International Journal of Applied and Advanced Multidisciplinary Research (IJAAMR)
Vol. 1, No. 4, 2023: 319-326

Enhancing Data Backup and Recovery in Cloud Computing with Secure Database Monitoring

Mrs. Anuja S. Phapale[1]*, Mehul Pawar[2]
Department of Information Technology, AISSMS
Institute Of Information Technology, Pune, Maharashtra, India.
Corresponding Author: Mehul Pawar mehulpawar1702@gmail.com

A R T I C L E I N F O

Keywords: Database, Performance, Backup, Recovery, Cloud Computing, Data Lose.

Received : 22, October
Revised : 20, November
Accepted: 27, December

A B S T R A C T

The company uses unregistered data to improve performance, but this comes at the cost of limited backup options, data loss, and a voluntarily damaging week-long downtime. Even if they have backup systems, they cannot meet the SLA recovery time. To solve these problems, this work presents a secure database monitoring method for cloud computing. This approach adjusts the backup speed according to the data volume; This is important when data grows at least 30% per year. For some companies, data doubles every 3-4 years or more and SLAs and recovery targets need to be updated. At the same time, business needs for data recovery continue to grow, highlighting the need for more robust and responsive data management strategies.

INTRODUCTION

The relentless shift of business processes into the realm of information technology is transforming the way companies operate. Traditional paper-based documentation is rapidly becoming obsolete as the core of operations revolves around IT systems. The repercussions of data loss in this digital era are profound, with direct and indirect consequences, including reputational damage and financial losses. This shift has prompted a reevaluation of recovery time objectives as data volumes increase and service level agreement (SLA) requirements become more stringent. Classic backup systems are struggling to keep pace with the evolving data landscape, often necessitating complete system restoration, a time-consuming process. In a world where data generation is incessant, the urgency to protect data from the moment of creation is paramount, a challenge that traditional backup solutions fail to address. This paper delves into the critical importance of safeguarding data in the contemporary IT ecosystem, highlighting the complexities and shortcomings of existing backup systems and the need for innovative approaches to data protection.

As businesses transition towards IT-centric operations, the significance of data cannot be overstated. The reliance on IT systems to store and manage data means that the loss of data can have catastrophic implications for organizations. Not only can it disrupt day-to-day operations, but it can also result in severe financial losses. The reputation of a company can also suffer when it cannot fulfill its core business processes due to data unavailability.

In the fast-paced, data-driven business landscape, recovery time objectives are of paramount importance. As data volumes continue to surge, companies must reevaluate their data protection strategies. The conventional backup systems that have served organizations for years are struggling to keep up with the growing demands. Restoring large volumes of data, such as a 15 TB database, can take days, leading to significant downtime and potential data loss. The need for faster and more efficient data recovery solutions is evident.

In the contemporary data ecosystem, where information is generated and modified in real-time, traditional backup systems fall short of providing the necessary protection. Classic backup tools often necessitate restoring the entire system, which is time-consuming and impractical. Businesses need solutions that can protect data from the moment of its creation, ensuring that no data is lost, and no valuable time is wasted.

As data becomes increasingly critical to business operations, customers demand more comprehensive data protection solutions. They expect that data can be recovered quickly, and they are unwilling to accept prolonged downtimes or data loss. Traditional periodic test recoveries, while essential, can be costly and time-consuming.

In conclusion, the digital transformation of business processes has made data the lifeblood of organizations. Data loss can be catastrophic, leading to operational disruptions, financial losses, and reputational damage. The traditional backup systems are struggling to keep up with the evolving data landscape, necessitating a revaluation of data protection strategies. In this data-

driven world, companies need innovative solutions that can protect data from the moment of creation and ensure rapid recovery. This paper explores the challenges and shortcomings of existing backup systems and emphasizes the need for cutting-edge approaches to data protection in the IT age.

LITERATURE REVIEW

Effective data backup is an essential part of today's IT operations, but it has often faced problems historically. In the past, backup systems were created by companies or organizations to meet urgent needs. However, as the IT environment evolves, the backup process is often updated without optimization and the implementation of initial measures is ignored. It is important to establish a good data protection system; Backing up is just one part of a larger strategy than just solving silver bullets.

System administrators maintain backup lists, schedule backups, and save necessary data in a reliable location. Back up server-managed data. This server uses an intermediary to instruct computer users to make backups according to policies and schedules. Archived data will be sent to the designated replication office. Snapshot technology used in software or hardware helps keep data consistent during backup.

The key to meeting IT and business needs is to create a Service Level Agreement (SLA). Data security and data backup and recovery systems are components of a good data center. This new technology provides near-perfect backup and recovery, distinguishing it from traditional systems that rely on external media.

In conclusion, this literature review highlights the historical challenges of developing backup systems and the need to consolidate backup data to preserve broader information. He also discusses the role of physical administrators, snapshot technology, and the importance of SLAs in ensuring data security and rapid recovery.

METHODOLOGY

In today's rapidly evolving digital environment, information is the lifeblood of the organization. Protecting this information through efficient and effective recovery is important to ensure business continuity. But as the IT environment evolves and data volumes grow, traditional backup systems are now struggling to meet the needs of modern businesses. To solve these problems, we offer an effective method for data backup and recovery in a dynamic IT environment.

1. Separation of Speed and Capacity

Past systems for backup systems are often inadequate to adapt to IT environments. These systems are designed to meet initial requirements but are not flexible enough to grow with the organization. To overcome this limitation, companies creating modern data storage, usage and management systems (RMS)

recommend the use of tools that can separate the backup and restore speed of data volume.
The basic mechanism to achieve this is the use of snapshots. Snapshots provide near-instant backup and recovery with minimal disruption to physical operations. Snapshots capture a portion of data and should be included in the backup strategy to ensure clear control of the data backup and recovery process.

2. Data Recovery Selection
An important aspect of our approach is the importance of data recovery selection. The main thing is not to restore the entire system, but to keep only the necessary elements. Snapshots play an important role in this process, allowing organizations to quickly access specific data in a backup. Continuous data protection, such as Oracle Standby with Flashback, enables rapid delivery of data copies. This approach ensures data recovery is effective and objective, minimizing time and business disruption. It follows the principle that organizations return only what is needed at a particular time, thus saving time and resources.

3. Reduce Data Gap
The short duration of data creation and preservation may vary depending on the importance of the data. For less critical systems, our approach recommends using snapshot technology to reduce backup times to just a few hours. Snapshots serve as backup data and can be created periodically (for example, every hour).
In contrast, continuous data protection is required for critical systems. Technologies such as Oracle Standby with Flashback and proprietary software and hardware provide the ability to roll back data to a previous state, saving all changes. This approach ensures continuous data protection, allowing organizations to roll back to a specific point in time, thus reducing data loss.

4. Reduce Errors
Organizing your backups and measuring their effectiveness is an important but often overlooked practice. This approach recommends maintaining a simple computer backup, such as a backup system that can be quickly used for testing. This approach reduces the time and effort required to ensure the reliability of the backup compared to restoring the entire system.
Some advanced solutions have a trial function. These machines can run virtual machines periodically in the same environment using predefined procedures to ensure data is restored, applications are available, data such as storage is shared, and applications respond to appropriate requests. Automated measurement reduces the administrator's burden and makes data recovery readily available.

5. Transparency and Implementation

Complex backup and recovery processes that involve multiple technologies from different companies can be difficult to implement. This approach offers two options based on the organization's capabilities and interests:

Autarky: In this approach, the customer is responsible for monitoring performance under the guidance of experts. Integration involves establishing processes, management responsibilities, guidelines, and plans that enable the customer's IT department to develop and operate independently.

Outsourcing: For organizations that are unsure of their ability to manage ongoing processes, outsourcing to external experts is an option. This approach is especially important when service level agreement (SLA) requirements are high. Outsourcing streamlines the ongoing backup and recovery process and helps manage data recovery plans.

RESEARCH RESULT

Comparative analysis of Database Monitoring Method (DMM) and various data management methods available, including Security and Recovery (SBRS), Data Recovery Reporting and Recovery (DDBRM), Disaster Recovery and Security Automation (ADRS), and Control and Communications (CCM) . The goal is to manage data backups and the various methods and decisions to ensure data availability and security against threats and destruction.

Data Backup Management

The text confirms that unforeseen events such as a house fire, equipment failure (such as battery problems in server rooms), or equipment theft can have a negative impact on IT infrastructure and business operations. creates bad effects. In this case, backed up data should be stored away from the central server to reduce data loss.

Offsite Duplication Management

A good feature of data recovery is the ability to quickly recover data and access the data needed to recover. The plan adopts an offsite backup method, which means saving a copy to a remote location. Two main ways to set up this process are discussed

Removable Data

Data can be written to removable media (e.g. external hard disk, tape) and moved into body space. However, this approach needs to be planned for efficient delivery and rapid recovery when surgery fails.

Serverless Replication Control

This method uses a virtual private network (VPN) over the Internet to transfer data to a remote location. The advantage of this is that there is no need to physically modify the data. However, it requires a wide enough network channel (which can be expensive) and stringent security measures to protect data transmission.

Management of Published Data

Articles about the importance of using security measures when storing data. This includes protecting carriers in protected areas and preventing unauthorized access. Security measures may include access, confidentiality agreements, and other measures to ensure the confidentiality of information.

Data Encryption

When using media removal the text is about the need to encrypt the data stored on this device. Encryption ensures that even unauthorized people cannot access the media and decrypt the data. The text also recommends using "fab numbers" for additional data carriers to thwart data interception and attackers' attempts to authenticate data.

In summary, this article provides detailed information about decisions and methods related to data backup and recovery management. He emphasized the need for off-site data storage to protect against various threats and covered various topics such as physical transfer and serverless solutions. There is also an emphasis on strong security measures, including encryption and non-disclosure agreements, to protect the integrity and confidentiality of information. This comprehensive approach is designed to ensure that information remains robust in the face of unforeseen events and potential threats to IT infrastructure.

CONCLUSION

This article describes the use of special software to perform backup and recovery procedures, including storing data on various devices, especially tape devices. It emphasizes the importance of deciding what data will be stored, where and at what bandwidth. Centralized backup software provides the ability to restore specific files and database files without having to restore all files. Keeping backups on tape devices can save and protect important data in the event of a disaster. It is also said that the data stored on the media tape can be used for up to 50 years. But the effectiveness of this backup process depends on their regularity and frequency, especially if the data changes frequently. The text emphasizes the importance of using specialized software to automate the backup process to reduce the risk associated with hardware failure and data loss. In business, data loss can cause significant financial losses and customer loss. Therefore, ease of data recovery is an important consideration when choosing a backup program.

REFERENCES

Abraham Ekow Dadzie (2019). Literature Review On Data Security In Cloud Computing.

I. Berger. (2010, 6 May 2010). Keeping Cloud Computing's Prospects Safe and Sunny. Available: http://www.theinstitute.ieee.org/portal/site/tionline/menuitem.130a3558587d56e8fb2275875bac26c8/index.jsp?&pName=institute-level1-article&TheCat=2201&article=tionline/legacy/inst2010/may10/featuretechnology.xml& data gathering and incident response model for data security using honey pot system. International Journal for Research & Development in Technology, 5(5), 310–314.

Nareshvurukonda B. Thirumala Rao (2016). A Study on Data Storage Security Issues in Cloud Computing. Elsevier, 92: 128-135 https://doi.org/10.1016/j.procs.2016.07.335.

Sutharasan, M., & Logeshwaran, J. (2016, May). Design intelligence

Wang, F., Wang, H., & Xue, L. (2021, March). Research on data security in big data cloud computing environment. In 2021 IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC) (Vol. 5, pp. 1446–1450). IEEE.

Wang, Q. (2021, December). Cloud Data Backup and Recovery Method Based on the DELTA Compression Algorithm. In 2021 IEEE International Conference on Industrial Application of Artificial Intelligence (IAAI) (pp. 183–188). IEEE.

Yao, L. (2022). Feasibility Study Report on Cloud Technology of High-Performance Self-Service Database. In Innovative Computing (pp. 1315–1323). Springer, Singapore.

Zhang, Y., Xu, C., & Muntean, G. M. (2021, December). A Novel Distributed Data Backup and Recovery Method for Software Definedv WAN Controllers. In 2021 IEEE Global Communications Conference (GLOBECOM) (pp. 01–06). IEEE.