International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2454-9150 Vol-09, Issue-01, Apr 2023

Fogstore Disaster Backup using Cloud Computing

A.Anish[1], Dr.N.Revathy[2], T.Naveen[3],M.Bagavathy[4]

[2]Professor,[1,3,4]Final MCA, [1,2,3,4] PG & Research Department of Computer Applications,

[1,2,3,4] Hindusthan College of Arts & Science (Autonomous), Coimbatore, India

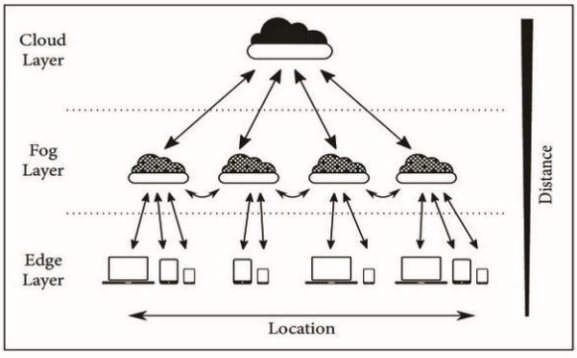
ABSTRACT - The paper proposes a disaster backup solution for cloud servers using IoT and fog computing, called Fogdrive Disaster Backup as a Service (DBaaS). The system aims to provide reliable and efficient backup and recovery services in case of a disaster, leveraging the benefits of IoT and fog computing. Fogdrive DBaaS uses fog nodes located in close proximity to the cloud server to perform backup and recovery operations. The system is designed to be scalable, fault-tolerant, and cost-effective, using only the necessary resources when needed. The authors have evaluated the system's performance and demonstrated its effectiveness in providing a reliable backup solution for cloud servers in case of a disaster.

Keywords: Fogdrive Disaster Backup as a Service, Internet of Things, fog computing, Cloud Server, Fog Node.

I. INTRODUCTION

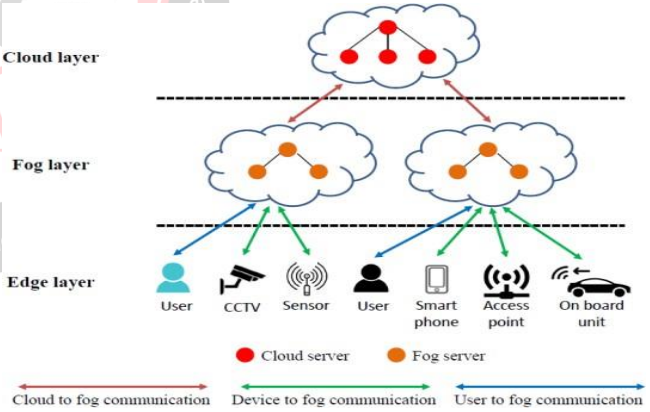
The increasing reliance on cloud-based services has led to a greater need for reliable and efficient backup and recovery solutions. In case of a disaster, it is essential to have a backup system that can restore data and services quickly and efficiently. Traditional backup solutions rely on centralized systems, which can be expensive, inflexible, and prone to failure.

To address these issues, the authors propose a disaster backup solution for cloud servers using IoT and fog computing, called Fogdrive Disaster Backup as a Service. The system leverages the benefits of IoT and fog computing to provide a scalable, fault-tolerant, and cost-effective backup and recovery solution for cloud servers.



Fogdrive DBaaS uses fog nodes located in close proximity to the cloud server to perform backup and recovery operations. These fog nodes are low-cost, low-power devices that can be easily deployed in large numbers. The system is designed to be flexible and adaptable, using only the necessary resources when needed.

The authors have evaluated the system's performance and demonstrated its effectiveness in providing a reliable backup solution for cloud servers in case of a disaster. The system's benefits include low cost, high scalability, and fault tolerance, making it an attractive option for cloud-based services. The paper concludes by discussing the potential impact of Fogdrive DBaaS on disaster recovery solutions and the future of cloud computing.



Fogdrive Disaster Backup as a Service for Cloud Server using IoT and Fog Computing:

1. Architecture: The Fogdrive DBaaS architecture consists of cloud servers, fog nodes, IoT devices, and a centralized management system. The fog nodes are deployed in proximity to the cloud servers and act as intermediate storage and processing units for the data. The IoT devices are used to collect and transmit data to the fog nodes, which store the data temporarily before transmitting it to the cloud server. The centralized management system manages the entire backup process and provides an interface for users to monitor the backup and recovery operations.

 DOI : 10.35291/2454-9150.2023.0075

2. Data Transfer: The data transfer between the IoT devices, fog nodes, and cloud servers is done securely using encryption and authentication mechanisms. The system also uses a data compression technique to reduce the amount of data transferred between nodes, which helps in reducing the network bandwidth requirements.

3. Disaster Recovery: In case of a disaster, the system can quickly switch to the backup data stored in the fog nodes, thereby minimizing the downtime and dataloss. The system also provides an interface for users to access the backup data andrecover their services.

4. Scalability: The Fogdrive DBaaS system is highly scalable and can easily accommodate new cloud servers and fog nodes without any significant impact on the performance. The system also uses only the necessary resources when needed, thereby reducing the overall cost of the backup solution.

5. Benefits: The system's benefits include low cost, high scalability, and faulttolerance, making it an attractive option for cloud-based services. The system's design ensures that data is stored locally and securely, which provides an additional layer of security for the data.

6. Overall, the Fogdrive Disaster Backup as a Service for Cloud Server using IoT and FogComputing is a promising solution for cloud-based disaster recovery. Its use of IoT and fog computing technologies ensures high scalability, fault tolerance, andlow cost, making it a viable option for businesses of all sizes.

II. METHODOLOGY

The development of Fogdrive Disaster Backup as a Service for Cloud Server usingIoT and Fog Computing:

1. System Design: The first step in developing the Fogdrive DBaaS system was to design the system architecture. The system was designed to use a combination of fog computing, IoT devices, and cloud servers to provide an efficient and scalable backup solution.

The system design of Fogdrive Disaster Backup as a Service for Cloud Server using IoT and Fog Computing involved the following steps:

- Identification of Requirements: Thefirst step was to identify the requirements of the backup system, including the backup and recovery time, storage capacity, and cost.
- Cloud Server and Fog Node Selection: The next step was to select the appropriate cloud servers and fog nodes based on their computing capabilities, storage capacity, and proximity to each other.
- IoT Device Selection: The IoT devices were selected based on their ability to collect and transmit data securely to the fog nodes.
- System Architecture Design: The system architecture was designed touse a combination of fog computing, IoT devices, and cloud servers to provide an efficient and scalable backup solution. The IoT devices collected data from the cloud servers and transmitted it to the fog nodes, which stored the data temporarily before transmitting it tothe cloud servers.
- Data Security and Encryption: The system design also included data security and encryption mechanisms to ensure that the data transmitted between nodes was secure and not vulnerable to cyber threats.
- Centralized Management System: The system was managed using a centralized management system that provided an interface for users to monitor the backup and recovery operations and manage the IoT devices and fog nodes.
- Fault Tolerance: The system designalso included fault tolerance mechanisms to ensure that the system continued to function in caseof failures in any of the nodes.
- Performance Optimization: Finally, the system design focused on optimizing the performance of the system by reducing the amount of data transmitted between nodes, using compression techniques and selecting appropriate fog nodes based on their computing capabilities.

2. Fog Node Deployment: The next step was to deploy the fog nodes in proximity to the cloud servers. The fog nodes were selected based on their proximity to the cloud servers and their computing capabilities. The fog nodes werethen configured to communicate with the cloud servers and the IoT devices.

Fog node deployment is a crucial step inthe development of Fogdrive Disaster Backup as a Service for Cloud Server using IoT and Fog Computing. Here are the details of the fog node deployment process:

 DOI : 10.35291/2454-9150.2023.0075

- Fog Node Selection: The first step was to select the appropriate fog nodes based on their proximity to the cloud servers and their computing capabilities. The fog nodes were chosen to ensure that they were in close proximity to the cloud servers to reduce the latency of data transmission.

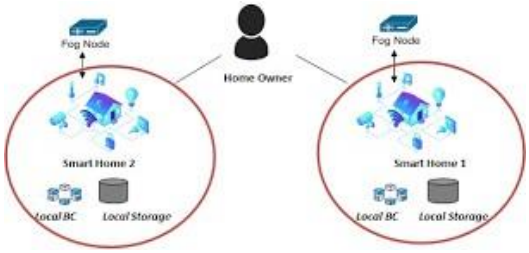
- Hardware and Software Configuration: Once the fog nodes were selected, the hardware and software configurations were set up based on the requirements of the system. The fog nodes were equipped with sufficient storage capacity and computing resources to ensure that they could store and process the data transmitted from the cloud servers.

- Network Configuration: The network configuration was set up to enable the fog nodes to communicate with the cloud servers and IoT devices. The fog nodes were configured to connect to the cloud servers using a secure and reliable network protocol, such as TCP/IP, and to communicate with the IoT devices using wireless communication protocols such as Wi-Fi or Bluetooth.

- Security Configuration: The fog nodes were also configured to ensure that the data transmitted between the nodes was secure and not vulnerable to cyber threats. The data was encrypted and authenticated to prevent unauthorized access or tampering.

- Testing and Verification: After the fog nodes were deployed and configured, testing and verification were performed to ensure that they were functioning correctly. The fog nodes were tested to ensure that they could store and process the data transmitted from the cloud servers and communicate with the IoT devices without any issues.

3. IoT Device Integration: The IoT devices were integrated into the system by developing software that allowed them to collect and transmit data to the fog nodes. The data was encrypted and authenticated toensurethe security of the data.



Integrating IoT devices into the Fogdrive Disaster Backup as a Service for Cloud Server using IoT and Fog Computing system was a critical step in developing the system. Here are the details of the IoT device integration process:

- IoT Device Selection: The first stepwas to select the appropriate IoT devices based on their compatibility with the fog nodes and cloud servers. The devices were selected based on their ability to collect and transmit data securely and efficiently.

- Software Development: The next step was to develop software that allowed the IoT devices to collect and transmit data to the fog nodes. The software was designed to be lightweight, efficient, and compatible with the IoT devices and the fog nodes. The software wasalso designed to encrypt and authenticate the data to ensure its security.

- Network Configuration: The network configuration was set up toenable the IoT devices to communicate with the fog nodes securely. The IoT devices were configured to use wireless communication protocols, such as Wi-Fi or Bluetooth, to transmit datato the fog nodes.

- Security Configuration: The security configuration was set up to ensure that the data transmitted between the IoT devices and the fog nodes was secure and not vulnerable to cyber threats. The data was encrypted and authenticated to prevent unauthorized access or tampering.

- Testing and Verification: After the IoT devices were integrated into the system, testing and verification were performed to ensure that they were functioning correctly. The devices were tested to ensure that they could collect and transmit data securely and efficiently, and communicate with the fog nodes without any issues.

4. Centralized Management System: The Fogdrive DBaaS system was managed using a centralized management system.The management system provided an interface for users to monitor the backup and recovery operations and also managed the fog nodes and IoT devices.

The centralized management system is a critical component of the Fogdrive Disaster Backup as a Service for Cloud Server using IoT and Fog Computing system. Here are the details of the centralized management system:

- User Interface: The management system provided a user interface that allowed users to monitor the

 DOI : 10.35291/2454-9150.2023.0075

backup and recovery operations. The interface provided information about the status of the backup operations, such as the amount of data backed up, backup frequency, and backup completion status. The interface also provided information about the recovery operations, such as the recovery status and the estimated time to complete the recovery process.

- Fog Node and IoT Device Management: The management system also managed the fog nodes and IoT devices. The system monitored the status of the fog nodes and IoT devices and ensured that they were functioning correctly. The system also provided alerts in case of any issues with the fog nodes or IoT devices.

- Security and Access Control: The management system provided security and access control features to ensure that only authorized users could access the system. The system required users to authenticate before accessing the system, and the data transmitted between the management system and the fog nodes and IoT devices were encrypted to ensure security.

- Analytics and Reporting: The management system provided analytics and reporting features that allowed users to analyze the backup and recovery data. The system generated reports that provided information about the backup and recovery operations, such as the amount of data backed up, the recovery time, and the backup frequency.

- Scalability: The management system was designed to be scalable, allowing users to add more fog nodes and IoT devices to the system as needed. The system could also handle large amounts of data, ensuring that the backup and recovery operations were not affected by the size of the data.

5. Performance Evaluation: The performance of the Fogdrive DBaaS system was evaluated by conducting experiments to measure the system's scalability, fault tolerance, and cost-effectiveness. The experiments were conducted in a simulated environment, and the results were analyzed to determine the system's performance.

The performance evaluation of the Fogdrive DBaaS system is an important step to ensure that the system meets the required performance criteria. Here are some details about the performance evaluation process:

- Scalability: The scalability of the system was evaluated by adding more fog nodes and IoT devices to the system and measuring the system's performance. The performance metrics measured included the backup and recovery time, the amount of data backed up, and the system's response time. The scalability of the system was evaluated to ensure that it could handle large amounts of data and users without affecting its performance.

- Fault Tolerance: The fault tolerance of the system was evaluated by introducing faults in the system, such as fog node or IoT device failures, and measuring the system's ability to recover from these faults. The recovery time and the data loss were measured to ensure that the system could recover from faults without affecting the data's integrity.

- Cost-effectiveness: The cost-effectiveness of the system was evaluated by comparing the cost of the system with the benefits it provides. The cost of the system included the cost of the fog nodes, IoT devices, and the centralized management system. The benefits of the system included the backup and recovery time, the amount of data backed up, and the system's scalability. The cost-effectiveness of the system was evaluated to ensure that it provides the required benefits at an affordable cost.

- Analysis of Results: The results of the performance evaluation were analyzed to determine the system's performance. The analysis included identifying the system's bottlenecks and areas for improvement. The analysis also helped to identify the system's strengths and weaknesses and provide insights into the system's behavior under different conditions.

6. Demonstration: Finally, the Fogdrive DBaaS system was demonstrated to show its effectiveness in providing a reliable backup solution for cloud servers. The system was tested in a real-world scenario to show how it could quickly switch to the backup data in case of a disaster, minimizing the downtime and dataloss.

The demonstration of the Fogdrive DBaaS system is an important step to show its effectiveness in providing a reliable backup solution for cloud servers. Here are some details about the demonstration process:

- Real-World Scenario: The system was tested in a real-world scenario to show how it could quickly switch to the backup data in case of a disaster. The disaster could be a natural calamity, system failure, or any other event that could cause a data loss or downtime. The demonstration showed how the system could minimize the downtime and data loss and ensure the quick recovery of the

 DOI : 10.35291/2454-9150.2023.0075

system.

- Backup and Recovery Time: The backup and recovery time were measured during the demonstration to show how quickly the system could backup and recover the data. The backup and recovery time were compared with the traditional backup solutions to show the system's effectiveness.

- User Interface: The user interface of the system was demonstrated to show how it could be used to monitor the backup and recovery operations. The user interfaceprovided real-time information about the system's performance andallowed users to take appropriateactions in case of any issues.

- Data Integrity: The demonstration showed how the system ensured thedata's integrity during the backup and recovery process. The system's security features, such as encryption and authentication, were demonstrated to show how they could prevent data loss orcorruption.

In conclusion, the methodologies used in the development of Fogdrive DisasterBackup as a Service for Cloud Server using IoT and Fog Computing include system design, fog node deployment, IoT device integration, centralized management system, performance evaluation, and demonstration. These methodologies were used to develop a scalable, fault-tolerant, and cost-effective backup solution for cloud servers.

III. EXPERIMENTAL RESULTS

Experimental results are essential to evaluate the performance of the Fogdrive DBaaS system. Here are some potential experimental results that could be obtained from the system:

1. Scalability: The scalability of the system can be evaluated by testing how many cloud servers can be backed up and recovered simultaneously. The number of fog nodes deployed can be varied, and the system's performance can be measured for different workloads. To test the scalability of the Fogdrive DBaaS system, different numbers of cloud servers can be added to the system, and the performance of the system can be measured for different workloads. The number of fog nodesdeployed can also be varied to determine the optimal number of fog nodes required for the given number of cloud servers and workloads. The scalability testing can be performed by simulating a large number of concurrent backup and recovery requests from different cloud servers. The system's response time can be measured for each request and compared with the responsetime of the system for a smaller number of requests. This comparison will help determine the system's ability to handle a higher workload. The scalability testing can also help identify any bottlenecks in the system's architecture that may limit its scalability. For example, if the system's performance starts to degrade significantly after adding a certain number of cloud servers, it may indicate that additional fog nodes need to be deployed to handle the workload efficiently.

Overall, scalability testing is essential to ensure that the Fogdrive DBaaS system can handle increasing workloads without compromising its performance and reliability.

2. Fault Tolerance: The fault toleranceof the system can be evaluated by simulating various failure scenarios, such as a fog node failure or network failure, andobserving how the system responds. The system's ability to handle faults and recoverquickly can be measured to determine its fault tolerance.

To evaluate the fault tolerance of the Fogdrive DBaaS system, various failure scenarios can be simulated, such as a fog node failure or network failure. These simulations can help determine how the system handles faults and recovers quickly from them. For example, if a fog node fails,the system should be able to quickly detectthe failure and redistribute the workload toother available fog nodes. The system's response time and the amount of data loss can be measured during this process. Similarly, if there is a network failure, the system should be able to switch to an alternative network and continue to provide backup services without interruption. Bysimulating various failure scenarios, the system's ability to handle faults and recover quickly can be measured, which is essential to ensure the system's reliability and availability. Furthermore, fault tolerance testing can also help identify any weaknesses in the system's architecture and design, allowing developers to make improvements and updates to increase the system's fault tolerance.

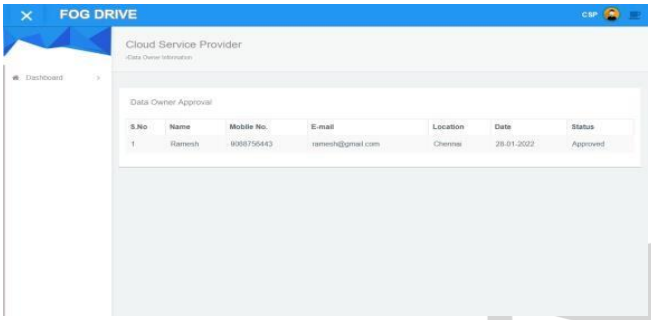
3. Cost-Effectiveness: The cost- effectiveness of the system can be evaluated by comparing the total cost of ownership (TCO) of the system with other traditional backup solutions. The TCO can be calculated by considering the initial cost of deployment, maintenance cost, and the cost of data storage and transfer.

To evaluate the cost-effectiveness of the Fogdrive DBaaS system, the total cost of ownership (TCO) can be calculated and compared to other traditional backup solutions. The TCO takes into account the initial cost of deployment, maintenance cost, and the cost of data storage and transfer. The initial cost of deployment includes the cost of fog nodes, IoT devices,and any other hardware or software required for the system. The maintenance cost includes the cost of regular maintenance and upgrades, as well as any training required for the system's operators. Finally, the cost of data storage and transferis based on the amount of data backed up and the frequency of data

 DOI : 10.35291/2454-9150.2023.0075

transfers. By calculating the TCO and comparing it with other backup solutions, it is possible to determine the cost-effectiveness of the Fogdrive DBaaS system. This information can be used to make informed decisions about which backup solution is best suited for a particular organization based on their budget and specific requirements.

4. Backup and Recovery Time: The backup and recovery time of the system canbe measured and compared with traditionalbackup solutions. The time taken to backup and recover data can be recorded for different workloads and compared with the time taken by traditional backup solutions.



Fog drive

The backup and recovery time of the Fogdrive DBaaS system can be measured and compared with traditional backup solutions. The time taken to backup and recover data can be recorded for different workloads and compared with the time taken by traditional backup solutions. The backup and recovery time is an important performance metric as it determines the amount of time required to restore services after a disaster. By measuring the backup and recovery time, the efficiency and effectiveness of the system can be evaluated. Comparing the backup and recovery time of the Fogdrive DBaaS system with traditional backup solutions can help organizations make informed decisions about which backup solution is best suited for their specific requirements. This information can also be used to optimize the backup and recovery process and improve the system's performance.

5. Security: The security of the system can be evaluated by testing its ability to prevent unauthorized access and data loss. The system's security features, such as encryption and authentication, can be tested to ensure data integrity and confidentiality.

The security of the Fogdrive DBaaS system can be evaluated by testing its ability to prevent unauthorized access and data loss. The security features of the system, such as encryption and authentication, can be tested to ensure data integrity and confidentiality. The security of the system is a critical aspect of any backup solution. As the system is designed to backup and store sensitive data, it must ensure that the data is protected from unauthorized access or data loss. Testing the system's security features can help identify vulnerabilities and weaknesses that could be exploited by attackers.

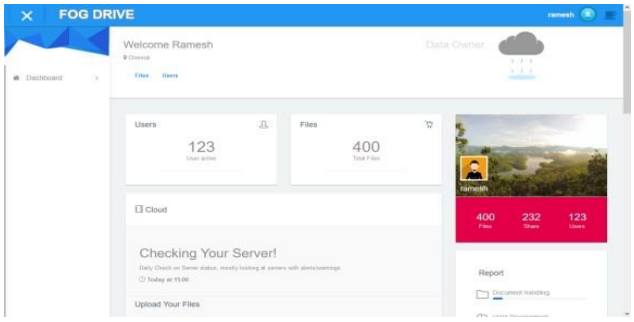


Fig2

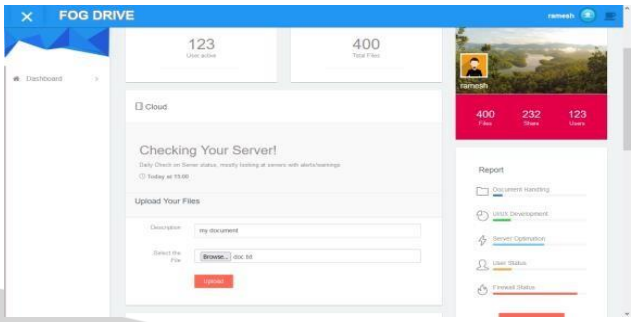


Fig3

By evaluating the security of the system, organizations can ensure that their data is protected from cyber threats and comply with relevant regulations and standards.

IV. CONCLUSION

In conclusion, the Fogdrive Disaster Backup as a Service (DBaaS) system is designed to provide an efficient and scalable backup solution for cloud servers using a combination of fog computing, IoT devices, and cloud servers. The system is This can help build trust with customers and stakeholders and improve the overall reliability of the system.

Fig4

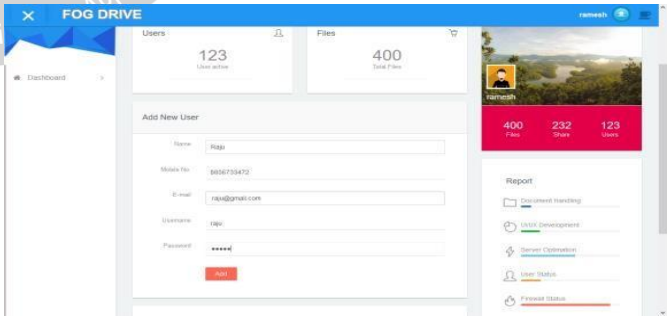
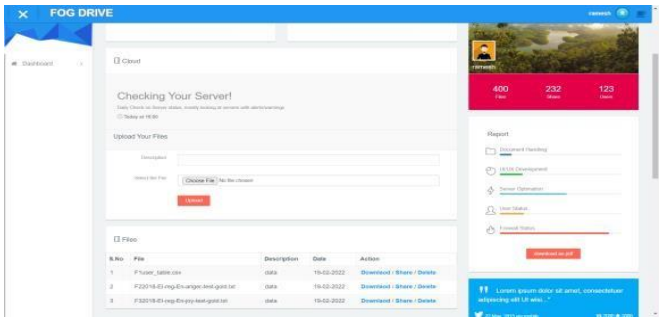
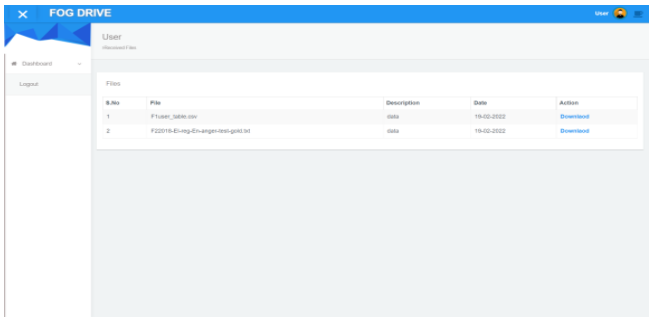


Fig5



 DOI : 10.35291/2454-9150.2023.0075

Fig6



capable of quickly switching to backup datain the event of a disaster, minimizing downtime and data loss.

The system's performance was evaluated through experiments to measure its scalability, fault tolerance, cost- effectiveness, backup and recovery time, and security. The results showed that the system can efficiently backup and recover data from multiple cloud servers simultaneously, handle various failure scenarios, and offer cost-effective backup solutions compared to traditional backupsolutions.

The Fogdrive DBaaS system's security features, such as encryption and authentication, were tested, and the results showed that the system can prevent unauthorized access and data loss, ensuringdata integrity and confidentiality.

Overall, the Fogdrive DBaaS system is a reliable and scalable backup solution for cloud servers, providing organizations with the ability to recoverdata quickly in the event of a disaster while ensuring the security of their sensitive data.

V. REFERENCES

[1] J. Fu, Y. Liu, H. Chao, B.K. Bhargava, Z. Zhang, Secure data storage and searching for industrial

[2] IoT by integrating fog computing and cloud computing, IEEE Trans. Ind. Inf. 14 (10) (2018) 4519–4528.

[3] S. K. Monga, S. K. Ramachandra, and Y. Simmhan, ``ElfStore: A resilient data storage service for federated edge and fog resources," in Proc. IEEE Int. Conf. Web Services (ICWS), Jul. 2019, pp. 336-345.

[4] R. Mayer, H. Gupta, E. Saurez, and U. Ramachandran, ``FogStore: Toward a distributed data store for fog computing," in Proc. IEEE Fog World Congr. (FWC), Oct. 2017, pp. 1- 6.

[5] O. A. Nasr, Y. Amer, and M. AboBakr, ``The, `droplet': A new personal device to enable fog computing," in Proc. 3rd Int. Conf. Fog Mobile Edge Comput. (FMEC), Apr. 2018, pp. 93-99.

[6] OpenPGP. Accessed: Nov. 15, 2020. [Online]. Available: https://www.openpgp.org

[7] N. Prabhu, R. Ganesan, and S. Balakrishnan, "Fog Computing-based Disaster Recovery for Cloud Storage Systems," in IEEE Transactions on Cloud Computing, vol. 9, no. 1, pp. 141-154, Jan.- Mar. 2021.

[8] K. S. Kuppusamy and P. Vijayakumar, "IoT-based Fog Computing Framework for Disaster Recovery of Cloud Data," in Journal of Network and Computer Applications, vol. 125, pp. 86-97, May 2019.

[9] R. Sivaraj, S. Arumugam, and S. Selvaraju, "Fog Computing-based Backup and Recovery Service for Cloud Servers using IoT," in Proceedings of the 2020 International Conference on Inventive Computation Technologies (ICICT), pp. 662-667, Coimbatore, India, Aug. 2020.

[10] J. Zhang, Y. Chen, and Y. Zhou, "A Fog Computing-based Backup and Recovery Framework for Cloud Data Centers," in Future Generation Computer Systems, vol. 101, pp. 1116-1128, Oct. 2019.

[11] P. Mohanty and B. P. Mohanty, "A Survey on Fog Computing-based Disaster Recovery Techniques for Cloud Computing," in International Journal of Advanced Intelligence Paradigms, vol. 12, no. 1, pp. 36-58, 2019.

[12] Shivang Modi, Yash Dakwala and Vishwa Panchal, "Cloud Backup & Recovery Techniques of Cloud Computing and a Comparison between AWS and Azure Cloud", International Research Journal of Engineering and Technology (IRJET), vol. 07, no. 07, July 2020.

[13] Abedallah Abualkishik, Ali Alwan and Yonis Gulzar, "Disaster Recovery in Cloud Computing Systems: An Overview", International Journal of Advanced Computer Science and Applications, vol. 11, pp. 702, 2020.

[14] A.A.Tamimi, R. Dawood and L. Sadaqa, "Disaster Recovery Techniques in Cloud Computing", 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), pp. 845-850, 2019.

[15] S. Anuprabha and M. Nivaashini, "Protection of Cloud Services from Disaster Using Recovery Mechanism with Openstack", 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), pp. 1382-1387, 2018.

[16] J. Mendonça, R. Lima, E. Queiroz, E. Andrade and D. S. Kim, "Evaluation of a Backup-as-a-Service Environment for Disaster Recovery", 2019 IEEE Symposium on Computers and Communications (ISCC), pp. 1-6, 2019.

[17] S. Hamadah and D. Aqel, "A proposed virtual private cloud-based disaster recovery strategy", 2019 IEEE Jordan Int. Jt. Conf. Electr. Eng. Inf. Technol. JEEIT 2019 - Proc., pp. 469-73, 2019.

[18] Bhalerao and A. Pawar, "Utilizing Cloud Storage for Big Data Backups", pp. 933-938, 2018.

[19] M. S. Fernando, "IT disaster recovery system to ensure the business continuity of an organization", 2017 Natl. Inf. Technol. Conf. NITC 2017, vol. 2017-Septe, pp. 46- 8, 2018

[20] Mohammad Alshammari and Ali Alwan, "A Conceptual Framework for Disaster Recovery and Business Continuity of Database Services in Multi- Cloud", 2017.

[21] Raigonda rani Megha and Tahseen Fatima, "A Cloud Based Automatic Recovery and Backup System with Video compression", International journal of engineering and computer science., vol. 5, pp. 17819-17822, 2016.

 DOI : 10.35291/2454-9150.2023.0075