IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 4, April 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304016 |

Shielding Cloud Secrets Revocable Storage With Identity Based Encryption

Dr.J.Jeyaboopathiraja[1], Sandhiya S[2]

[1]Assistant Professor, PG & Research Department of Computer Science, Sri Ramakrishna College of Arts & Science, Coimbatore, India

[2]UG Student, PG & Research Department of Computer Science, Sri Ramakrishna College of Arts & Science, Coimbatore, India

ABSTRACT: This paper explores the safeguarding of confidential cloud information through the implementation of revocable storage with identity-based encryption, ensuring enhanced security measures for protecting sensitive data. The revocable storage mechanism adds an additional layer of protection, allowing for swift and effective revocation of access privileges when needed. This proactive measure ensures that compromised credentials or changes in authorization status are promptly addressed, minimizing the window of vulnerability. Through meticulous integration of these techniques, we present a comprehensive strategy for shielding sensitive data in the cloud environment. Key features of our approach include dynamic access control, cryptographic key management, and efficient revocation protocols. These elements collectively contribute to a resilient defense against evolving cyber threats. The system's adaptability enables seamless integration with existing cloud architectures, making it a practical and scalable solution for diverse cloud environments. Furthermore, our solution prioritizes user privacy by maintaining a balance between security and usability. By carefully considering the trade-offs, we achieve a solution that not only fortifies cloud secrets but also ensures a user-friendly experience. The proposed framework serves as a robust foundation for secure data sharing, fostering trust and confidence in cloud-based services. As the digital landscape continues to evolve, our approach provides a forward-looking solution to the ever-present challenges of cloud security. Personality based encryption is a promising crypto graphical crude to assemble commonsense information sharing framework. Be that as it may, access control isn't static. That is, the point at which some client's approval is terminated, there ought to be an instrument that can eliminate him/her from the framework. Thusly, the renounced client can't get to both the beforehand and consequently shared information. To this end, we propose an idea called revocable-capacity character-based encryption (RS-IBE), which can give the forward/in reverse security of code text by presenting the functionalities of client renouncement and code message update all the while.

KEYWORDS: Cloud, storage, encryption, security, decryption

I. INTRODUCTION

This part describes the need for cloud technology, As the internet sprang up, the amount of data increased day by day and many new methodologies were needed to increase the speed of access and to manipulate (store and retrieve) the data efficiently. The Operating Systems subject has clearly stated a point that the efficiency of the processors and other hardware components are not utilised completely. Hence different techniques such as Time Sharing, Batch Processing are been implemented. Even though these techniques use the resources efficiently, still there is a void in the concept. Apart from this today everything has been networked and the IT industry's want to serve their customers at any place. This makes the concern to scale their business to a wide area. Scaling involves many pre planned activities such as to buy the required hardware and software components to deploy their service. This is a very cost consuming process which the business needs to reduce. The reason that is the result of scaling process is maintenance. Once the required resources are been deployed and implemented it has to be maintained to achieve the desired result by the company. Again this is also an high expense for the concern. Along with this thinking from the social and environmental perspective, buying new resources and deprecating significantly increases the amount of e-waste which is an environmental hazard.

Distributed computing has as of late risen as a convincing worldview for managing and conveying administrations over the web [1]. The ascent of this system is quickly changing the scene of data innovation, and eventually transforming the long-held guarantee of utility figuring into a reality. The most recent development of this system is a noteworthy advance towards understanding this utility registering model since it is vigorously determined

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304016 |

by industry merchants [2]. It draws in entrepreneurs because of its capacity to wipe out the provisioning plan overhead, and enables ventures to begin from the little scale and progressively increment their assets all the while with the expansion of their administration request. It guarantees to convey solid administrations through cutting edge server farms based on virtualized register and capacity advances [3]. Clients will have the capacity to get to applications and information from a Cloud anyplace on the planet following the compensation as you-go money related model. The difficulties confronting the new worldview, for example, security, and accessibility and assets administration; ought to be precisely considering in future research with a specific end goal to ensure the long achievement of distribute computing [4].

Cloud security issues might stem because of the center innovations usage (Virtual Machine (VM) escape, session riding, and so forth.), cloud benefit contributions, and emerging from cloud qualities (information recuperation weakness, Internet convention powerlessness, and so on.) [5]. For a cloud to be secure, the majority of the taking interest elements must be secure. In any given framework with different units, the mainly abnormal amount of the frameworks security is equivalent to the security level of the weakest element [6]. In this way, in a cloud, the security of the benefits doesn't exclusively rely upon a person's safety efforts [5]. The neighbouring elements may give a chance to an assailant to sidestep the client's resistances.

Cross- tenant virtualized organize access might likewise trade-off information protection and trustworthiness. Uncalled for media sterilization can likewise release client's private information [5]. The information outsourced in the direction of an open cloud has to be secured. Unapproved information access by different clients and procedures should be counteracted [6]. As examined over, any weak substance is able to put the entire cloud in danger. In such a situation, the security instrument should significantly get bigger an assailant's push in the direction of recover a sensible measure of information even following a successful interruption in the cloud. Besides, the likely measure of data loss should likewise be limited.

A cloud should make sure throughput, dependability, and safety [15]. A type issue formative the throughput of a cloud with the purpose of stores information is the information retrieval time [7]. In large-scale systems, the issues of information reliability, information availability, and response time are solved by using the information replication strategies [8]. On the other hand, placing replicas information over a number of nodes enhances the attack surface for with the purpose of specific information.

From the above discussion, we are able to assume with the purpose of together security and performance are significant for the future generation large-scale systems. Adaptive Particle Swarm Division and Replication of Data Optimization (APSDRDO) are proposed for enhancing security of cloud data and automatic updating of the data storage. It is calculated to introduce an automatic update algorithm with the intention of be able to find and update the needed fragments only. It is not only enhances the security level of the cloud system, in addition it also saves the time and resources make use of it downloading, updating, and uploading the file again.

II. RELATED WORKS

Tu et al [8] considered the issue of ideal allotment of secure data objects. The framework topology likewise regard as includes of two layers. In the upper layer, various groups frame a system topology with the purpose of be able to be spoken to by a general graph model. The nodes inside each group additionally have a topology spoke to by a general graph. At that point decay the offer replication designation issue into two sub-issues, the tenant set issue, which apportions a subset of offers to groups, and the intra-group portion issue which decides the quantity of offer copies to be distributed and their arrangements. Two diverse heuristic calculations are created for the two sub-issues. The calculation for the ideal occupant set issue has a period multifaceted nature of O(n/sup 2/). An O(n/sup 3/) calculation is exhibited for the intra-group distribution issue. In any case, the plan concentrates just on the security of the encryption key.

Juels and Opera [10] proposed a new technique which expanding the information trust border from the venture to people in general cloud requires more than encryption. Besides, the likely measure of misfortune if there should arise an occurrence of information tempering because of interruption or access by different VMs can't be reduced. Mei et al [11] displayed a distributed system for document portion with the purpose of make ensures high affirmation, accessibility, and versatility in a large distributed file system. The calculation is able to make use of replication and discontinuity plans to dispense the records over various servers. The confidentiality and honesty are saved, even within the sight of a successful assault with the purpose of bargains a subset of the document servers. The calculation is adaptive as in it changes the document assignment as the read-compose designs and the area of the customers in the system change. Likewise formally demonstrate with the purpose of accepting read-compose designs are steady; the

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304016 |

calculation focalizes toward an ideal file allocation, where optimality is characterized as expanding the record confirmation.

Loukopoulos and Ahmad [12] proposed an enhanced Genetic Algorithm (GA) with the purpose of considers as info the present copy conveyance and figures one utilizing information regarding the system characteristics and the progressions happened. Keeping in see more businesslike situations in the present circulated data conditions, we assess these calculations as for the capacity limit limitation of each site and in addition varieties in the disrepute of items, and furthermore look at the exchange off between running time and arrangement quality.

Tang et al [13] built up a protected overlay distributed storage framework with the purpose of accomplishes fine-grained, approach depending on the access control and record guaranteed deletion. It partners outsourced documents with record get in the direction of arrangements, and certainly erases records in the direction of make them unrecoverable to tons of record get to strategies. To accomplish such security objectives, FADE are performed depending upon an arrangement of cryptographic key tasks with the purpose of are self-kept up by a majority of key supervisors with the purpose of are free of outsider mists. Particularly, FADE goes about as an overlay framework with the purpose of works again and again on the present distributed storage administrations. Likewise actualize a proof-of-idea model of FADE on Amazon S3, single of the present distributed storage administrations.

Zissis and Lekkas [14] proposed a Trusted Third Party, entrusted by means of guaranteeing particular security attributes inside a cloud domain. The proposed work named upon the cryptography, particularly Public Key Infrastructure working together with Single sign-on (SSO) and Lightweight Directory Access Protocol (LDAP) in order in the direction of guarantee the confirmation, trustworthiness and secrecy of included information and correspondences. The arrangement, exhibits a flat level of administration, accessible in the direction of every single involved substance, which understands a security work, inside which fundamental trust is kept up.

III. METHODOLOGY

The security of a huge-scale scheme proposed for cloud based on the security as a complete and the security of specific nodes. A winning intrusion interested in a particular node might have rigorous consequences, not simply for information and applications on the victim node, other than moreover designed for the previous nodes. A doing well intrusion might be a result of some software susceptibility [11]. In case of homogenous systems, the same flaw is able to be making use of target previous nodes inside the system. The achievement of an attack on the following nodes determination needs less effort as compared in the direction of the attempt on the first node. Relatively, additional effort is needed intended for varied systems. On the other hand, cooperation a solitary file determination needs the attempt in the direction of go through merely a solitary node. The amount of compromised information be able to be decreased with creation fragments of an information file and storing information them on divide nodes [11]. A doing well intrusion on a particular or a small number of nodes determination only give admission towards a portion of information with the purpose of capacity not be of some importance. Furthermore, if an attacker is vague regarding the positions of the fragments, the probability of discovering fragments on each and every one of the nodes is extremely low. Let us regard as a cloud by means of M nodes and a file by means of z number of fragments. Let s be the quantity of winning intrusions on different nodes, such with the purpose of s>z.

The proposed system aims to enhance cloud security through the implementation of Identity-Based Encryption (IBE) for revocable storage of sensitive data. Users' identities serve as public keys, facilitating granular access control and streamlined revocation processes. The system integrates seamlessly with existing cloud storage infrastructure, offering robust protection against unauthorized access and data breaches. Key management is simplified, ensuring efficient management of access privileges. Additionally, the system provides administrators with intuitive tools for swift and effective revocation of access. By leveraging IBE, the proposed system strengthens cloud security, safeguarding sensitive information and bolstering trust in cloud services.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304016 |

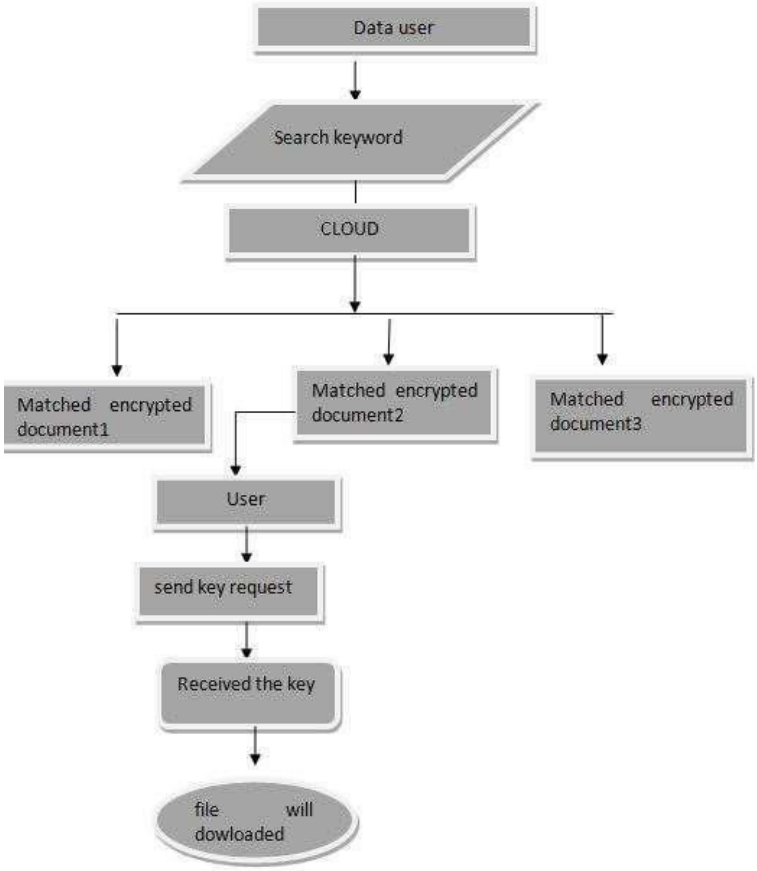

Figure-1 System Architecture

The Blowfish algorithm is a symmetric-key block cipher that can be utilized as part of the encryption process within the Shielding Cloud Secrets Revocable Storage system. Here's how the Blowfish algorithm can be integrated into the proposed framework:

Data Encryption using Blowfish

Before encrypting data for storage in the cloud, the Blowfish algorithm can be employed to encrypt the data symmetrically. Blowfish operates on fixed-size blocks of data and uses a key-dependent algorithm for encryption. The plaintext data is divided into fixed-size blocks suitable for Blowfish encryption. The Blowfish encryption algorithm, using a symmetric key \(K \), is applied to each block of data to produce ciphertext.

Data Decryption using Blowfish

When retrieving encrypted data from the cloud, the Blowfish algorithm can be used for decryption. The ciphertext data is divided into fixed-size blocks.The Blowfish decryption algorithm, using the same symmetric key \(K \), is applied to each block of ciphertext to recover the plaintext data.

3. Integration with Identity-Based Encryption (IBE)

Before applying Blowfish encryption, the symmetric encryption key \(K \) needs to be encrypted using Identity-Based Encryption (IBE). The user's public key obtained from the Identity-Based Encryption system is used to encrypt the symmetric key \(K \). The encrypted symmetric key is then combined with the Blowfish-encrypted data for storage in the cloud.

IV. RESULTS AND DISCUSSION

The system has been extensively tested to ensure that it fulfills its intended functionalities, including:

Secret Storage: Users can securely store sensitive data in the cloud, leveraging the identity-based encryption mechanism to protect their secrets.

Secret Retrieval: Authorized users can retrieve their stored secrets securely, ensuring data confidentiality and integrity during transmission.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304016 |

Access Control: Granular access control mechanisms allow users to manage permissions effectively, ensuring that only authorized individuals can access specific secrets.

Revocation Mechanism: The system implements a robust revocation mechanism, enabling users to revoke access to their secrets promptly and effectively when necessary

The communicational backbone of distributed computing is the Data Center Network (DCN) [22-23]. In this work, make use of three DCN designs in the direction of be precise: (a) Three level, (b) Fat tree, and (c) DCell [22]. The Three levels is the heritage DCN engineering. Be with the purpose of as it might, in the direction of meet the introducing requests of the distributed computing, the Fat tree and Dcell models were introduced [23]. In this way, make use of the previously mentioned three designs in the direction of assess the execution of plan on inheritance and in addition best in class models. The Fat tree and three level models are switch-driven systems. The nodes are associated by means of the entrance layer switches. Numerous entrance layer switches are associated utilizing total layer switches. Center layers switches interconnect the entire layer switches. The Dcell is a server driven system engineering that utilizations servers notwithstanding changes to play out the communication procedure contained by the system [1]. A server in the Dcell design is associated with different servers and a switch. The lower level dcells recursively construct the more elevated amount dcells. The dcells at a similar level are completely associated. For insights about the previously mentioned structures and their execution examination, the perusers are urged to peruse [1] and [2].

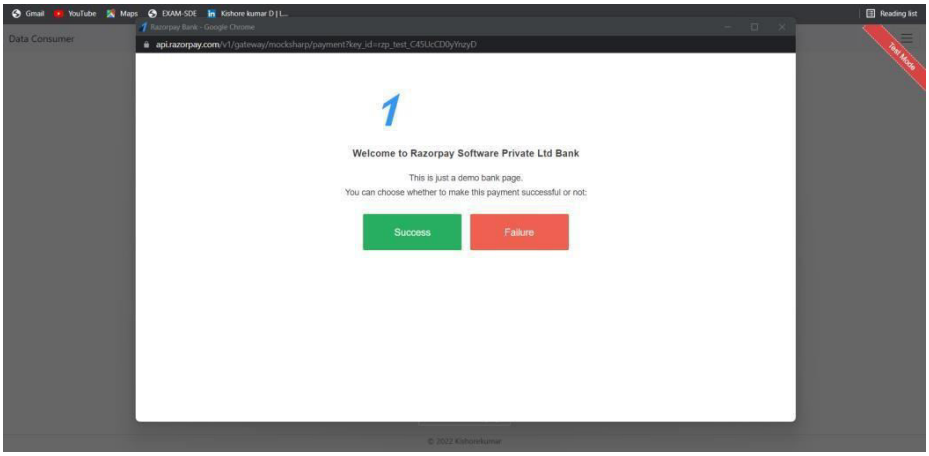

Fig-2 Cloud storage Results

V. CONCLUSION

Cloud computing has many advantages such as space of storage is increased and cost of storage is reduced and decreases overheads on cloud, storage security. Proving the security to the data placed in cloud computing has become major issue in this IT platform. This paper mainly concentrates on security and privacy issues and also discusses about the different techniques used in existing cloud environments. Further, these different techniques are used in improving the security of the data stored and also giving privacy to data. Cloud computing has the potential to be a disruptive affected by the force of technology uses.

REFERENCES

1. Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. and Zaharia, M., 2010. A view of cloud computing. Communications of the ACM, 53(4), pp.50-58.
2. Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J. and Brandic, I., 2009. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation computer systems, 25(6), pp.599-616.
3. Zhang, Q., Cheng, L. and Boutaba, R., 2010. Cloud computing: state-of-the-art and research challenges. Journal of internet services and applications, 1(1), pp.7-18.
4. Hayes, B., 2008. Cloud computing. Communications of the ACM, 51(7), pp.9-11.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304016 |

5. B. Grobauer, T.Walloschek, and E. Stocker, "Understanding cloud computing vulnerabilities," IEEE Security and Privacy, Vol. 9, No. 2, 2011, pp. 50-57.
6. L. M. Kaufman, "Data security in the world of cloud computing," IEEE Security and Privacy, Vol. 7, No. 4, 2009, pp. 61-64.
7. N. Khan, M. L. M. Kiah, S. U. Khan, and S. A. Madani, "Towards Secure Mobile Cloud Computing: A Survey," Future Generation Computer Systems, Vol. 29, No. 5, 2013, pp. 1278-1299.
8. M. Tu, P. Li, Q. Ma, I-L. Yen, and F. B. Bastani, "On the optimal placement of secure data objects over Internet," In Proceedings of 19th IEEE International Parallel and Distributed Processing Symposium, pp. 14-14, 2005.
9. D. Boru, D. Kliazovich, F. Granelli, P. Bouvry, and A. Y. Zomaya, "Energy-efficient data replication in cloud computing datacenters," In IEEE Globecom Workshops, 2013, pp. 446-451.
10. A. Juels and A. Opera, "New approaches to security and availability for cloud data," Communications of the ACM, Vol. 56, No. 2, 2013, pp. 64-73.
11. A. Mei, L. V. Mancini, and S. Jajodia, "Secure dynamic fragment and replica allocation in large-scale distributed file systems," IEEE Transactions on Parallel and Distributed Systems, Vol. 14, No. 9, 2003, pp. 885-896.
12. T. Loukopoulos and I. Ahmad, "Static and adaptive distributed data replication using genetic algorithms," Journal of Parallel and Distributed Computing, Vol. 64, No. 11, 2004, pp. 1270-1285.
13. Y. Tang, P. P. Lee, J. C. S. Lui, and R. Perlman, "Secure overlay cloud storage with access control and assured deletion," IEEE Transactions on Dependable and Secure Computing, Vol. 9, No. 6, 2012, pp. 903-916.
14. D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Future Generation Computer Systems, Vol. 28, No. 3, 2012, pp. 583-592.
15. G. Kappes, A. Hatzieleftheriou, and S. V. Anastasiadis, "Dike: Virtualization-aware Access Control for Multitenant Filesystems," University of Ioannina, Greece, Technical Report No. DCS2013-1, 2013.
16. Ali, M., Bilal, K., Khan, S., Veeravalli, B., Li, K. and Zomaya, A., 2015. DROPS: division and replication of data in the cloud for optimal performance and security. IEEE Transactions on Cloud computing., pp.1-15.
17. W. Zhang and Y. Liu, "Reactive power optimization based on PSO in a practical power system," in Proceedings of the IEEE Power Engineering Society General Meeting, pp. 239–243, 2004.
18. N. K. Sharma, D. SureshBabu, and S. C. Choube, "Application of particle swarm optimization technique for reactive power optimization," Proceedings of the International Conference on Advances in Engineering, Science and Management (ICAESM '12), pp. 88–93, IEEE, Nagapattinam, India, 2012.
19. W. Zhang and Y. T. Liu, "Multi-objective reactive power and voltage control based on fuzzy optimization strategy and fuzzy adaptive particle swarm," International Journal of Electrical Power and Energy Systems, vol. 30, no. 9, pp. 525–532, 2008.
20. S. Cheng and M.-Y. Chen, "Multi-objective reactive power optimization strategy for distribution system with penetration of distributed generation," International Journal of Electrical Power and Energy Systems, vol. 62, pp. 221–228, 2014.
21. Q. Liu and J. Yue, "An improved mind evolutionary algorithm for reactive power optimization," in Proceedings of the 32nd Chinese Control Conference (CCC '13), pp. 8048–8051, Xi'an, China, 2013.
22. K. Bilal, S. U. Khan, L. Zhang, H. Li, K. Hayat, S. A. Madani, N. Min-Allah, L. Wang, D. Chen, M. Iqbal, C. Z. Xu, and A. Y. Zomaya, "Quantitative comparisons of the state of the art data center architectures," Concurrency and Computation: Practice and Experience, Vol. 25, No. 12, 2013, pp. 1771-1783.
23. K. Bilal, M. Manzano, S. U. Khan, E. Calle, K. Li, and A. Zomaya, "On the characterization of the structural robustness of data center networks," IEEE Transactions on Cloud Computing, Vol. 1, No. 1, 2013, pp. 64-77

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details