documents. Multi-Cloud storage systems offer high availability, strong security, and prevent service provider lockouts. However, these systems have limitations. To overcome these limitations, future research on multi-Cloud storage systems should focus on implementing redundancy techniques to ensure data reliability and improving interactivity and sharing features. Additionally, security measures must be in place to mitigate potential security risks associated with the use of third-party providers.

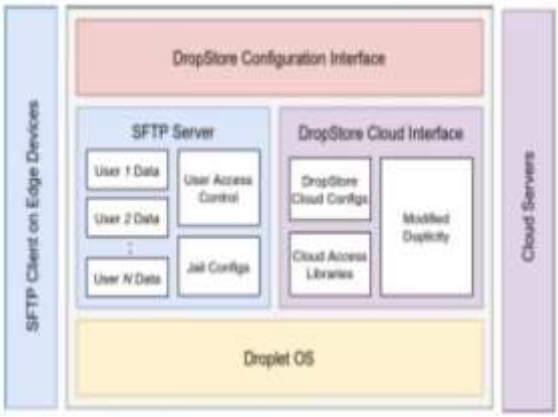
IV.SYSTEM DESIGN

4.1 SYSTEM ARCHITECTURE

The below diagrams depict the entire system architecture of the droplet in network and Dropstore software architecture.



4.1. System Architecture of the droplet in network



4.2. Dropstore software architecture

V. SYSTEM IMPLEMENTATION

5.1. MODULES

There are 4 modules

- Edge Nodes
- Droplet
- Public Cloud
- DropStore- System

5.1.1 Edge Nodes

- Register
- Login
- Register Device
- Upload Data
- View Data
- My Profile
- Logout

5.1.2 Droplet: -

- Login
- User management
- Fog layer
- Logout

5.1.3 Public Cloud: -

- Login
- Edge devices
- Droplet Fog Layer

5.1.4 DropStore-System: -

- Login
- Edge Nodes
- Droplet Fog Layer
- Logout

VI. RESULTS

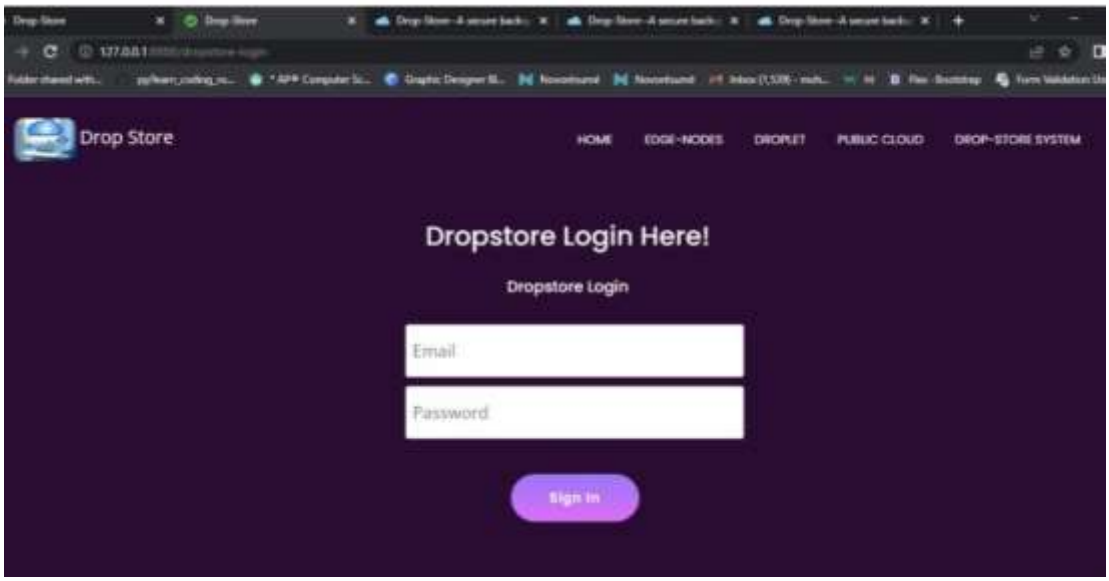


Fig. 6.1 DropStore Login Page

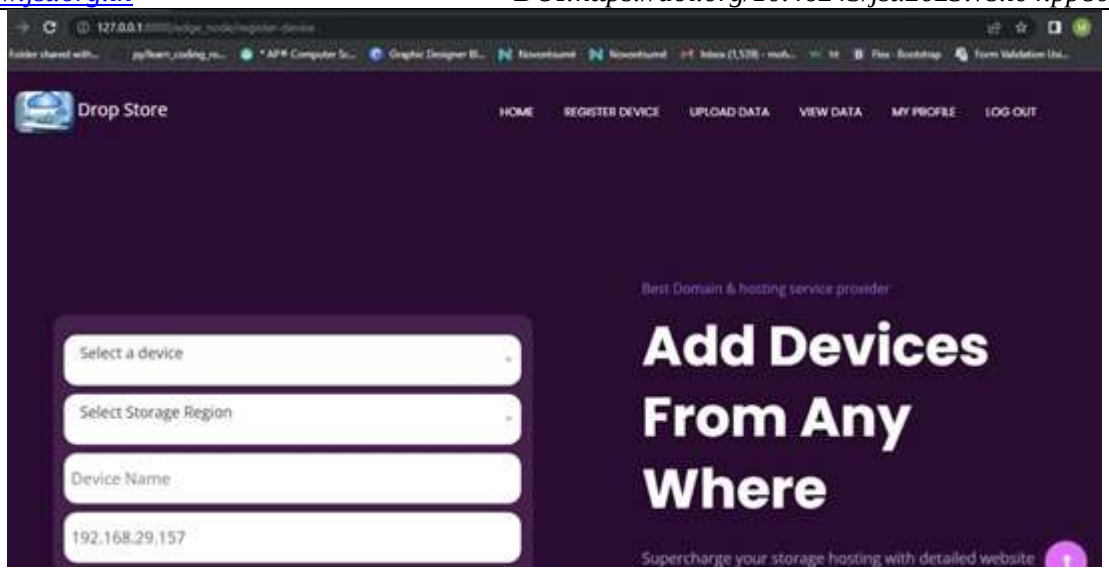


Fig. 6.2 Adding Devises to Dropstore

VII.CONCLUSION AND FUTURE WORK

In conclusion, DropStore presents a novel solution to address the challenges of data security and reliability by utilizing the Multi-Cloud and Fog Computing paradigms. The system is designed to provide a seamless backup experience for individual users while abstracting them from the system's complexities. DropStore ensures data security and user privacy through encryption and data partitioning on Multi-Cloud Storage. The system's efficiency and reliability were validated through real-world experiments using two different implementations. The results demonstrate that DropStore is capable of storing and retrieving data reliably with minimal complexity at the edge side.

As future work, we plan to explore better scheduling strategies for data uploading to the cloud. New scheduling strategies will consider QoS parameters and the remaining storage at each CSP to optimize the system's performance. Additionally, we will develop linear block codes for
data replication to enhance the system's error detection and correction capabilities. These advancements will further improve the system's reliability and efficiency while reducing complexity, making it an even more attractive backup solution for individual users.

REFERENCES :

[1] L. Wang, J. Tao, M. Kunze, A. C. Castellanos, D. Kramer, and W. Karl, ‘‘Scientific cloud computing: Early definition and experience,’’ in Proc. 10th IEEE Int. Conf. High Perform. Comput. Commun., Sep. 2008, pp. 825–830.

[2] Y. Singh, F. Kandah, and W. Zhang, ‘‘A secured cost-effective multi-cloud storage in cloud computing,’’ in Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS), Apr. 2011, pp. 619–624.

[3] P. Habibi, M. Farhoudi, S. Kazemian, S. Khorsandi, and A. Leon-Garcia, ‘‘Fog computing: A comprehensive architectural survey,’’ IEEE Access, vol. 8, pp. 69105–69133, 2020.

[4] R. K. Naha, S. Garg, D. Georgakopoulos, P. P. Jayaraman, L. Gao, Y. Xiang, and R. Ranjan, ‘‘Fog computing: Survey of trends, architectures, requirements, and research directions,’’ IEEE Access, vol. 6, pp. 47980–48009, 2018.

[5] S. Yi, C. Li, and Q. Li, ‘‘A survey of fog computing: Concepts, applications and issues,’’ in Proc. Workshop Mobile Big Data, New York, NY, USA, Jun. 2015, pp. 37–42, doi: 10.1145/2757384.2757397.

[6] S. Sarkar and S. Misra, ‘‘Theoretical modelling of fog computing: A green computing paradigm to support IoT applications,’’ IET Netw., vol. 5, no. 2, pp. 23–29, Mar. 2016.

[7] B. Tang, Z. Chen, G. Hefferman, T. Wei, H. He, and Q. Yang, ‘‘A hierarchical distributed fog computing architecture for big data analysis in smart cities,’’ in Proc. ASE BigData SocialInform., New York, NY, USA, 2015, pp. 1–6. [Online].

Available: https://dl.acm.org/doi/10.1145/2818869.2818898

[8] K. Kai, W. Cong, and L. Tao, ‘‘Fog computing for vehicular ad-hoc networks: Paradigms, scenarios, and issues,’’ J. China Universities Posts Telecommun., vol. 23, no. 2, pp. 56–96, Apr. 2016. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1005888516600213

[9]S. U. Zaman, R. Karim, M. S. Arefin, and Y. Morimoto, ‘‘Distributed multi cloud storage system to improve data security with hybrid encryption,’’ in Intelligent Computing and Optimization, P. Vasant, I. Zelinka, and G.-W. Weber, Eds. Cham, Switzerland: Springer, 2020, pp. 61–74.

[10] P. Singh, N. Agarwal, and B. Raman, ‘‘Secure data deduplication using secret sharing schemes over cloud,’’ Future Gener. Comput. Syst., vol. 88, pp. 156–167, Nov. 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X17327474

[11] A. Sreekumar and S. B. Sundar, ‘‘An efficient secret sharing scheme for n out of n scheme using POB-number system,’’ Hack, vol. 33, pp. 1–88, Mar. 2009.

[12] V. J. Katz, A. Imhausen, E. Robson, J. W. Dauben, K. Plofker, and J. L. Berggren, The Mathematics of Egypt, Mesopotamia, China, India, and Islam: A Sourcebook. London, U.K.: Princeton Univ. Press, 2007. [Online]. Available: https://books.google.com.eg/books?id=3ullzl036UEC.