IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 9, May 2023

A Secure Backup System using Multi-Cloud and Fog Computing

Dhanushree A N, Thotli Roopa, Srilekha L. J, Gudipati Bhargavi, Shwetha A
Department of CSE
S J C Institute of Technology, Chickballapur, India

Abstract: *Backing up data is essential for disaster recovery. The infrastructure for cloud-based solutions is already secure. But when all of your data is kept in one cloud, you can't be sure it's private. An additional choice is multi-cloud technology. Data privacy can be increased by using many clouds to store smaller amounts of data, but doing so necessitates that the edge device handles numerous accounts and connections to other clouds. This technology isn't often employed because of these drawbacks. We introduce Drop Store as a simple, extremely safe, and dependable backup system using cutting-edge multi-Cloud and encryption techniques. To hide any system complexities from the end-user, Drop Store uses a locally hosted device to build an abstraction layer. The user has complete control over "The Droplet." The user won't need to do anything as a result. rely on any unreliable outsiders. This was accomplished via fog computing. DropStore uniqueness comes from the fusion of Multi-Cloud and Fog Computing ideas. The software is available online and is free source. According to performance results, the suggested approach enhances data protection in terms of dependability, security, and privacy preservation while maintaining a clear and simple interface with edge devices.*

Keywords: backing up data, disaster recovery cloud-based solutions, data privacy

I. INTRODUCTION

Many people can now easily share their data with others via online external storage. People can easily share highly sensitive personal health records with pals by uploading them to online data servers like Microsoft Health Vault and Google Health, or they can upload private photographs or messages to online social networks like Facebook and Myspace. Primary care physicians or to cut costs.

People's worries about access control and data security increase as they take use of the latest services and technology. Their data may be at danger from unauthorized access by outside users or improper data use by the storage server. Individuals want to make their own decisions. People desire their private or sensitive information. being accessible only to those who possess the credentials they specify. Data sharing and cost savings are two key advantages of cloud storage. As a result, more companies and individuals are outsourcing their data to the cloud in order to benefit from this service.

However, there are serious problems with this new data storage paradigm when it comes to data confidentiality. The cloud service separates the data from the cloud service client (individuals or enterprises), denying them direct control over the data, therefore the data owner cannot trust the cloud server to implement safe data access control. Secure access control has consequently become a challenging issue in public cloud storage.

Data sharing and cost savings are two key advantages of cloud storage. As a result, more companies and individuals are outsourcing their data to the cloud in order to benefit from this service. However, there are serious problems with this new data storage paradigm when it comes to data confidentiality.

The cloud service separates the data from the cloud service client, denying them direct control over the data, therefore the data owner cannot trust the cloud server to implement safe data access control. Secure access control is now a challenging issue in public cloud storage as a result. The cryptographic method of CP-ABE for restricting access to data in cloud storage. All of these CP-ABE-based strategies enable data owners to put into practice adaptable and fine-grained data access control. On the other hand, CP-ABE ignores any other important factors like time and simply

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 9, May 2023

assesses users' access privileges based on their fundamental characteristics. The time factor frequently plays a key role when dealing with time-sensitive data, such as when publishing the most recent electronic version.

II. RELATED WORK

Lu, Rong Xing, [1] It has been proposed that the mobile healthcare (healthcare) system will be an important computing application for raising the standard of medical care and preventing fatalities. An opportunistic computing paradigm can be employed in an m-Healthcare emergency to solve the difficult reliability problem in the PHI procedure. We present SPOC, a novel secure and privacy-preserving opportunistic computing paradigm, to address this issue.Ning Cao [2] Cloud computing is the long-awaited realization of computing as a utility, in which cloud customers can store their data remotely in the cloud and access high-quality apps and services on demand from a shared pool of programmable computer resources.

Individuals and businesses are both motivated to outsource their local complicated data management system to the cloud because of its excellent flexibility and cost savings. Sensitive data must be protected in the cloud and beyond to prevent unauthorized access.

Jing Chen and co. [3] Applications for wireless mesh networks range from military operations to environmental monitoring to industrial management. A potential solution that could enhance the performance of wireless mesh networks is network coding. Network coding is appropriate since the fixed backbone of wireless mesh networks typically has infinite energy. By incorporating the information process, which significantly reduces the decoding failure rate, it effectively addresses the flow coding collision problem. Reifying Du and co. [4] A user-revocable ABE system that combines broadcast encryption methods with ABE schemes solves this issue. The data owner should accept full responsibility for keeping the entire membership list for each attribute group in this scheme in order to enable direct user revocation. Since the data owners will no longer have direct control over their data after saving it on an external storage server, this technique is not applicable to the data sharing system. Yu et al. recently addressed user revocation in the ABE-based data sharing system. In this technique, user revocation is carried out by the data server utilizing proxy encryption. However, the KGC should produce all secret keys for the data server, including the proxy, in order to revoke users.

III. IMPLEMENTATION

Researchers have been concerned about the concept of big data. Using big data to gather useful information has become a popular trend in recent years.Big data research's main purpose is to process massive amounts of data in order to extract useful information. Furthermore, in the long run, a proper approach to large data processing is crucial. However, dealing with large amounts of data requires more than a single computer or server. As a result, in the building of big data, the distributed structure is extremely crucial. Cloud computing originated from distributed computing, which may provide a variety of big data-related services such as distributed processing, virtualization, and distributed databases researchers have expressed reservations about the concept of big data. In recent years, using big data to obtain meaningful information has become a popular trend. The primary goal of big data research is to process huge amounts of data in order to extract usable information. Furthermore, a good approach to massive data processing is critical in the long run. However, dealing with enormous amounts of data necessitates the use of more than one computer or server. As a result, the distributed structure is critical in the construction of big data. Cloud computing evolved from distributed computing, which may offer a wide range of big data-related services such as distributed processing, virtualization, and distributed databases. It is impossible to manage massive amounts of data on a single computer or server. When all data must be uploaded to the cloud, a slew of security risks can arise. They use a deniably encrypted plan-ahead symmetric data encryption key to encrypt real data via a symmetric key encryption process [4]. The majority of decryption error concerns appear in defensible encryption schemes. These issues are the result of poorly constructed decryption techniques.

The subset decision procedure is used for decryption. The receiver chooses the decrypted message based on the outcome of the subset decision. If the sender selects an element from the universal set while the element is found in the specialized subset, an error occurs.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 9, May 2023

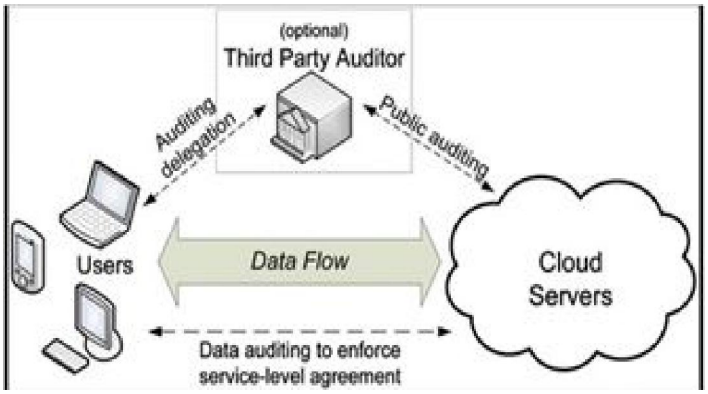

Fig: Architecture of the cloud storage environment

Through a CSP, a user uploads data to a collection of cloud servers that are distributed, cooperating, and operating in parallel. The user depends on the CS for cloud data maintenance and storage. After that, for a variety of application-related reasons, the user can dynamically interact with the CS via CSP to access, retrieve, and change the stored data. The user must make sure that his or her data is saved and preserved properly because they no longer have local access to their data, hence the user must be given the required tools [8].He can continue to verify the accuracy of his saved data even in the absence of local copies in order to uphold cloud storage service level agreements. Data stored on cloud servers should be audited to verify its accuracy and integrity. To assure the security of the outsourced data's storage while maintaining his data's privacy from the TPA, the user can assign data auditing tasks to an optional trusted TPA of their choice.

IV. BLOCK DIAGRAM

Fig 2. Block diagram of Computer Network Architecture

The architecture is represented by a diagram that illustrates the various components and their interconnections. A network architecture may include:

Network topology: The physical or logical layout of network devices, such as routers, switches, and servers. The topology can be hierarchical, mesh, star, ring,orbus. Network protocols: The rules and procedures that govern how data is transmitted and received over the network.TCP/IP, HTTP, DNS, and FTP are examples of protocols. Network hardware: The physical components of the network, such as routers, switches, modems, and cables. Network software: The software components that enable network communication and data transmission, such as network operating systems, firewalls, and antivirus software. Network security: The measures taken to protect the network from unauthorized access, such as firewalls, intrusion detection systems, and encryption. Network management: The processes and tools used to monitor and manage the network, such as network monitoring software, performance analysis tools, and configuration management tools.

V. PROBLEM STATEMENT

Additionally, traditional backup systems may not provide the level of security required to protect sensitive data from cyber threats such as hacking, malware, and ransomware attacks. Moreover, traditional backup systems may not be scalable enough to support enough to support large amounts of data, which is a critical requirement for many

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 9, May 2023

organizations. Therefore, there is a need for a backup system that leverages the power of multi-cloud storage and fog computing to ensure high availability, fault tolerance, data durability. Cloud Fog Backup is to provide a secure and efficient backup system that uses advanced technologies such as multi-cloud storage and fog computing to protect data from loss or corruption. The system should be scalable, customizable, and provide granular control over data, enabling users to define backup polices and configure retention rules. Additionally, the system should be secure, offering data encryption both in transit and at rest, to protect against cyber threats and ensure business continuity.Therefore, there is a need for a backup system that uses cutting-edge multi-cloud and encryption techniques, provides complete control to end-users, and simplifies the complexity of managing multiple cloud accounts while ensuring data dependability, security, and privacy preservation.

VI. METHODOLOGY

The Requirement Analysis: The first step is to gather requirements from stakeholders to understand their backup needs. The analysis should consider factors such as data size, backup frequency, recovery time, and retention period. System Design: Based on the requirements gathered in the previous step, a system design should be created that outlines the architecture and components of the backup system. The design should consider factors such as the cloud providers to use, the data replication strategy, the backup policy, and the backup client. Cloud Provider Selection: Cloud providers should be selected based on factors such as cost, performance, reliability, and data privacy. Multiple cloud providers should be chosen to provide redundancy and eliminate the risk of a single point of failure. Implementation: After the system design and cloud providers have been selected, the next step is to implement the system. This includes configuring cloud accounts, deploying the backup client, and setting up the backup policy.

Testing: The system should be tested to ensure that it meets the requirements gathered in the first step. This includes testing the backup and restore functions, verifying data encryption, and testing the failover mechanism. Deployment: After testing, the system should be deployed in a production environment, and user training should be provided.

Maintenance: The backup system should be regularly maintained to ensure that it continues to meet the requirements of the stakeholders. Maintenance tasks include monitoring system.

VII. SYSTEM ARCHITECTURE

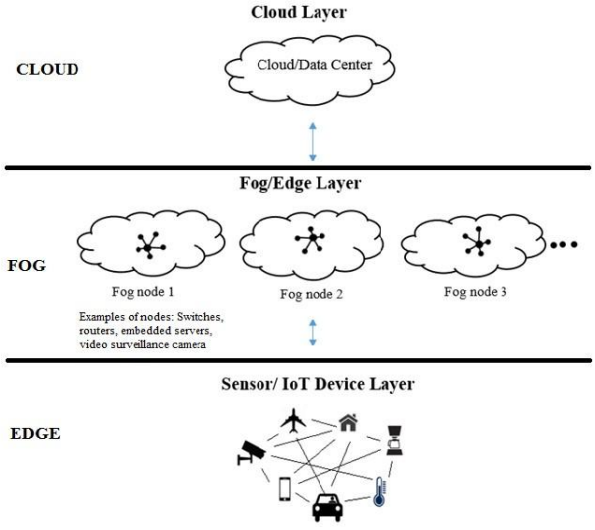

Fig.3. A typical architecture of fog computing

As seen in Figure 3, fog computing makes use of both cloud and edge resources in addition to its own architecture. Fundamentally, the technology manages IoT data locally by relying on clients or edge devices close to users to handle a sizeable amount of storage, communication, control, configuration, and management. The method takes use of the close proximity of edge devices to sensors while utilizing the flexibility of cloud resources to scale on demand. Applications for data processing or analytics running on distributed clouds and edge devices are included in fog computing. Additionally, it makes it easier to manage and program storage, networking, and compute services between

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 9, May 2023

datacenters and endpoints. In order to meet the needs of widely dispersed applications that demand low latency, it also supports user mobility, resource and interface heterogeneity, and distributed data analytics.

VIII. OBJECTIVE

High availability and fault tolerance are provided by Cloud Fog Backup, which makes use of many clouds to store data in order to assure data redundancy and reduce the chance of data loss. In order to provide a distributed storage solution with high availability and fault tolerance, it also leverages fog computing to process data using edge devices.Data durability and scalability should be ensured by the system, which should be able to handle enormous amounts of data. Granular control over data is possible thanks to Cloud Fog Backup, which lets users set up retention schedules and backup policies. Users can choose which data to save and create personalized backup schedules, allowing for flexibility and personalization.

IX. FUTURE SCOPE

- Integration with Artificial Intelligence (AI): Integration with AI can improve the performance and efficiency of the backup system. AI algorithms can be used to optimize backup policies, predict storage requirements, and automate backup and recovery tasks.
- Blockchain-based Data Protection: Blockchain technology can be used to provide an immutable and secure backup system. The integration of blockchain technology can help prevent data tampering, fraud, and unauthorized access.Hybrid Cloud-Fog Architecture: Hybrid cloud-fog architecture can provide additional benefits by leveraging the strengths of both cloud and fog computing. Hybrid architecture can offer more flexibility in data placement, faster data transfer, and better fault tolerance.
- Multi-Tier Storage: Multi-tier storage can provide an efficient and cost-effective backup solution. The integration of multi-tier storage can help store frequently accessed data on fog nodes and less frequently accessed data on cloud providers, optimizing the storage cost and performance.
- Disaster Recovery: The Cloud Fog Backup architecture can be extended to provide disaster recovery services. Disaster recovery services can help businesses and organizations recover from unexpected events and ensure business continuity.

In conclusion, Cloud Fog Backup has significant potential for future advancements and improvements. The integration of AI, blockchain, hybrid cloud-fog architecture, multi-tier storage, and disaster recovery services can provide additional benefits and improve the overall efficiency and effectiveness of the backup system.

X. RESULT

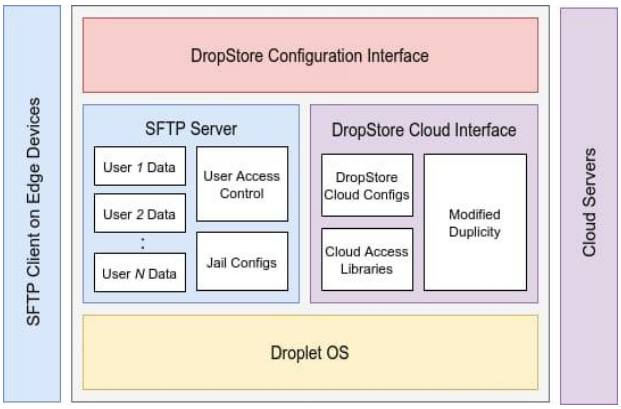

Fig.4.Cloud fog Software Architecture

Cloud fog architecture is a network architecture that combines cloud computing and fog computing technologies to provide a secure and efficient backup system. It consists of multiple cloud providers and fog nodes that work together to provide backup services to end users. The components are cloud providers, fog nodes, backup clients, data replication mechanism, backup policy,encryption.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 9, May 2023

XI. CONCLUSION

Create a brand-new symbol-based tier-traverse searching technique that builds a multi-way tree structure utilizing symbols that have been translated from the resulting expressive keyword sets. We demonstrate through a thorough security analysis that our suggested technique is safe and privacy-preserving while correctly achieving expressive keyword search's objective. Results from extensive experiments show that the suggested solution works well. The problem of open audits was resolved while protecting privacy. A brand-new safe cloud storage technique is offered to shield businesses' data from third-party auditors, cloud providers, users with expired accounts, and other potential threats.

The proposed system makes use of the automatic blocker protocol (ABP) and the time-based one-time password (TOTP) as two different authentication methods.The suggested system includes the owner of the data has total control over all privileges, guaranteeing that only people with the proper authorization can access the data that has been outsourced to cloud storage servers. Two-factor authentication is used to verify user authentication in order to increase security. The first step is completed using a login and password, and the second is started by utilizing TOTP. The experimental findings demonstrate the effectiveness and efficiency of the provided approach for auditing shared data integrity. In conclusion, there is a lot of room for growth and development for Cloud Fog Backup in the future. AI, blockchain, hybrid cloud-fog architecture, multi-tier storage, and disaster recovery services can all be integrated to increase the backup system's overall efficiency and efficacy.Cloud disaster recovery solutions typically involve replicating data and applications to a secondary location or cloud environment to ensure they can be restored in the event of a disruption.

REFERENCES

[1] S. Bell, C. L. Zitnick, K. Bala, and R.Girshick. Insideoutside net: Detecting objects in context with skippooling and recurrent neural networks. arXiv preprint arXiv:1512.04143, 2015. 6

[2] J. Deng, W. Dong, R. Socher, L.-J. Li, K. Li, and L. FeiFei.Imagenet: A large-scale hierarchical image database. In Computer Vision and Pattern Recognition, 2009. CVPR 2009. IEEE Conference on, pages 248–255. IEEE, 2009. 1

[3] M. Everingham, L. Van Gool, C. K. Williams, J. Winn, and A. Zisserman. The pascal visual object classes (voc)challenge. International journal of computer vision,88(2):303– 338, 2010. 1

[4] P. F. Felzenszwalb, R. B. Girshick, and D. McAllester. Discriminatively trained deformable partmodels,release4.http://people.cs.uchicago.edu/pff/latent-release4/. 8

[5]R.B.Girshick.FastRCNN.CoRR,abs/1504.08083,2015. 5, 6

[6] K. He, X. Zhang, S. Ren, and J. Sun. Deep residual learning for image recognition. ArXivpreprintarXiv:1512.03385, 2015. 2, 5, 6

[7] S. Ioffe and C. Szegedy. Batch normalization: Accelerating deep network training by reducing internal covariate shift. arXiv preprint arXiv:1502.03167, 2015. 2,5

[8] A. Krizhevsky, I. Sutskever, and G. E. Hinton. Imagenet classification with deep convolutional neural networks. In Advances in neural information processing systems, pages 1097–1105, 2012. 2

[9] M. Lin, Q. Chen, and S. Yan. Network in network. arXiv preprint arXiv:1312.4400, 2013. 4

[10] T.-Y. Lin, M. Maire, S. Belongie, J. Hays, P. Perona,D.Ramanan, P. Doll´ar, and C. L. Zitnick. Microsoft coco: Common objects in context. In European Conference on Computer Vision, pages 740–755. Springer, 2014. 1, 6

[11] W. Liu, D. Anguelov, D. Erhan, C. Szegedy, and S. E.Reed. SSD: single shot multibox detector. CoRR, abs/1512.02325, 2015. 5, 6

[12] G. A. Miller, R. Beckwith, C. Fellbaum, D. Gross, and K.J.Miller.Introductiontowordnet:Anonlinelexical database.International journal of lexicography, 3(4):235–244, 1990.6

[13] J. Redmon. Darknet: Open source neural networks in c. http://pjreddie.com/darknet/, 2013–2016. 5

[14] J. Redmon, S. Divvala, R. Girshick, and A. Farhadi. You only look once: Unified, real-time object detection. arXiv preprint arXiv:1506.02640, 2015. 5, 6

[15] S. Ren, K. He, R. Girshick, and J. Sun. Faster r-cnn: Towards real-time object detection with region proposal networks. arXiv preprint arXiv:1506.01497, 2015. 2, 3, 5, 6