Data Recovery and Backup management: A Cloud Computing Impact

Conference Paper · June 2023

DOI: 10.1109/ICEST56843.2023.10138852

6 authors, including:

Muhammad Zulkifl Hasan
University of Central Punjab
131 PUBLICATIONS **252** CITATIONS
SEE PROFILE

Nadeem Sarwar
Bahria University
100 PUBLICATIONS **1,197** CITATIONS
SEE PROFILE

Intakhab Alam
University of Sialkot
4 PUBLICATIONS **25** CITATIONS
SEE PROFILE

Muhammad Zunnurain Hussain
Universiti Putra Malaysia
143 PUBLICATIONS **349** CITATIONS
SEE PROFILE

2023 IEEE International Conference on Emerging Trends in Engineering, Sciences and Technology (ICES&T) | 978-1-6654-5560-2/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICEST56843.2023.10138852

Data Recovery and Backup management: A Cloud Computing Impact

Muhammad Zulkifl Hasan
Faculty of Computer Science
and Information Technology
University of Central Punjab
Lahore, Pakistan
zulkifl.hasan@ucp.edu.pk
$[0000-0002-2733-5527]$

Nadeem Sarwar
Department of Computer Science
Bahria University Lahore Campus
Pakistan
Nadeem$_{s}rwr@yahoo.com$
$[0000-0001-8681-6382]$

Intakhab Alam
Department of Information Technology
University of Sialkot
Sialkot, Pakistan
Intakhab.alam@uskt.edu.pk

Muhammad Zunnurain Hussain
Department of Computer Science
Bahria University Lahore Campus
Pakistan
zunnurain.bulc@bahria.edu.pk
$[0000-0002-6071-1029]$

Adeel Ahmad Siddiqui
Department of Computer Science
National College of Business
Administration and Economics
Lahore, Pakistan
siddiquison6@gmail.com

Asma Irshad
School of Biochemistry
and Biotechnology
University of the Punjab
Lahore, Pakistan
asmairshad76@yahoo.com
$[0000-0002-0594-5877]$

***Abstract*—Cloud computing is the collection of excellent services (storage, databases, etc.) provided to customers and organizations over the internet to fulfill their requirements efficiently. Everything depends on the internet, and you can access your data anywhere. On the other hand, cloud service clients must ensure that the outsourced backup is secure enough to entrust with their data. This research highlighted how the cloud has benefited people by providing unlimited, secure storage without any high cost of investment in hardware. Cloud storage also aids in the security of your data backup, allowing you to access your files and documents even if your hardware is lost or damaged. It is also known as disaster recovery. Google Photos and Google Drive are examples of adequately encrypted backup storage. This paper also discusses the core functionalities of Google photos and Google drive and their advantages in a more comprehensive form. This research's main aim is to provide users with awareness regarding data loss and recovery. Furthermore, threats related to modern technology are also part of this research. In addition, the article also included some graphs and figures to explain the results and facts in detail.**

***Index Terms*—data recovery, formatting, backup management, cloud computing, physical storage**

I. Introduction

Google Cloud is an emerging and innovative technology that provides efficient computing and secure services for storing data and information on the internet. Storage is the feature of the cloud that makes it unique. Big companies and entrepreneurs prefer storing their data online, so they do not have to worry about any loss or deletion of data in the event of any loss or damage to the hardware system. It can be a hectic and lengthy process for companies and individuals to purchase the required media that can help store the data and get the backups. As a result, it may be preferable for them to enlist the assistance of cloud providers to provide cloud storage and backup services tailored to their specific requirements. The benefit of cloud computing is that people do not need to spend money on buying any hardware device for storage; all they need to invest in is an internet connection. It is not something that has the risk of fraud or any other disadvantage because already a lot of big companies and successful people in business are using it for storing data and having a timely backup of their company in a matter of minutes. The highlighted feature of cloud computing is its mobility, and users can access their data with the help of a good internet connection. They can access anything from anywhere. The assurance of deleting data while storing data online with a fully encrypted backup can be a genuine concern. The users may be hesitant to believe that the data is deleted and no longer accessible. The backup of sensitive data that can cause leaks of information or any other harm for a lifetime is not always preferred. That is why enterprises, businesses, and others desire to keep the backup of their liabilities and data for a fixed period and delete it afterward. "For example, the US Congress is formulating the Internet Data Retention legislation and is asking ISPs to retain data for two years, while in the United Kingdom, companies are required to retain wages and salary records for six years" [1].

The two main concerns for businesses and individuals were where their data was secure and propeller storage at a lower cost. The cost can be saved with the help of the cloud because companies do not have to spend much money buying new storage devices. After all, the previous ones are already full. Moreover, you do not have to spend extra on unwanted storage, and you can keep updating the storage according to your requirements and will only pay for the resources used instead of paying extra. Similarly, moving on to the concern of cloud security helped the users solve it. That is why people choose the most trusted option while selecting the cloud. The clouds have designed a securely backed-up storage system in which the files you choose to delete are entirely cleared from the cloud. Google places a high value on security by emphasizing it to employees at various office events and meetings. In their orientation process, they also provide proper training to their employees for security and privacy. A few steps that the Google cloud takes to ensure the security of your data are that it reviews and approves Google access before taking the user to private data, builds and runs secured workflows that adhere to international privacy regulations, and uses strong encryption to protect online privacy all through the data lifecycle. Strong encryption helps handle internet threats, such as viruses, spam, malware, etc. Different clouds claim different levels of security. The public internet is your most significant risk while accessing your data. In this paper, we discussed how the data can be kept secure with the help of the cloud and how Google Drive and Google Photos provide fully encrypted backups to users. The paper discussed how, because it is always possible to recover data, data recovery is also known as disaster backup.

The rest of the paper is organized as follows: Section 2 will provide the background and related work; Section 3 is the contribution. Section 4 is about recovery and data storage in cloud computing. Section 5 discusses our work, and the conclusion is discussed in Section 6.

II. BACKGROUND AND RELATED WORK

Cloud computing is a popular field among researchers. Much work has been published on this domain based on various parameters such as data recovery and backup management. Some of the current results are discussed as follows:

A paper by Suguna and Suhasini [2] states that organizations generate a lot of helpful information electronically in the modern world. This data needs to be saved in a secure place. Data recovery and backup issues are becoming very popular in networks nowadays. Due to the increase in data creation, the value of its safety is increasing every day. To meet goal recovery objectives in the modern world, business organizations require a proper backup plan at an affordable cost. Organizations must assess the likelihood of disasters and their potential implications. Supporting data is necessary for resistance against significant failures; in many cases, keeping backup information is regulated by law. The main objective of this paper is to show different cloud solutions that can help people and organizations manage their data. The comments in this article can be used to weigh the various options. To generate specifications, the application should first be investigated in terms of computational requirements and RTO. It is necessary to collect sufficient data to create construction models that will eventually allow the problem to be set up as a mathematical optimization. It is possible to create a model that links RTO and cost. According to some studies, the relationship between RTO and cost is non-linear.

Another paper written by Sharma and Singh [3] says that nowadays, data acts as fuel for different organizations. There is a lot of important information created by companies every day, so it is essential to save this information in a secure place. Therefore, we have different cloud platforms to do this job for us. Cloud platforms provide various organizations and infrastructure where they can store and play with their data. This makes the cloud a safe place for organizations. Due to the creation of a lot of data, the demand for an efficient technique is increasing to secure and manage company data. Many different strategies have been offered so far to attain this goal. We look at some current strategies in the form of disaster recovery techniques and online data backup in this review paper. This review article aims to compile a list of the most effective data backup and recovery solutions utilized in the cloud computing area. Of all the solutions examined in this research, the PCS is the most trustworthy solution because it protects each resource's privacy and costs very low.

A paper by Javeria [4] discusses that in cloud computing, failing in data recovery and backup management leads to many problems for organizations and businesses. Most cloud service providers charge a premium for data backup on their premises, which consumers and small businesses may not be able to afford. The research presents a straightforward solution for this challenging task in the form of cloud-based disaster recovery and data backup methods. This technique lowers the solution's cost, protects data from calamity, and allows switching from one cloud service provider to another more easily. This method relieves the consumer's dependency on service providers and reduces data backup costs. Even though the cloud is an extraordinarily diverse and fast-supplied solution, it currently needs a backup solution. We recommend that data be backed up on the consumer's premises. Consumers can get peace of mind at a low cost with cloud services. Without a backup plan, no solution is complete. For any business, business continuity and disaster recovery are crucial. The lack of cloud backup capability must be addressed by business organizations so that there will be no negative impact on businesses later.

Another paper by Baginda et al. [5] claims that the application's accessibility is incomparable. So, the application should be available twenty-four hours a day, seven days a week. The response time should be a blink of an eye because even for a single minute if the application is not investigated, this can cost the company's reputation and create substantial business problems. Now big organizations require cloud service providers to duplicate their infrastructure to make service available every time. Also, cloud providers are now providing data recovery services to help businesses recover their systems in the event of a disaster and maintain business stability. Many companies are still unsure which service will best fit their needs. RPO and RTO are two critical indicators for efficient data recovery. This paper focuses on the creation and implementation of two clouds and compares two parameters between them. In prior studies, prices, infrastructure, management, location, and other variables were used to compare DRaaS providers. There is no way to measure disaster recovery between cloud service providers. Therefore, an implementation strategy is introduced in this research. This strategy includes RTO and RPO benchmarking studies for choosing between cloud service providers.

”Security is the most important factor to consider when choosing a cloud storage provider because cloud storage is the location for data, and three aspects of data security must be met.” The cloud can be used as storage. The cloud should be checked and appropriately studied before trusting it completely. As time passes, innovations keep taking place. Now, numerous cloud and storage options are available for managing your profile and data online. Clouds ensure that your data is safe and secure over the internet.” Roughly 15% of business Cloud users have been hacked,” according to Google Drive and Dropbox, two companies that offer high-end secure and encrypted storage [6].”Our dedicated security team includes some of the world’s foremost experts in information security, application security, cryptography, and network security,” says Google while talking about its security and privacy policies. They also noted that the employees receive proper training for their job type. Google Cloud has developed a close relationship with the research community of security experts to provide its users with the best service possible. Google Cloud tries to improve its facilities over time by involving its team in continuous research. ”Our dedicated privacy team supports internal privacy initiatives that help improve critical processes, internal tools, products, and privacy infrastructure” [7].

The risk of failing to delete a file from the cloud due to overwriting is a big issue. Cloud security, or data assurance, ensures that your file is completely removed from the cloud. For the previous version, each backup version was typically built. It is normal to store only one copy of the file if the same file appears in multiple versions. A person should thoroughly search the cloud and its policies before trusting it with their data and files [8]–[12]. Data backup and recovery is one of the most critical issues in cloud computing environments, and the demand for practical approaches to data recovery is growing daily. Fault tolerance is a real concern in the cloud to ensure dependability and availability. The data recovery strategies are used to retrieve the data from the backup server when the server is unable to give the users the data or when the data has been lost due to one of several types of failures. This research included examples of cloud computing issues (loss of hardware, application failure, etc.), solutions (proactively tolerant of faults, clustering dynamically, etc.), and administration tools and methods (seeded block algorithm, parity cloud, etc.) [13].

Information technology professionals are drawn to cloud computing because it incorporates several evolving technologies. Furthermore, four cloud backup servers are used in a multi-server system based on enriched genetic algorithms to recover lost data. When the main cloud server fails and cannot offer data to users, the proposed approach gives the user the freedom to acquire information from any backup server to achieve dependability [14]. A technique called disaster recovery can be used to minimize downtime when hardware or software fails. A crucial necessity for the majority of enterprises is business continuity. This research explored the academic literature on business continuity, disaster recovery, and cloud computing. A literature search was done using numerous electronic databases after systematically evaluating the research on cloud computing, disaster recovery, and business continuity. However, the information technology sector will benefit from a clear understanding of the principles of the fields above and the advantages and problems they may present [15].

This research develops an experiment for data recovery and describes the experimental setting and objects in the experimental section. The challenge-response-verification framework, the number of data packets, the cost of computation and communication, the selection of the Spark method, the throughput of various platforms, and the iteration and cache analysis are all examined in the analysis section of this paper. The testing findings demonstrate that each node’s loss rate is less than 5% and that database 1’s loss rate in the fourth node is 0.4%, 2.4%, 1.6%, and 3.2%, demonstrating the system’s ability to handle applications [16]. Alzahrani et al. [17] discussed an architecture that uses a hybrid method to combine the benefits of replication and erasure coding to achieve the best storage solution, emphasizing reliability and recovery. Learning and training methods were created to offer dynamic structure building in the future and to verify the data model. The RAID architecture is utilized to create several configurations for the tests. RAID-1 through RAID-6 are separated into two categories, with RAID-1 to 4 in the first category and RAID-5 and 6 in the second, with additional classification depending on FTT, parity, failure range, and capacity. On the server side, reliability and recovery are tested, as well as data in transit at the virtual level. The aggregate findings suggest that the proposed hybrid framework considerably influences cloud storage performance. RAID-6c on the server was the ideal setup for optimal performance. Mirroring for replication using RAID-6 and erasure coding for recovery work in total coherence to produce good results for the existing framework while revealing fascinating and challenging future research routes. A computer security problem and legal system based on cloud computing are presented to enhance the safety and accuracy of computer information storage effectively. To begin, this essay delves into the evolution of cloud computing, its features, architecture, and application status. Second, we reviewed security techniques to maintain the confidentiality and integrity of cloud computing information, focusing on cloud data encryption technology and designing and implementing a data backup and recovery system based on a cloud platform. The system layer and data operation layer are the system’s essential layers. The system employs multithreading technology based on epoll and thread pools to boost data transmission efficiency. Simultaneously, the entire visual page is realized, and users may utilize it to develop a convenient operating system.

High-Security Distribution and Rake Technology (HSDRT) is employed in this study. Finally, the system is created in the laboratory and thoroughly tested. The test results reveal that the system in this work has a specific improvement in data transmission rate compared to the present generally used systems, but the use rate of node CPU is as high as 40%, which leads to certain demands for node CPU performance [18]. This article gives assessment findings for a high-security disaster recovery system that uses distribution and rake technology. If the verification is correct, the data user checks the document with the evidence and decrypts the encrypted file. The encryption and spatial scrambling performances and the average reaction time were estimated in an experimental assessment in terms of data file size. An efficient shuffling strategy for determining scattered position locations is also discussed. Finally, this study offers a system prototype setup for several practical network applications, including the hybrid use of commercially available cloud computing capabilities and settings [19].

III. Contribution

We conducted qualitative research in this study by researching various books and authors' journal papers utilizing search engines such as Google Scholar, Google, and others. The study discusses different cloud platforms businesses employ to store critical information since data is now used as fuel. We also discussed the literature comparing two cloud systems and how they handle data backup and recovery. Cloud systems provide infrastructure to different organizations; therefore, companies generate and store their data in a cloud. Because data is generated daily, cloud service providers compete regarding the management and maintenance of data.

IV. RECOVERY AND DATA STORAGE IN CLOUD COMPUTING

Because data storage processes are offered as services in cloud computing, it has unique features in terms of data security. First, the user information is kept on a cloud server, and since both uploads and downloads must pass across a network, the potential for data and information leakage in the medium grows. Second, cloud computing is based on a dispersed network, with computer servers acting as nodes and user data being saved in a network node. Third, information is stored by the third party to overcome these challenges. Similarly, redundant user data in the cloud storage system will put more storage demand on the cloud storage server, slow down network transmission, and demand more distant bandwidth. Data redundancy technology has become a prominent research issue in recent years to minimize the substantial quantity of duplicated data in cloud storage servers and conserve storage space and network traffic to the maximum degree.

Additionally, it's crucial to back up and recover any existing data. It is under pressure from the cloud storage system. Cloud storage security concerns are more concerned to data issues than cloud computing security issues. Security issues might result from data dissemination during the cloud node transmission operation. Data loss and leaks may occur as a result of internal assaults or unethical behaviour on the part of workers. User data may be compromised when the system is attacked.

Compared to traditional storage, the new characteristics of cloud storage have given rise to several new security concerns, including the requirement to guarantee the privacy and security of stored data and its availability and integrity [16], [20]–[22]. Some common data recovery approaches include the Seed Block Algorithm Architecture, Parity Cloud Services, and Bloom Filter [13].

V. Discussion

In the present era, organizations create a large amount of data daily, so it is very important to save this data securely. Different cloud platforms provide us with the benefit of storing important data for various organizations; even if the information is lost, they can still get it from cloud storage. We can use Google Photos as an example; you may have noticed that you take photos of yourself. In case of an emergency or mishap, your photos from phone storage are deleted. This is not an issue nowadays because Google Photos has already created a backup for its users. You can go into the Google Photos app, and all the pictures you clicked in the past are available there. You must download it and then get your photos again.

Similar is the case with organizations; cloud services provide SAAS, PAAS, and IAAS to different organizations depending on their needs. Organizations create a tremendous amount of information daily, so cloud services must provide secure and protected data for organizations and protect it from hackers. Because when you create a lot of helpful information daily, you become a favourite for hackers. It is good that the cloud provides a backup for every organization so that the data can be recovered, but it also must protect that information. Many organizations are using cloud services because it is the new and cheap solution for their data management, according to what an organization will pay for a service. However, organizations are also concerned about how cloud service providers store and use their data. The data may be stored in some hidden storage area by the cloud service providers, so there is a risk. Comparing the types of services provided by cloud service providers is impossible because there are different varieties of services, and each service has its pricing. AWS can be used as an example, which provides services depending on the input and output requirements, like CPU and GPU. However, we all know that if the amount of data produced is low, there are very low chances for data backup requirements. As a result, based on use-based pricing, the cost of a cloud server that is rarely fully installed would be relatively low. Cloud service providers can deal with many customers if customers need only I/O power or computational services randomly [13]–[16]. This allows for efficient multiplexing. Cloud service providers also benefit from significant economies of scale. Not only are locations or infrastructure shared due to cloud service providers, but the cost of maintenance per customer is also reduced. Table I shows the three backup possibilities of cloud computing.

TABLE I
THREE BACKUP POSSIBILITIES

Option	Data Synchronization	Statistical Independent	Ci	Co	Cd
Onsite	High	Low	High	D	High
Onsite	Medium	High	Low	D	High
Cloud	Low	High	Low	D	High

As we know, the speed of light does not apply when the distance is less than a few miles. In the same way, a backup server would allow for a high degree of synchronization. On the other hand, a geographical calamity would have a high likelihood of affecting such a server. Ongoing costs for cloud options may be lower. However, this depends on a variety of factors. There are some restrictions on the cloud; in the same region, the cloud may act as a disaster recovery site for some clients. Therefore, the cloud server may become overloaded with too many requests from different users. Cloud service providers promise a reserved capacity for consumption. However, it cannot guarantee that all computational resources will be available for non-service users. One of the dangerous drawbacks of the cloud is that it is vulnerable to undiscovered cloud-specific sabotage and vulnerabilities. The information regarding cloud system safety is not too much, and there are also some cases of cloud outages. Table II shows the three backup possibilities of cloud computing.

TABLE II
DATA RECOVERY APPROACHES

Factors	Managed Primary and DR instances	Cloud-Based backup and restore	Replication in Cloud
Instances	Salesforce.com, CRM, Email in the Cloud	On-premises into the cloud, Cloud to Cloud	On-premises into the cloud, Cloud to Cloud
Merits	Fully managed DR, 100% usage-based, Least complex	Only requires Cloud storage: Cloud virtual machines are optional, Usually less complex than replication	Best Recovery Time Objectives (RTOs) and Recovery Point Objectives (RP O's), More likely to support application consistent recovery
Caution	Service level agreements define access to production and DR instances	Less favorable RTO's and RPOs than replication	A high degree of complexity
Implementation	N/A	Backup applications and appliances	Replication software, cloud gateways, and cloud storage software such as EMC Atmos and Hitachi HCP

There is a need for an efficient system where people and organizations feel their data is secure and safe. It is still unknown whether the cloud system is entirely safe from hackers; when businesses generate a large amount of data and store it in the cloud, it becomes a popular target for many hackers to exploit. Fig. 1 and 2 describe the data recovery architecture.

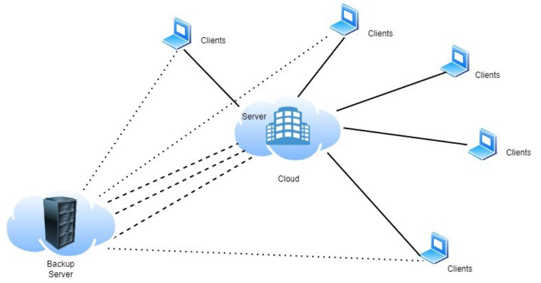

Fig. 1. Describes the data recovery architecture

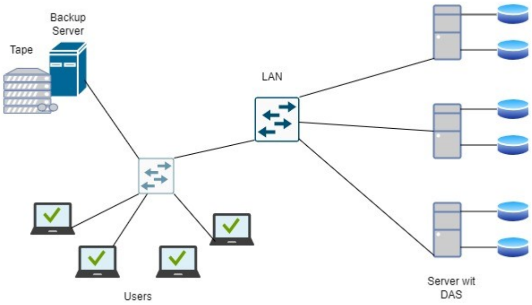

Fig. 2. Describes the data recovery across the network

Across the production LAN, three departmental servers share a shared tape backup resource. The most excellent sustained throughput from server to tape is around 25 GB per hour, even with switched 100 Mbps Ethernet and no competing user traffic. A full backup of the department's data will take 12 hours if each server supports a modest 100 GB of data. On the other hand, copies are typically scheduled daily for incremental backups of updated data, with complete disc backups occurring only once a month or quarter. Full backup routines would have to be rotated among different servers on different days and only when full LAN bandwidth was available to allow full and incremental backups. Fig. 3 shows the tradeoffs for disaster recovery in the cloud. Tape backup is difficult to justify due to the price and quickness of online, remote backup. Disaster recovery using cold site solutions has become unnecessary due to cloud computing. Warm site disaster recovery on private cloud-shared platforms has become a ubiquitous, cost-effective platform due to cloud computing, which allows virtual server backups to be located in minutes. In Fig. 4 cloud disaster recovery and backup can be seen.

VI. Conclusion

This paper provides qualitative research related to data recovery and backup management. Data management and recovery may help retrieve images, locations, data, etc. As a result, several cloud platforms offer this service to store our data so we can retrieve it promptly. Aside from these advantages, there is a significantly increased danger to data

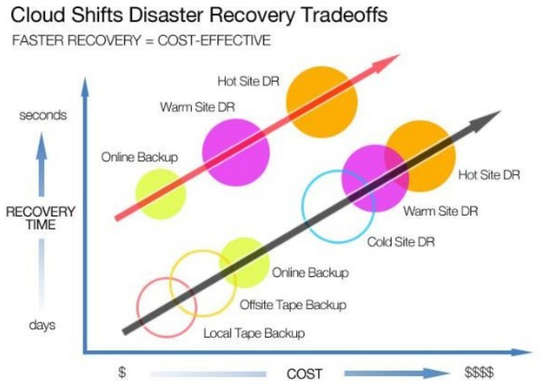

Fig. 3. Cloud disaster recovery tradeoffs

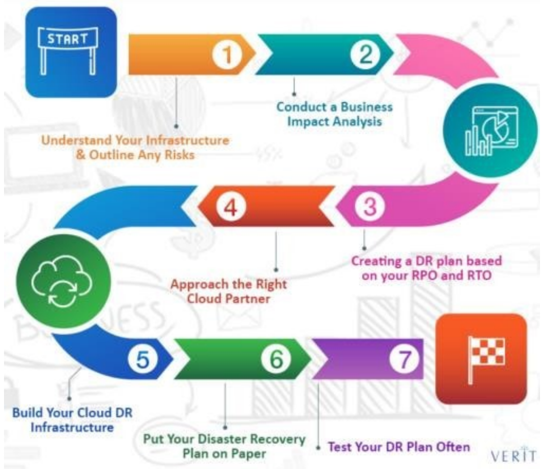
START
1
2
Understand Your Infrastructure & Outline Any Risks
Conduct a Business Impact Analysis
3
4
Creating a DR plan based on your RPO and RTO
Approach the Right Cloud Partner
5
6
7
Build Your Cloud DR Infrastructure
Put Your Disaster Recovery Plan on Paper
Test Your DR Plan Often
VERIT

Fig. 4. Cloud disaster and backup recovery programs

privacy and security. Some businesses also worry about how cloud service providers utilize and keep their data. There is insufficient information to develop an analytical model to determine the optimum implementation method. Even though the cloud is a quick and diversely provided option, it presently lacks a backup solution. According to our findings, the data should be restored depending on user choices. Users may be sure that their data is being backed up at a cheaper cost. For any business to run correctly, they require a backup plan, so it is clear that the solution is incomplete if there is no backup plan. To address the negative impact on enterprises, the absence of backup in cloud computing must be addressed.

References

[1] A. Rahumed, H. C. H. Chen, Y. Tang, P. P. C. Lee and J. C. S. Lui, ”A Secure Cloud Backup System with Assured Deletion and Version Control,” 2011 40th International Conference on Parallel Processing Workshops, Taipei, Taiwan, 2011, pp. 160-167, doi: 10.1109/ICPPW.2011.17.

[2] S. Suguna and A. Suhasini, ”Overview of data backup and disaster recovery in cloud,” International Conference on Information Communication and Embedded Systems (ICICES2014), Chennai, India, 2014, pp. 1-7, doi: 10.1109/ICICES.2014.7033804.

[3] Singh, K.. (2012). Online Data Backup and Disaster Recovery Techniques in cloud computing: A Review. IJET. 2. 249-254.

[4] V. Javaraiah, ”Backup for cloud and disaster recovery for consumers and SMBs,” 2011 Fifth IEEE International Conference on Advanced Telecommunication Systems and Networks (ANTS), Bangalore, India, 2011, pp. 1-3, doi: 10.1109/ANTS.2011.6163671.

[5] Y. P. Baginda, A. Affandi and I. Pratomo, ”Analysis of RTO and RPO of a Service Stored on Amazon Web Service (AWS) and Google Cloud Engine (GCE),” 2018 10th International Conference on Information Technology and Electrical Engineering (ICITEE), Bali, Indonesia, 2018, pp. 418-422, doi: 10.1109/ICITEED.2018.8534758.

[6] Agus, Irwan & Destiawati, Fitriana & Dhika, Harry. (2019). Perbandingan Cloud Computing Microsoft Onedrive, Dropbox, dan Google Drive. Faktor Exacta. 12. 20. 10.30998/faktorexacta.v12i1.3631.

[7] Saleem, Khizra & Bajwa, Imran & Sarwar, Nadeem & Anwar, Dr & Ashraf, Amna. (2020). IoT Healthcare: Design of Smart and Cost-Effective Sleep Quality Monitoring System. Journal of Sensors. 2020. 1-17. 10.1155/2020/8882378.

[8] Sarwar, Barera & Bajwa, Imran & Jamil, Noreen & Ramzan, Shabana & Sarwar, Nadeem. (2019). An Intelligent Fire Warning Application Using IoT and an Adaptive Neuro-Fuzzy Inference System. Sensors. 19. 3150. 10.3390/s19143150.

[9] Sattar, H., Bajwa, I. S., Sarwar, N., Shafi, U., Jamil, N., & Malik, M. G. (2019). An IoT-based Intelligent Wound Monitoring System. ArXiv. https://doi.org/10.48550/arXiv.1910.10062

[10] Kashif Hameed, Imran Sarwar Bajwa, Nadeem Sarwar, Waheed Anwar, Zaigham Mushtaq, Tayyaba Rashid, ”Integration of 5G and Block-Chain Technologies in Smart Telemedicine Using IoT”, Journal of Healthcare Engineering, vol. 2021, Article ID 8814364, 18 pages, 2021. https://doi.org/10.1155/2021/8814364

[11] Wajid Rafique, Maqbool Khan, Nadeem Sarwar, Wanchun Dou ”A Security Framework to Protect Edge Supported Software Defined Internet of Things Infrastructure”, COLLABORATECOM, Springer.

[12] Hussain, M. Z., Hasan, M. Z., Sarwar, N., Nasir, J., & Aslam, N. Cloud application importance and challenges: A Systematic Review. In 2021 International Conference on Innovative Computing (ICIC), pp. 1-6. IEEE. 2021.

[13] L. Saleh, “Cloud Computing Failures, Recovery Approaches, and Management Tools.” In 2020 21st International Arab Conference on Information Technology (ACIT), pp. 1-10. IEEE. 2020.

[14] P. S. Challagidad, A. S. Dalawai, and M. N. Birje. “Efficient and reliable data recovery technique in cloud computing.” Internet of Things and Cloud Computing, 5(1), pp. 13-18. 2017.

[15] A. M. Matar and A. I. Fakhri, Data recovery and business continuity in Cloud computing: A Review of the Research Literature. Int J Adv Comput Technol, 2016.

[16] D. Chang, L. Li, Y. Chang, and Z. Qiao. “Cloud computing storage backup and recovery strategy based on secure IoT and spark.” Mobile Information Systems, 2021.

[17] A. Alzahrani, T. Alyas, K. Alissa, Q. Abbas, Y. Alsaawy, and N. Tabassum. Hybrid Approach for Improving the Performance of Data Reliability in Cloud Storage Management. Sensors, 22(16), 5966. 2022.

[18] H. Li. Computer Security Issues and Legal System Based on Cloud Computing. Computational Intelligence and Neuroscience, 2022.

[19] R. Tripathi, V. Rai and A. Shrivastava. A Framework for Cloud Computing Data Backup and Recovery, 2022.

[20] S. Gokulakrishnan and J. M. Gnanasekar, “Data integrity and recovery management under peer-to-peer convoluted fault recognition cloud systems,” Journal of Computational and Theoretical Nanoscience, vol. 17, no. 5, pp. 2147–2150, 2020.

[21] F. Deng, L. Dong, and C. Zhe, “Control strategy of wind turbine based on permanent magnet synchronous generator and energy storage for stand-alone systems,” Chinese Journal of Electrical Engineering, vol. 3, no. 1, pp. 51–62, 2017.

[22] W. Wei, X. Fan, and H. Song, “Imperfect information dynamic Stackelberg game based resource allocation using hidden Markov for cloud computing,” IEEE Transactions on Services Computing, vol. 11, no. 99, pp. 78–89, 2018.