IJARETY

International Journal of Advanced Research in Education and TechnologY (IJARETY)

Volume 11, Issue 6, November-December 2024

Impact Factor: 7.394

www.ijarety.in editor.ijarety@gmail.com

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 7.394| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 11, Issue 6, November-December 2024 ||

DOI:10.15680/IJARETY.2024.1106037

Cloud Split: Enhancing and Security with Data Division and Replication

Mr.Shaikh Mohammed[1], Mr. D.Sai Kumar[2], Mr.D. Sai[3], Mr.G.Chandu[4]

Assistant Professor, Department of CSE, Guru Nanak Institute of Technology, Hyderabad, Telangana, India[1]

Student, Department of CSE, Guru Nanak Institute of Technology, Hyderabad, Telangana, India[2,3,4]

ABSTRACT: Outsourcing data to a third-party administrative control, as is done in cloud computing, gives rise to security concerns. The data compromise may occur due to attacks by other users and nodes within the cloud. Therefore, high security measures are required to protect data within the cloud. However, the employed security strategy must also take into account the optimization of the data retrieval time. In this paper, we propose Division and Replication of Data in the Cloud for Optimal Performance and Security (DROPS) that collectively approaches the security and performance issues. In the DROPS methodology, we divide a file into fragments, and replicate the fragmented data over the cloud nodes. Each of the nodes stores only a single fragment of a particular data file that ensures that even in case of a successful attack, no meaningful information is revealed to the attacker. Moreover, the nodes storing the fragments, are separated with certain distance by means of graph T-coloring to prohibit an attacker of guessing the locations of the fragments. Furthermore, the DROPS methodology does not rely on the traditional cryptographic techniques for the data security; thereby relieving the system of computationally expensive methodologies. We show that the probability to locate and compromise all of the nodes storing the fragments of a single file is extremely low. We also compare the performance of the DROPS methodology with ten other schemes. The higher level of security with slight performance overhead was observed.

I. INTRODUCTION

The cloud computing paradigm has reformed the usage and management of the information technology infrastructure. Cloud computing is characterized by on-demand self-services, ubiquitous network accesses, resource pooling, elasticity, and measured services. The aforementioned characteristics of cloud computing make it a striking candidate for businesses, organizations, and individual users for adoption. However, the benefits of low-cost, negligible management (from a users perspective), and greater flexibility come with increased security concerns. Security is one of the most crucial aspects among those prohibiting the wide-spread adoption of cloud computing. Cloud security issues may stem due to the core technology′ s implementation (virtual machine (VM) escape, session riding, etc.), cloud service offerings (structured query language injection, weak authentication schemes, etc.), and arising from cloud characteristics (data recovery vulnerability, Internet protocol vulnerability, etc.). For a cloud to be secure, all of the participating entities must be secure.

II. LITERATURE SURVEY

Ali, S., & Khan(2023) Data splitting for enhanced security in cloud computing involves dividing sensitive information into smaller, non-sensitive fragments before storage. This technique mitigates the risks associated with data breaches, as individual fragments alone do not reveal meaningful information. By storing these fragments across multiple locations or cloud servers, the approach leverages redundancy while minimizing the chances of unauthorized access to complete datasets. Additionally, data splitting can be combined with encryption to further protect each fragment, ensuring that even if an attacker gains access to one fragment, it remains useless without the others. This method not only bolsters security but also enhances data availability and resilience against server failures. Overall, data splitting is a crucial strategy in modern cloud architectures, addressing both security concerns and compliance with regulations regarding data protection. In practice, data splitting involves several steps. First, sensitive data is identified and then divided into smaller pieces, often through techniques such as sharding or splitting based on predefined criteria (e.g., data type, sensitivity level). Each fragment can be encrypted individually before storage, adding another layer of security. These fragments are then distributed across various cloud servers or storage solutions, often in different geographical locations. This geographic diversification not only helps in complying with regional data protection regulations but also reduces the risk of a single point of failure.

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 7.394| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 11, Issue 6, November-December 2024 ||

DOI:10.15680/IJARETY.2024.1106037

Sinha, A., & Gupta(2023)Distributed data security in cloud computing refers to the practices and technologies employed to protect data that is stored across multiple servers and locations in a cloud environment. As businesses increasingly adopt cloud services, the need for robust security measures becomes paramount, given the unique vulnerabilities associated with distributed architectures. This approach encompasses a variety of techniques aimed at ensuring the confidentiality, integrity, and availability of data, while also addressing the challenges that come with such a decentralized model. One of the most fundamental techniques for securing distributed data is encryption. Data is encrypted both at rest (when stored) and in transit (when being transmitted). Strong encryption algorithms ensure that even if data fragments are intercepted or accessed without authorization, they remain unreadable without the proper decryption keys. Implementing strict access controls is essential for protecting sensitive data in distributed environments. Role-based access control (RBAC) and attribute-based access control (ABAC) can be used to ensure that only authorized users have access to specific data sets, reducing the risk of insider threats and unauthorized access. By dividing data into smaller fragments and storing them across multiple servers, organizations can minimize the risks associated with data breaches. Each fragment can be encrypted separately, and even if an attacker gains access to one fragment, it will not provide complete information.

Patel et. al(2020) As organizations increasingly migrate to cloud computing, the security of data management practices has become a critical concern. The cloud offers numerous advantages, including scalability, cost efficiency, and flexibility, but it also introduces unique challenges related to data security and privacy. This survey explores various secure data management techniques used in cloud computing, highlighting their effectiveness, implementation challenges, and the evolving landscape of cloud security. Data encryption is a cornerstone of secure data management in the cloud. It involves encoding data to prevent unauthorized access. Both symmetric and asymmetric encryption methods are employed to protect data at rest (stored data) and in transit (data being transmitted). Techniques like end-to-end encryption ensure that only authorized users can decrypt and access the data. Robust access control mechanisms are essential for ensuring that only authorized users can access sensitive data. Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), and Identity and Access Management (IAM) are commonly used models. These methods define user roles and permissions, helping to mitigate insider threats and unauthorized access.

EXISTING SYSTEM

- In existing, the security issue is main thing for the users because data compromise may occur due to attacks by other users and nodes within the cloud.
- The data will be loss because of security issues. Therefore, high security measures are required to protect data within the cloud.

Existing System Disadvantages

- No Security authentication.
- Not detect a attackers.
- Data's are not secure.
- No file fragmentation is in existing system.

PROPOSED SYSTEM

We propose Division and Replication of Data in the Cloud for Optimal Performance and Security (DROPS) that collectively approaches the security and performance issues. In the DROPS methodology, we divide a file into fragments, and replicate the fragmented data over the cloud nodes. Each of the nodes stores only a single fragment of a particular data file that ensures that even in case of a successful attack, no meaningful information is revealed to the attacker. Furthermore, the DROPS methodology does not rely on the traditional cryptographic techniques for the data security; thereby relieving the system of computationally expensive methodologies.

PROPOSED SYSTEM ADVANTAGE

➢ The data outsourced to a public cloud must be secured.

➢ The user can detect whether the server is launching attack.

➢ Unauthorized data access by other users and processes (whether accidental or deliberate) must be prevented.

SYSTEM ARCHITECTURE

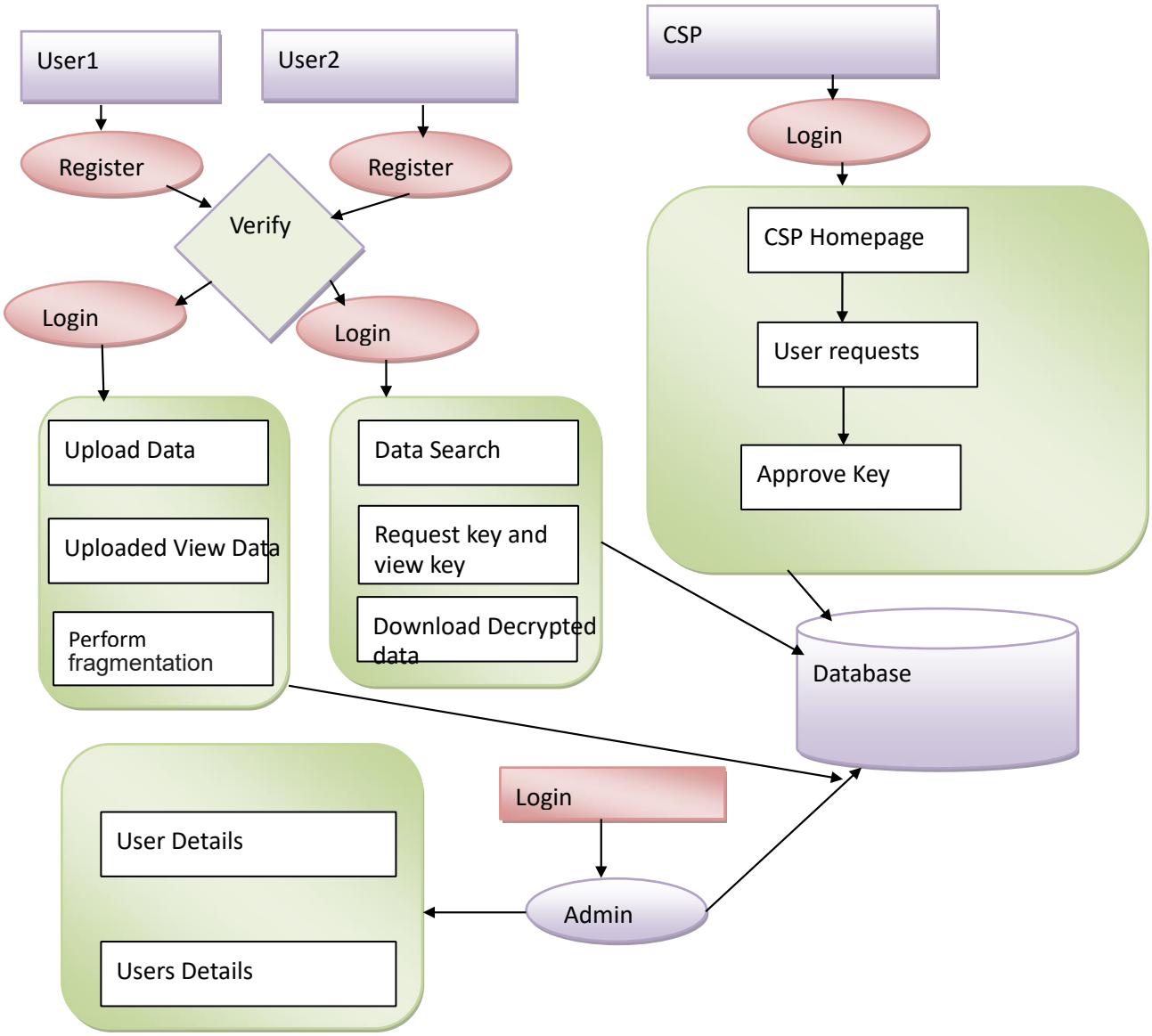
In this project we have a four modules. user has a register with all details. After user Login, user has to upload data and store inside database. User can view his data. While uploading the data , the data it should perform fragmentation that means it should split data into different nodes and store inside server with encryption using SHA algorithm. Create one

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 7.394| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 11, Issue 6, November-December 2024 ||

DOI:10.15680/IJARETY.2024.1106037

more user and that user has to search data. User can access data but he will get encrypted data to decrypt this data he have to take access from csp. CSP has a login with a user id and password. After login it will check user request and generate key to user. After getting the key the user have to decrypt the searched data with this key and he download the data. Here there is another module called as admin, which controls all data. Here we can see user details and file details.



III. METHODOLOGY

Modules Name:

1. User Interface Design

In this module we design the windows for the project. These windows are used for secure login for all users. To connect with server user must give their username and password then only they can able to connect the server. If the user already exits directly can login into the server else user must register their details such as username, password and Email id, into the server. Server will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter a specific page.

2. CSP

The second module is a CSP. First csp has to login with a user id and password. After Login csp home page will be displayed, after this csp will view user request and it will approve keys to user.

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 7.394| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 11, Issue 6, November-December 2024 ||

DOI:10.15680/IJARETY.2024.1106037

3. User
The third module is user has a register and login with a user id and password. user has a uploaded data. We can view a uploaded view data. While uploading the data it will be divided and gets encrypted.

4. Search
The fourth module is a Search. User has a to login and Search data and access data, while accessing data it will show encrypted data for that we have to request for key to decrypt the data. So here csp will approve key to encrypt data for that you have to make request. After making request view key and accessing data.

5. Admin
Cloud has a fifth module. Admin has a login with a user id and password. Admin has a Stored data in the database. Admin controls all this data from database, here admin store every operation of an user. We can see here file details and user details.

PROPOSED ALGORITHM:
Division and Replication of Data in the Cloud for Optimal Performance and Security (DROPS)

ALGORITHM DEFINITION:-
DROPS is a strategy in cloud computing designed to enhance data storage and access. It involves breaking down data into smaller partitions and replicating them across multiple cloud servers or locations. This division and replication ensure redundancy, fault tolerance, and optimal performance. By distributing data, DROPS enables load balancing, reducing latency by serving requests from the closest server. Additionally, it enhances security by safeguarding data with multiple replicas and encryption techniques.

Experimental Results

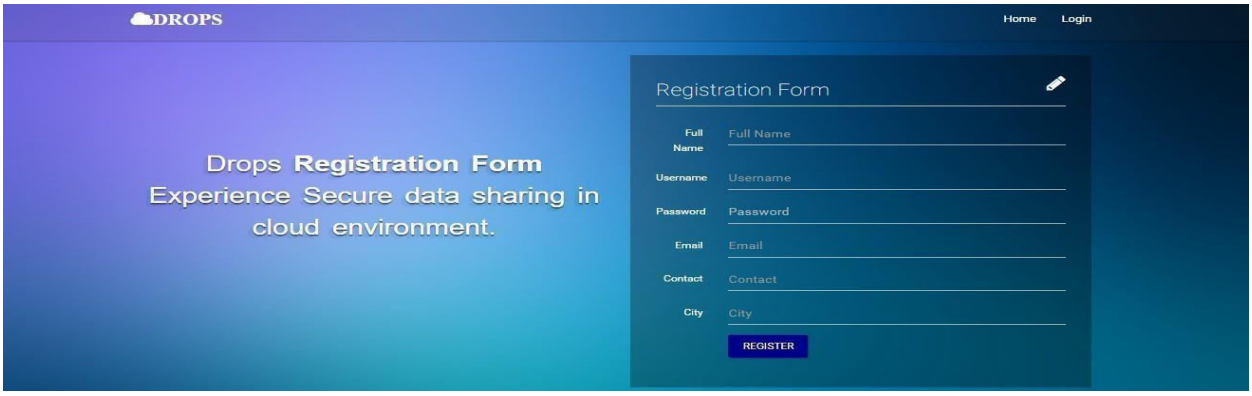


Fig:Registration Form

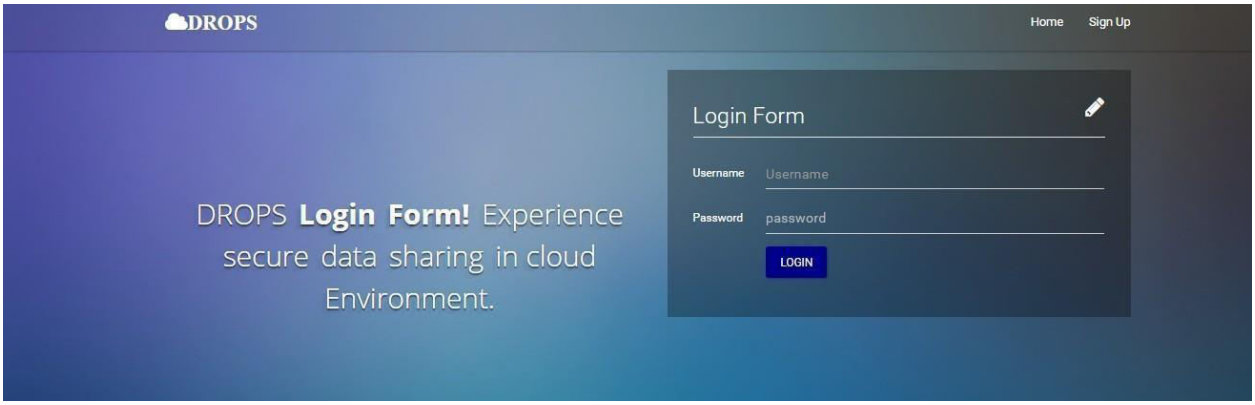


Fig:Login Form

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 7.394| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 11, Issue 6, November-December 2024 ||

DOI:10.15680/IJARETY.2024.1106037

Fig:Home Page

Fig:File Upload Page

Fig:View Request Page

IV. CONCLUSION

We proposed the DROPS methodology, a cloud storage security scheme that collectively deals with the security and performance in terms of retrieval time. The data file was fragmented and the fragments are dispersed over multiple nodes. The nodes were separated by means of Tcoloring. The fragmentation and dispersal ensured that no significant information was obtainable by an adversary in case of a successful attack. No node in the cloud, stored more than a single fragment of the same file. The performance of the DROPS methodology was compared with fullscale replication techniques. The results of the simulations revealed that the simultaneous focus on the security and performance, resulted in increased security level of data accompanied by a slight performance drop.

V. FUTURE ENHANCEMENT

Currently with the DROPS methodology, a user has to download the file, update the contents, and upload it again. It is strategic to develop an automatic update mechanism that can identify and update the required fragments only. The aforesaid future work will save the time and resources utilized in downloading, updating, and uploading the file again. Moreover, the implications of TCP incast over the DROPS methodology need to be studied that is relevant to distributed data storage and access.

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 7.394| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 11, Issue 6, November-December 2024 ||

DOI:10.15680/IJARETY.2024.1106037

REFERENCES

1. 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.
2. 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.
3. 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.
4. Y. Deswarte, L. Blain, and J-C. Fabre, "Intrusion tolerance in distributed computing systems," In Proceedings of IEEE Computer Society Symposium on Research in Security and Privacy, Oakland CA, pp. 110-121, 1991.
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. W. K. Hale, "Frequency assignment: Theory and applications," Proceedings of the IEEE, Vol. 68, No. 12, 1980, pp. 1497-1514.
7. K. Hashizume, D. G. Rosado, E. Fernndez-Medina, and E. B. Fernandez, "An analysis of security issues for cloud computing," Journal of Internet Services and Applications, Vol. 4, No. 1, 2013, pp. 1-13.
8. M. Hogan, F. Liu, A.Sokol, and J. Tong, "NIST cloud computing standards roadmap," NIST Special Publication, July 2011.
9. W. A. Jansen, "Cloud hooks: Security and privacy issues in cloud computing," In 44th Hawaii IEEE International Conference onSystem Sciences (HICSS), 2011, pp. 1-10.
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. 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.
12. L. M. Kaufman, "Data security in the world of cloud computing," IEEE Security and Privacy, Vol. 7, No. 4, 2009, pp. 61-64.
13. S. U. Khan, and I. Ahmad, "Comparison and analysis of ten static heuristics-based Internet data replication techniques," Journal of Parallel and Distributed Computing, Vol. 68, No. 2, 2008, pp. 113-136.
14. A. 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.
15. A. N. Khan, M.L. M. Kiah, S. A. Madani, and M. Ali, "Enhanced dynamic credential generation scheme for protection of user identity in mobile-cloud computing, The Journal of Supercomputing, Vol. 66, No. 3, 2013, pp. 1687-1706 .
16. 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.
17. 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.
18. L. Qiu, V. N. Padmanabhan, and G. M. Voelker, "On the placement of web server replicas," In Proceedings of INFOCOM 2001, Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies, Vol. 3, pp. 1587-1596, 2001.
19. D. Sun, G. Chang, L. Sun, and X. Wang, "Surveying and analyzing security, privacy and trust issues in cloud computing environments," Procedia Engineering, Vol. 15, 2011, pp. 2852 2856.
20. 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, Nov. 2012, pp. 903-916.
21. 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.
22. D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Future Generation Computer Systems, Vol. 28, No. 3, 2012, pp. 583-592.
23. J. J. Wylie, M. Bakkaloglu, V. Pandurangan, M. W. Bigrigg, S. Oguz, K. Tew, C. Williams, G. R. Ganger, and P. K. Khosla, "Selecting the right data distribution scheme for a survivable storage system," Carnegie Mellon University, Technical Report CMU-CS-01-120, May 2001.
24. M. Newman, Networks: An introduction, Oxford University Press, 2009.

International Journal of Advanced Research in Education and Technology

ISSN: 2394-2975 Impact Factor: 7.394

www.ijarety.in editor.ijarety@gmail.com