Description of the architecture

Fig. 1, shows the splitting of data into five meaningless chunks.

Fig. 2, shows how each of the chunks are dispersed to buckets in a cloudlet using dictionary structure. Each chunk is structured in a such a way that it has an identifier known here as key. That is to say when stored in a cloudlet bucket, each share is assigned a unique key common to all the shares made out of a data. Just same way, each file has a name unique to it which helps to save and retrieve it from folders or disk. To retrieve a share, the user simly types the file name, and by so doing the system recalls all the shares made from the file/data/key and recreates it to its former state.

As stated in C above, Secret sharing algorithms are used to split data into meaningless chunks determined by the number of participants involved in the process. In the case of TCloud, we have five cloudlets participating in the process and that determines the number of share made out of every data to be transmitted to cloudlets for hosting, while the number of participants or here cloudlets needed to recreate data at each point is three. Out of the five cloudlets, one is a virtual store, which does not participate in the daily process of data recovery.

In TCloud, every Denial of Service (DoS) experienced during each process is regarded as cloud disaster. In the case of one cloud failure, TCloud will continue to provide data services to its subscribers, but at the failure of second cloudlets, the system triggers an alarm that causes any administrative staff to break the normal working protocol, by logging into the system using his/her emergency login details and this is referred to as a break-glass mechanism. When a break-glass mechanism is used to log into the system, the system automatically opens up access to the virtual store, thereby giving the system access to a third share that will allow it to continue to provide data services to its clients.

When the failed cloudlets are brought back, the failed back procedure follows the normal process of restoration and the ability of the system to work with the magic share in the virtual store makes it possible to have a zero downtime and robust failover protection. At the failback stage, the system performs a self-healing process so as to make sure all failed cloudlets have correct shares in them. The process entails maintaining access to the magic share while trying to access shares from the recoverd cloudlets. Any failed share recovery calls for a recreation of the data using the magic share and thereafter redistributes to all cloudlets, in this case overwrting previously stored shares in every cloudlet buckets.

IV. Conclusions

In current cloud-based disaster recovery systems, the focus has been on faster system recovery after an outage leading to huge losses to businesses and discouragement to prospective cloud subscribers. The need thus arises for research to focus on contending cloud-based interruptions so as to keep system running uninterruptedly as the main focus of disaster recovery subscription by data owners is for data availability for business continuity. The system thus proposed above has been able to provide the gap, proposed a wholistic system, which when fully implemented will be able to bridge the system downtime as the use of secret sharing scheme in data dissemination using the required threshold has proved to be resilient and secured in its all entirety once the issue of latency could be properly handled.

V. References

[1] M. Pokharel, S. Lee, and J. S. Park, 'Disaster recovery for system architecture using cloud computing', in *Applications and the Internet (SAINT), 2010 10th IEEE/IPSJ International Symposium on*, 2010, pp. 304–307.

[2] J. I. Khan and O. Y. Tahboub, 'Peer-to-Peer Enterprise Data Backup over a Ren Cloud', in *Information Technology: New Generations (ITNG), 2011 Eighth International Conference on*, 2011, pp. 959–964.

[3] Z. Jian-Hua and Z. Nan, 'Cloud computing-based data storage and disaster recovery', in *Future Computer Science and Education (ICFCSE), 2011 International Conference on*, 2011, pp. 629–632.

[4] S. R. Patil, R. M. Shiraguppi, B. P. Jain, and S. Eda, 'Methodology for Usage of Emerging Disk to Ameliorate Hybrid Storage Clouds', in *IEEE International Conference on Cloud Computing in Emerging Markets (CCEM)*, 2012, pp. 1–5.

[5] T. Wood, H. A. Lagar-Cavilla, K. K. Ramakrishnan, P. Shenoy, and J. Van der Merwe, 'PipeCloud: using causality to overcome speed-of-light delays in cloud-based disaster recovery', in *Proceedings of the 2nd ACM Symposium on Cloud Computing*, 2011, p. 17.

[6] B. Cully, G. Lefebvre, D. Meyer, M. Feeley, N. Hutchinson, and A. Warfield, 'Remus: High availability via asynchronous virtual machine replication', in *Proceedings of the 5th USENIX Symposium on Networked Systems Design and Implementation*, 2008, pp. 161–174.

[7] S. Rajagopalan, B. Cully, R. O'Connor, and A. Warfield, 'SecondSite: disaster tolerance as a service', in *ACM SIGPLAN Notices*, 2012, vol. 47, pp. 97–108.

[8] A. Shamir, 'How to share a secret', *Commun. ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[9] G. R. Blakely, 'Safeguarding cryptographic keys', in *Proc. AFIPS*, 1979, vol. 48, pp. 313–317.

[10] M. Russ, 'Secret Sharing Schemes PowerPoint PPT Presentation'. 2012.

[11] H. Krawczyk, 'Secret sharing made short', in *Advances in Cryptology—CRYPTO'93*, 1993, pp. 136–146.

[12] Y. Dodis, 'Exposure-resilient cryptography', 2000.

[13] E. Ukwandu, W. J. Buchanan, L. Fan, G. Russell, and O. Lo, 'RESCUE: Resilient Secret Sharing Cloud-Based Architecture', in *Trustcom/BigDataSE/ISPA, 2015 IEEE*, 2015, vol. 1, pp. 872–879.

[14] W. J. Buchanan, D. Lanc, L. Fan, G. Russell, and others, 'The Future Internet: A World of Secret Shares', *Future Internet*, vol. 7, no. 4, pp. 445–464, 2015.

[15] F. Alsolami and T. E. Boult, 'CloudStash: using secret-sharing scheme to secure data, not keys, in multi-clouds', in *Information Technology: New Generations (ITNG), 2014 11th International Conference on*, 2014, pp. 315–320.

[16] B. Fabian, T. Ermakova, and P. Junghanns, 'Collaborative and secure sharing of healthcare data in multi-clouds', *Inf. Syst.*, vol. 48, pp. 132–150, 2015.

[17] T. Ermakova and B. Fabian, 'Secret sharing for health data in multi-provider clouds', in *Business Informatics (CBI), 2013 IEEE 15th Conference on*, 2013, pp. 93–100.

[18] N. Joint, 'COCIR/JIRA Security And Privacy Committee (SPC)', *Break-Glass Approach Grant. Emerg. Access Healthc. Syst.*, 2004.

[19] D. Ghosh, R. Sharman, H. R. Rao, and S. Upadhyaya, 'Self-healing systems—survey and synthesis', *Decis. Support Syst.*, vol. 42, no. 4, pp. 2164–2185, 2007.

[20] M. Nojoumian, D. R. Stinson, and M. Grainger, 'Unconditionally secure social secret sharing scheme', *Inf. Secur. IET*, vol. 4, no. 4, pp. 202–211, 2010.