BOHR

ISSN (online) 2583-455X

BOHR International Journal of Computer Science
2023, Vol. 2, No. 1, pp. 1–7
https://doi.org/10.54646/bijcs.019
www.bohrpub.com

A Secured Database Monitoring Method to Improve Data Backup and Recovery Operations in Cloud Computing

G. Ramesh[1], J. Logeshwaran[2,*] and V. Aravindarajan[1]

[1]*Department of Information Technology, KLN College of Engineering, Madurai, India*
[2]*Department of ECE, Sri Eshwar College of Engineering, Coimbatore, India*
[*]*Corresponding author: drlogeshj@gmail.com*

Abstract. In general, the company sometimes uses unregistered functions in database, which significantly improves performance, but does not leave the possibility of recovery except for backup. That is, actions must be performed immediately after passing the session. A queue problem is likely to cause data loss and downtime of about a week. In modern conditions, this can lead to the bankruptcy of the company. It can be seen that backup systems have been installed and configured, but despite this, they have not succeeded in restoring within the time frame specified in the SLA. In this study, a secured database monitoring method was proposed to improve data backup and recovery operations in cloud computing. In this proposed method, the backup speed is directly proportional to the amount of data, while having at least 30% annual data growth. In 3–4 years, the data at least doubled, but for some companies, this number is even higher, while the backup speed does not change. Those terms and those SLAs that were relevant 3–4 years ago now need to be at least doubled. At the same time, business requirements for data recovery (recovery point objective/recovery time objective) continue to grow.

Keywords: Database, performance, recovery, backup, operating system, queue, downtime.

INTRODUCTION

All the business processes of the company are being transferred to information technology, and the paper primary (copies and originals of documents, reports, scans, etc.) is disappearing [1, 2]. Everything revolves around IT systems, and data loss literally means losing everything [3]. There is no more room for error. In the cases we presented, all the time, companies were unable to function due to the unavailability of data due to various circumstances [4, 5]. This led to direct and indirect losses, for example, reputational losses, when the company could not carry out its main business process, which is not easy to measure in monetary terms but in the long run does not cause less damage to the company [6–8]. We have reflected on our observations regarding recovery time objective. As your data grow, the actual recovery time must also grow, and the SLA requirements become stricter [9]. The point where the actual graph time equals the required time has already been sent to most clients [10]. In fact, most errors are associated with the loss of some part of the data. At the same time, traditional backup tools allow you to restore data directly from the backup, but often you need to restore the entire system [11–13]. If your database is 15 TB, this will take several days [14]. In a world where the master sheet disappears and everything is stored in IT systems, every second creates data that we want to protect immediately, the moment it is created. But this cannot be done using classic backup systems [15, 16]. Each data have a certain length of time, and these data exist all over the world in one copy [17].

The customers want to continue to protect their data from the moment it appears [18]. When you decide to restore from a backup, you often need to restore a day earlier and then have the data retrieved somewhere else a day later [19, 20]. As a rule, this is a long task for administrators that takes several days [21]. With a very negative development of events, it can lead to the loss of very important information [22]. Of course, the problem is not limited to backup; it is about the construction of

the IT system as a whole, and the title in this case is so important that it cannot be ignored [23, 24]. Unfortunately, there are no cheap and quick options to check how well the backup was done [25]. Of course, this can be done with periodic test recoveries, but this is a very expensive operation in terms of human effort and IT resources [26]. It is the work of a separate team on a separate hardware [27]. Most of the customers do not do this. It often happens that everyone creates backups, but during restoration, it turns out that they could not have been done – despite the outwardly correct operation of RMS, they cannot be restored [28, 29]. This happens for various reasons. This is best explained with an example [30]. A backup system is a service subsystem of a data center and has the following features:

- The backup process is not critical to solving IS problems. A failure of a backup system does not lead to a reduction in the availability of critical information services [31].
- The computational burden that the backup process creates is not beneficial to the provision of IS information services [32].

Naturally, it was forgotten in the maintenance industry for many years. Thus, a part of the data is completely lost [33, 34]. It took several more days to completely recreate the infrastructure services – no backups of operating systems, binaries, configurations, etc. [35]. All the missing information was collected from primary documents [36]. One of our customers used a SAP system with an Oracle database. The backup was carried out by inbuilt SAP tools with the help of huge vendors [37, 38]. Two different backup policies were configured: the first was file-based and copied the data of operating and software systems, and the second was the database itself [39]. Since they were sent to the same system, an exclusion list was constructed and entered into the database [40]. The file policy takes this list into account and does not allocate directories in the database [41]. Due to the uniqueness of the architecture, the database backup policy ignored the list of exclusions and correctly copied the required data [42].

RELATED WORKS

An improper approach to the problem of backup is a critical problem. Historically, the company or an integrator built it. At the time of construction, it certainly met all the requirements and performed its function perfectly [43]. Over the years, the enterprise IT landscape has changed. At the same time, the backup system was simply adjusted as the system evolved, and often no systematic approach was followed, which would take into account the importance of system compliance with initial indicators in all subsequent phases [44]. When developing a data protection system in your organization, you should take into account that this is only one part of your data protection strategy [45]. A reserve parachute is not a silver bullet, as many case studies prove that the approach to data protection must be comprehensive, so when developing it, we must consider where it will fit in the global strategy for data protection [46].

Table 1. The related issues and proposed suggestions.

Issues	Proposed Suggestions
The IBS was misconfigured, and no test reconfigurations were performed.	Use Database Standby located on a different queue. This will allow some time to transition to the running data instance.
There are no mechanisms for quick recovery in case of disaster and redundant systems.	Database ZDLRA backup appliances will allow database restoration in a very short period of time.
The number of attacks here was high because no clear DR plan was defined.	Smart planning of backup and recovery processes can avoid such huge losses and recover within a day.

A system administrator maintains an inventory of backup client computers, recording devices, and backup storage media and schedules backups. All this information is contained in a special database stored on the backup management server [47]. The management server instructs the agent program installed on the client computer to start backing up data according to the selected policy in accordance with the schedule or according to the operator's command [48]. The agent program collects and transfers the data to be backed up to the copy server specified by the management server [49]. The mechanism of action of "snapshots" is different and can be implemented both in software on a production server and in hardware within the array [50]. At the moment when the backup needs to be started, the agent program instructs the application to complete all transactions and save the cache memory [51]. A fundamental challenge for any data center is implementing a service level agreement between the IT department and the business [52]. A key aspect of meeting business needs is the assurance of data security, so a data backup and recovery system is an integrated infrastructure unit of a properly organized data center's data storage subsystem [53]. This type of backup and recovery actually takes a few seconds, which distinguishes this technology from classical systems with foreign media [54]. The issues in the existing systems and the proposed solutions are shown in Table 1.

PROPOSED MODEL

First, it is necessary to disconnect the backup and recovery speed from the computer volume. Data storage systems, application software, and RMS manufacturers recommend using some tools that can be used to solve this problem.

Snapshots allow you to back up and restore data in seconds with little or no impact on performance. This is done through sequence, while being able to control SRK, and should be part of its policy. Another solution may be to use various utility tools like Oracle Standby, DB2 HADR, and MS SQL Always On. All of these tools allow you to have a working copy of the production system, separated from the original, which can be deployed immediately. It allows you to work immediately after failures. The second is to make it possible to restore only the data you need. Our approach takes into account that when restoring a part of the data, there is no need to copy the entire system, we can restore the data we need at this time. This is achieved by the ability to quickly deploy or use existing systems that contain this data. As in the first case, the snapshot allows you to solve this problem (you can quickly open a snapshot on a neighboring server and extract the necessary data). It also includes continuous data protection technologies, for example, Oracle Standby with Flashback. They allow you to quickly deploy a working copy of your data in a timely manner.

If you need to get a logical volume, for example, a row or a database table, these tools greatly simplify the task, allowing you to restore the necessary data without restoring the entire copy. The third is to reduce the gap between the origin of data and its protection. This can be achieved in several ways, depending on the specifics of a particular case and the degree of importance of the data. For example, for less critical systems, the time interval for backups can be reduced to a few hours. In this case, we use snapshots. They can act as a restore point that can be done once per hour. Some modern arrays handle these processes very well and can store large numbers of system snapshots. This is a great way out of a situation where you need to step back for a while. For more critical systems, there may be no time interval, and data must be protected continuously. There are many solutions of this class, for example, Oracle Standby with Flash Back, which allows you to roll back the database for a while by recording all changes. You can use Oracle ZDLRA PAK, which will receive almost synchronously all changes in database, or general purpose software and hardware systems. They record all changes and allow you to restore to any point in time. Regular backups can be an indispensable tool in the event of major disasters or the need to recover data from long ago. However, in the present situation, it is only a reserve parachute, used at the last moment. The proposed model has the following important blocks (Figure 1):

- Backup
- Recovery
- Content analysis
- Contextual search
- Mobile data access
- Seamless integration with the cloud
- Information security tasks

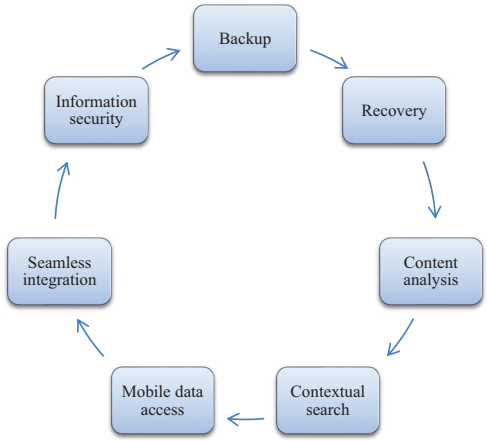

Figure 1. Important blocks of the proposed model.

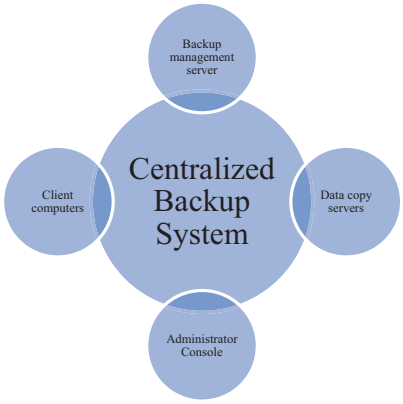

Figure 2. Components of centralized backup system.

The fourth is to reduce hidden errors. There is only one way to make sure that the backup is working correctly – try to restore it. This is the most perfect and rarely used method by our clients. But we offer a way out of this situation. First, have easily recoverable instances of computers. This is again a story about snapshot and standby systems that can be quickly deployed and tested. It takes incomparably less time and effort than "unpacking" an entire backup. Of course, this does not always help; but in case of an emergency, at least it gives a little more confidence that the data can be recovered by these means. Second, some SRCs allow automated testing. At a specific point in time on a schedule, you can run virtual machines in an isolated environment and use predefined algorithms to verify that data have actually been retrieved, that the application is available, that it is consistent, and that it is responding to the necessary requests. In this way, administrators can be relieved of long, routine tasks. A centralized backup system has a multi-layered architecture, which includes the following, as shown in Figure 2:

- A backup management server that can also incorporate the functions of a data copy server.

- One or more data copy servers to which backup devices are attached.
- Client computers that have backup agent programs installed.
- Backup System Administrator Console.

The fifth was the backup system's transparency. The described integrated approach involves creating a complex system using different technologies from different manufacturers. The task of making this system actually work, with further changes and scaling possible, is not trivial and can be tackled in two ways:

- The first way is that the customer is self-sufficient and wants to implement the system. Here, as a coordinator, we help create all the necessary processes, create regulatory frameworks, create all the necessary instructions and plans so that the customer's IT department can develop, and run the system in the right direction more independently. Then, transfer all this practical basis of terms and tasks to the customer in the form of functional organization of business processes.
- The second option is when the customer is not sure that the SRK system can be continuously maintained in a combat condition; the solution is to partially or fully outsource the system. We have clients who successfully use this service as both SLA requirements and our engagement levels as an IT outsourcer continue to increase.

Unfortunately, there is still no universal recipe for solving the problem of data recovery under the current conditions of constant system development and problems. Only a combination of the above solutions and a systematic approach will allow organizations to recover data at the point of business need. Backup systems ensure the continuity of business processes.

RESULTS AND DISCUSSION

The proposed database monitoring method (DMM) was compared with the existing storage backup and recovery strategy (SBRS), Distributed Data Backup and Recovery Method (DDBRM), Automation of Disaster Recovery and Security (ADRS), and control and communication management (CCM)

Data backup management: Events may have undesirable consequences for the IT infrastructure and business in general; for example, a fire in a building, the breakthrough of the central heating battery in the server room, or casual theft of equipment and components. One of the ways to avoid data loss in such situations is to store backups in a location away from the central area of the server equipment. The comparison of data backup management is shown in Figure 3.

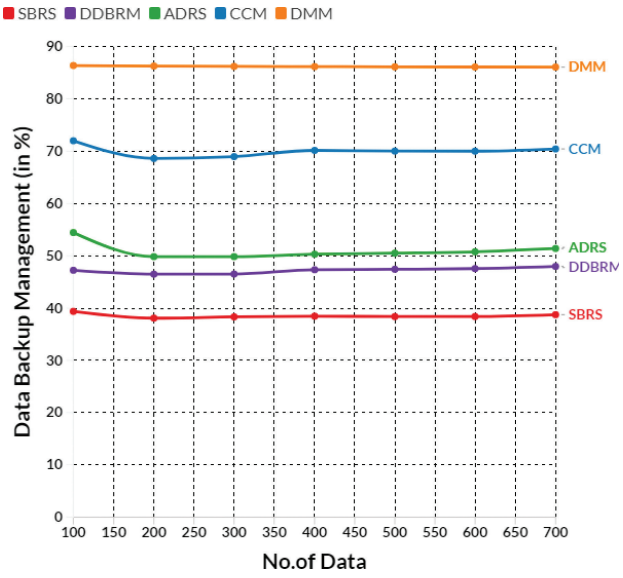

Figure 3. Comparison of data backup management.

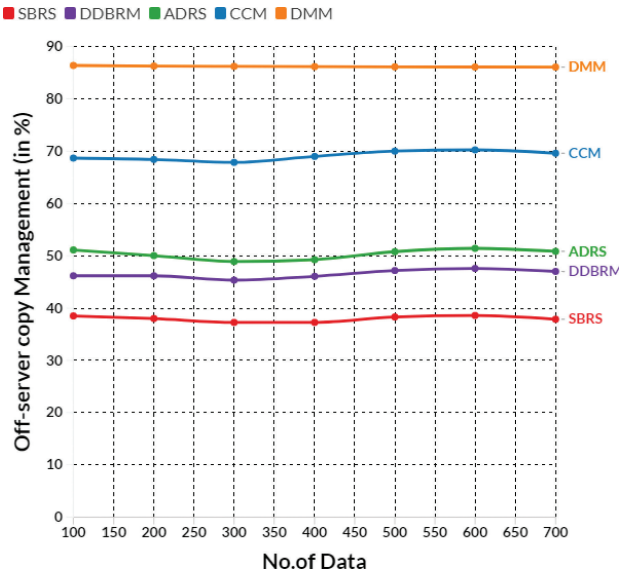

Figure 4. Comparison of off-server copy management.

Off-server copy management: Providing a quick way to access the data needed for recovery is essential. The method described is off-site (in other words, keeping copies off-site). Two methods are used to organize this process. It has been writing data to removable media and physically moving it. In this case, you need to take care of the means to provide the press quickly in case of failure. The comparison of off-server copy management is shown in Figure 4.

Storage device management: The advantage of this method is the ability to organize without difficulty. The downside is the difficulty of retrieving the media, the need to transfer the information to storage, and the risk of damaging the media in transit. They are copying data to

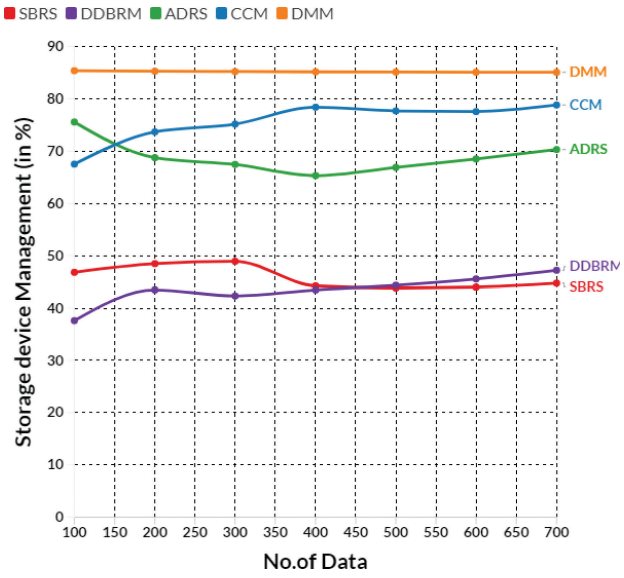

Figure 5. Comparison of storage device management.

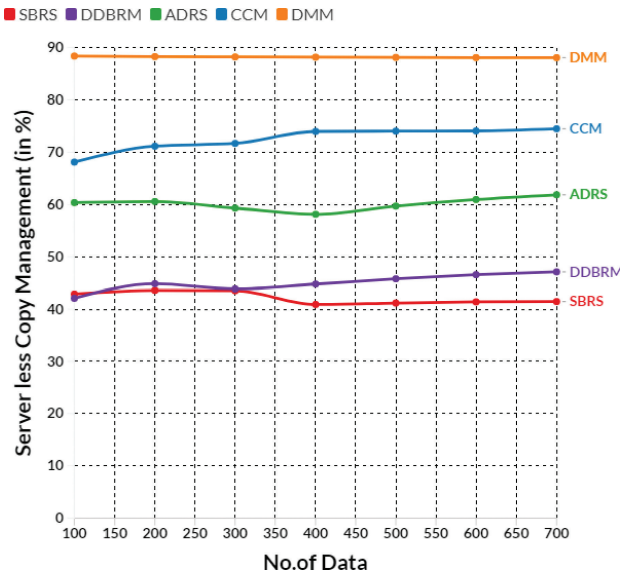

Figure 6. Comparison of server-less copy management.

another location over a network channel. The comparison of storage device management is shown in Figure 5.

Server-less copy management: This method uses a VPN tunnel over the Internet. The advantage is that there is no need to transport the information somewhere; the disadvantage is the need to use a sufficiently wide channel (as a rule, it is costly) and protect the transmitted data (e.g., using the same VPN). Compression algorithms or deductive technology can significantly reduce the difficulty in converting large amounts of data. The comparison of server-less copy management is shown in Figure 6.

Data copy management: Separately, security measures should be taken when organizing data storage. First, it is necessary to ensure that the data carriers are in a protected

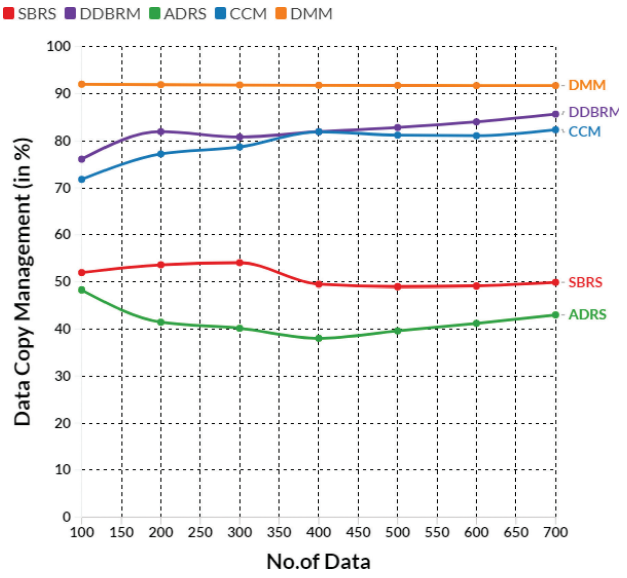

Figure 7. Comparison of data copy management.

area and that measures are in place to prevent unauthorized persons from reading the data, for example, by using an encryption system, entering a nondisclosure agreement, and so on. The comparison of data copy management is shown in Figure 7.

If removable media is involved, the data on it must also be encrypted. In this case, the marking system should not help the attacker analyze the data. It is necessary to use a faceless numbering scheme to indicate the carriers of the names of the changed files.

CONCLUSION

To automate backup processes, special software is used that controls the process of creating backups and the recovery process and allows you to work with various data carriers, including tape devices. What data should be stored, where, and on which bandwidth? Additional features of centralized backup software allow you to restore individual characters and database tables without restoring the entire volume of data. Writing backups to tape allows you to organize remote storage of backups and the protection of critical data in the event of a disaster. Using tape media to store archival copies allows data to be read 50 years after it was written. It will only be effective if done regularly. If data change frequently, replication should also be frequent. Therefore, rather than copying data manually, many prefer to use specialized software to automate this process. Any computer has many risks that can lead to hardware failure and loss of important data. In the business sector, this is even worse because the loss of business data results in huge losses and lost customers. When choosing a backup program, it wants to make sure that you can easily restore the data it wants.

REFERENCES

[1] Adhikari, N., Logeshwaran, J., & Kiruthiga, T. The Artificially Intelligent Switching Framework for Terminal Access Provides Smart Routing in Modern Computer Networks. BOHR International Journal of Smart Computing and Information Technology, 3(1), 45–50

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

[3] Gopi, B., Logeshwaran, J., Gowri, J., & Kiruthiga, T. (2022). The moment probability and impacts monitoring for electron cloud behavior of electronic computers by using quantum deep learning model. NeuroQuantology, 20(8), 6088–6100.

[4] 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.

[5] J. Logeshwaran (2022, October). The Topology configuration of Protocol-Based Local Networks in High speed communication networks. In Multidisciplinary Approach in Research, Vol. 15, pp. 78–83.

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

[7] Ramesh, G., Logeshwaran, J., & Aravindarajan, V (2022). The Performance Evolution of Antivirus Security Systems in Ultra dense Cloud Server Using Intelligent Deep Learning. BOHR International Journal of Computational Intelligence and Communication Network, 1(1), 15–19.

[8] Jin, D., & Wang, Q. (2021, January). CDP backup and recovery method for ensuring database consistency. In 2021 IEEE International Conference on Power Electronics, Computer Applications (ICPECA) (pp. 722–728). IEEE.

[9] Ramesh, G., Logeshwaran, J., Gowri, J., & Ajay Mathew (2022). The management and reduction of digital noise in video image processing by using transmission based noise elimination scheme. ICTACT Journal on image and video processing, 13(1), 2797–2801.

[10] Adee, R., & Mouratidis, H. (2022). A Dynamic Four-Step Data Security Model for Data in Cloud Computing Based on Cryptography and Steganography. Sensors, 22(3), 1109.

[11] Jasmine, J., Yuvaraj, N., & Logeshwaran, J. (2022, April). DSQLR-A distributed scheduling and QoS localized routing scheme for wireless sensor network. In Recent trends in information technology and communication for industry 4.0, Vol. 1, pp. 47–60.

[12] Jing, F., Huang, D., Wang, Y., Lv, X., & Du, Q. (2021, September). Remote Sensing Data Backup and Recovery System for Power Industry. In 2021 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom) (pp. 1717–1723). IEEE.

[13] Logeshwaran, J., Adhikari, N., Joshi, S. S., Saxena, P., & Sharma, A. (2022). The deep DNA machine learning model to classify the tumor genome of patients with tumor sequencing. International Journal of Health Sciences, 6(S5), 9364–9375

[14] Ravimaran, S., & Sathish, A. (2021). Robust Security With Strong Authentication in Mobile Cloud Computing Based on Trefoil Congruity Framework. Journal of Organizational and End User Computing (JOEUC), 33(6), 1–28.

[15] Logeshwaran, J., Ramkumar, M., Kiruthiga, T., & Sharan Pravin, R. (2022, February). SVPA - the segmentation based visual processing algorithm (SVPA) for illustration enhancements in digital video processing (DVP). ICTACT Journal on Image and Video Processing, 12(3), 2669–2673.

[16] Smara, M., Aliouat, M., Harous, S., & Pathan, A. S. K. (2022). Robustness improvement of component-based cloud computing systems. The Journal of Supercomputing, 78(4), 4977–5009.

[17] Ramesh, G., Aravindarajan, V., Logeshwaran, J., Kiruthiga, T., & Vignesh, S. (2022). Estimation analysis of paralysis effects for human nervous system by using Neuro fuzzy logic controller. Neuro Quantology, 20(8), 3195–3206.

[18] Ampera, D., & Fibriasari, H. (2021). Implementation of Cloud Computing System in Learning System Development in Engineering Education Study Program. International Journal of Education in Mathematics, Science, and Technology (IJEMST), 9(4), 728–740.

[19] Logeshwaran, J., Ramkumar, M., Kiruthiga, T., & Sharanpravin, R. (2022). The role of integrated structured cabling system (ISCS) for reliable bandwidth optimization in high-speed communication network. ICTACT Journal on Communication Technology, 13(01), 2635–2639.

[20] Jeslin, J. G., & Kumar, P. M. (2022). Implementing an Efficient Data Deduplication Framework for Cloud Storage. Indian J. Comput. Sci. Eng, 13, 136–144.

[21] Logeshwaran, J., Rex, M. J., Kiruthiga, T., & Rajan, V. A. (2017, December). FPSMM: Fuzzy probabilistic based semi morkov model among the sensor nodes for realtime applications. In 2017 International Conference on Intelligent Sustainable Systems (ICISS) (pp. 442–446). IEEE.

[22] Zhao, J., Zhang, L., & Zhao, Y. (2022). Informatization of Accounting Systems in Small-and Medium-Sized Enterprises Based on Artificial Intelligence-Enabled Cloud Computing. Computational Intelligence and Neuroscience, 2022.

[23] Raja, S., Logeshwaran, J., Venkatasubramanian, S., Jayalakshmi, M., Rajeswari, N., Olaiya, N. G., & Mammo, W. D. (2022). OCHSA: Designing Energy-Efficient Lifetime-Aware Leisure Degree Adaptive Routing Protocol with Optimal Cluster Head Selection for 5G Communication Network Disaster Management. Scientific Programming, 2022.

[24] Shaik, V., & Natarajan, K. (2021). Asynchronous Method of Oracle: A Cost-Effective and Reliable Model for Cloud Migration Using Incremental Backups. In Data Science and Security (pp. 417–427). Springer, Singapore.

[25] Ramesh, G., Logeshwaran, J., & Rajkumar, K. (2022). The smart construction for image preprocessing of mobile robotic systems using neuro fuzzy logical system approach. NeuroQuantology, 20(10), 6354–6367

[26] Belgacem, A. (2022). Dynamic resource allocation in cloud computing: analysis and taxonomies. Computing, 104(3), 681–710.

[27] Gopi, B., Ramesh, G., & Logeshwaran, J. (2022). An innovation for energy release of nuclear fusion at short distance dielectrics in semiconductor model. ICTACT Journal On Microelectronics, 8(3), 1430–1435.

[28] Zhou, J., & Zou, W. (2021, June). Construction and application of Wenhua education cloud based on Huawei FusionSphere. In 2021 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA) (pp. 477–481). IEEE.

[29] Logeshwaran, J. (2021, December). AICSA - an artificial intelligence cyber security algorithm for cooperative P2P file sharing in social networks. ICTACT Journal on Data Science and Machine Learning, 3(1), 251–253.

[30] Chang, D., Li, L., Chang, Y., & Qiao, Z. (2021). Cloud computing storage backup and recovery strategy based on secure IoT and spark. Mobile Information Systems, 2021.

[31] Logeshwaran, J., Malik, J. A., Adhikari, N., Joshi, S. S., & Bishnoi, P. (2022). IoT-TPMS: An innovation development of triangular patient monitoring system using medical internet of things. International Journal of Health Sciences, 6(S5), 9070–9084

[32] 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.

[33] Gopi, B., Ramesh, G., & Logeshwaran, J. (2022). The fuzzy logical controller based energy storage and conservation model to achieve

maximum energy efficiency in modern 5g communication. ICTACT Journal on Communication Technology, 13(3), 2774–2779.

[34] Tiwari, P. K., Pandey, S. K., Thamba Meshach, W., Parashar, J., Kumar, A., Altuwairiqi, M., & Krah, D. (2022). Improved Data Security in Cloud Environment for Test Automation Framework and Access Control for Industry 4.0. Wireless Communications and Mobile Computing, 2022.

[35] Sekar, G., Sivakumar, C., & Logeshwaran, J. (2022). NMLA: The Smart Detection of Motor Neuron Disease and Analyze the Health Impacts with Neuro Machine Learning Model. NeuroQuantology, 20(8), 892–899.

[36] Peng, X., Song, Y., Yuan, K., Guo, X., Lu, Z., & Liu, J. (2022, October). UCloudStack-A Private Cloud Platform for Lightweight Delivery. In 2022 IEEE 7th International Conference on Smart Cloud (SmartCloud) (pp. 184–189). IEEE.

[37] Ramkumar, M., Logeshwaran, J., & Husna, T. (2022). CEA: Certification based encryption algorithm for enhanced data protection in social networks. In Fundamentals of Applied Mathematics and Soft Computing, Vol. 1, pp. 161–170.

[38] Perri, D., Simonetti, M., Tasso, S., Ragni, F., & Gervasi, O. (2021, September). Implementing a scalable and elastic computing environment based on cloud containers. In International Conference on Computational Science and Its Applications (pp. 676-689). Springer, Cham.

[39] Logeshwaran, J., & Karthick, S. (2022, April). A smart design of a multi-dimensional antenna to enhance the maximum signal clutch to the allowable standards in 5G communication networks. ICTACT Journal on Microelectronics, 8(1), 1269–1274.

[40] Shareef, T. H., Sharif, K. H., & Rashid, B. N. (2022). A Survey of Comparison Different Cloud Database Performance: SQL and NoSQL. Passer Journal of Basic and Applied Sciences, 4(1), 45–57.

[41] Logeshwaran, J. (2022, March). The control and communication management for ultra dense cloud system using fast Fourier algorithm. ICTACT Journal on Data Science and Machine Learning, 3(2), 281–284.

[42] Subramani, R., Kaliappan, S., Arul, P. V, Sekar, S., Poures, M. V. De, Patil, P. P., & Esakki, E. S. (2022). A Recent Trend on Additive Manufacturing Sustainability with Supply Chain Management Concept, Multicriteria Decision Making Techniques. 2022.

[43] Logeshwaran, J., & Shanmugasundaram, R. N. (2019, December). Enhancements of Resource Management for Device to Device (D2D) Communication: A Review. In 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) (pp. 51–55). IEEE.

[44] Raja, S., & Rajan, A. J. (2022). A Decision-Making Model for Selection of the Suitable FDM Machine Using Fuzzy TOPSIS. 2022.

[45] Ramesh, G., Logeshwaran, J., Aravindarajan, V., & Feny Thachil. (2022). Eliminate the interference in 5g ultra-wide band communication antennas in cloud computing networks. ICTACT Journal On Microelectronics, 8(2), 1338–1344.

[46] Raja, S., Rajan, A. J., Kumar, V. P., Rajeswari, N., Girija, M., Modak, S., Kumar, R. V., & Mammo, W. D. (2022). Selection of Additive Manufacturing Machine Using Analytical Hierarchy Process. 2022.

[47] Gopi, B., Logeshwaran, J., Gowri, J., & Aravindarajan, V. (2022). The Identification of quantum effects in electronic devices based on charge transfer magnetic field model. NeuroQuantology, 20(8), 5999–6010.

[48] Venkatasubramanian, S., Raja, S., Sumanth, V., Dwivedi, J. N., Sathiaparkavi, J., Modak, S., & Kejela, M. L. (2022). Fault Diagnosis Using Data Fusion with Ensemble Deep Learning Technique in IIoT. 2022.

[49] Vaniprabha, A., Logeshwaran, J., Kiruthiga, T., & Krishna Bikram Shah (2022). Examination of the Effects of Long-term COVID-19 Impacts on Patients with Neurological Disabilities Using a Neuro machine Learning Model. BOHR International Journal of Neurology and Neuroscience, 1(1), 21–28.

[50] Nasurudeen, T. F. K., Shukla, V. K., & Gupta, S. (2021, June). Automation of Disaster Recovery and Security in Cloud Computing. In 2021 International Conference on Communication information and Computing Technology (ICCICT) (pp. 1–6). IEEE.

[51] Gopi, B., Logeshwaran, J., & Kiruthiga, T (2022). An Innovation in the Development of a Mobile Radio Model for a Dual-Band Transceiver in Wireless Cellular Communication. BOHR International Journal of Computational Intelligence and Communication Network, 1(1), 20–25.

[52] Saravanakumar, K., & Logeshwaran, J. (2016, February). Auto-Theft prevention system for underwater sensor using lab view. International Journal of Innovative Research in Computer and Communication Engineering, 4(2), 1750–1755.

[53] Sutharasan, M., & Logeshwaran, J. (2016, May). Design intelligence data gathering and incident response model for data security using honey pot system. International Journal for Research & Development in Technology, 5(5), 310–314.