Mitigating Disaster using Secure Threshold-Cloud Architecture

Elochukwu Ukwandu, William J Buchanan & Gordon Russell
The Cyber Academy, Edinburgh Napier University, Edinburgh. UK
e.ukwandu@napier.ac.uk, w.buchanan@napier.ac.uk, g.russell@napier.ac.uk

Abstract: There are many risks in moving data into public cloud environments, along with an increasing threat around large-scale data leakage during cloud outages. This work aims to apply secret sharing methods as used in cryptography to create shares of cryptographic key, disperse and recover the key when needed in a multi-cloud environment. It also aims to prove that the combination of secret sharing scheme and multi-clouds can be used to provide a new direction in disaster management by using it to mitigate cloud outages rather than current designs of recovery after the outages. Experiments were performed using ten different cloud services providers at share policies of 2 from 5, 3 from 5, 4 from 5, 4 from 10, 6 from 10 and 8 from 10 for which at different times of cloud outages key recovery were still possible and even faster compared to normal situations. All the same, key recovery was impossible when the number of cloud outages exceeded secret sharing defined threshold. To ameliorate this scenario, we opined a resilient system using the concept of self-organisation as proposed by Nojoumian *et al* in 2012 in improving resource availability but with some modifications to the original concept. The proposed architecture is as presented in our Poster: Improving Resilience in Multi-Cloud Architecture.

Keywords—secret shares, disaster mitigation, thresholds scheme, cloud service providers.

I. Introduction

With the introduction of cloud services for disaster management on a scalable rate, there appears to be the needed succour by small business owners to get a cheaper and more secure disaster recovery mechanism so as to provide business continuity and remain competitive with other large businesses. But that is not to be so, as cloud outages became a nightmare. Recent statistics by Ponemon Institute [1] on Cost of Data Centre Outages, shows an increasing rate of 38% from $505,502 in 2010 to $740,357 as at January 2016. Using activity-based costing they were able to capture direct and indirect cost to: Damage to mission-critical data; Impact of downtime on organizational productivity; Damages to equipment and other assets and so on. The statistics were derived from 63 data centres based in the United States of America.

These events may have encouraged the adoption of multi-cloud services so as to divert customers traffic in the event of cloud outage. Some fine-grained proposed solutions on these are focused on Redundancy and Backup such as: Local Backup by [2]; Geographical Redundancy and Backup [3]; The use of Inter-Private Cloud Storage [4]; Resource Management for data recovery in storage clouds [5], and so on. But in all these, cloud service providers see disaster recovery as a way of getting the system back online and making data available after a service disruption, and not on contending disaster by providing robustness that is capable of mitigating shocks and losses resulting from these disasters.

This work aims to apply secret sharing methods as used in cryptography [6], [7] to create shares of cryptographic key, disperse and recover the key when needed in a multi-cloud environment. It also aims to prove that the combination of secret sharing scheme and multi-clouds can be used to provide a new direction in disaster management by using it to mitigate cloud outages rather than current deigns of recovery after the outages. Experiments were performed using ten different cloud services providers for storage services, which at different times of cloud outages, key recovery were still possible and even faster compared to normal situations. All the same, key recovery was impossible when the number of cloud outages exceeded secret sharing defined threshold. To ameliorate this scenario, we look forward to employ the concept of self-organisation as proposed by Nojoumian *et al* [8] in improving resource availability but with some modifications as proposed.

The rest of the work is organised into section II, Literature Review takes a closer look at current practices, use of secret sharing and cloud-based disaster recovery with much interest in the method used in design. III. Presents our approach, in section IV, present Results and Evaluations and Conclude in section V with future works and lessons learnt.

II. Literature Review

There are research solutions based on different variants of secret sharing schemes and multi-cloud architecture that give credence to its resilience in the face of failures, data security in keyless manner, such as: Ukwandu *et al*, [9] - RESCUE: Resilient Secret Sharing Cloud-based Architecture; Alsolami & Boult, [10], - CloudStash: Using Secret-Sharing Scheme to Secure Data, Not Keys, in Multi-Clouds. Others are: Fabian *et al,* [11] on Collaborative and secure sharing of healthcare data in multi-clouds and [12] on Secret Sharing for Health Data in Multi-Provider Clouds. While RESCUE provided an architecture for a resilient cloud-based storage with keyless data security capabilities using secret sharing scheme for data splitting, storage and recovery, CloudStash also relied on the above strengths to prove security of data using secret sharing schemes in a multi-cloud environment and Fabian *et al* proved resilience and robust sharing in the use of secret sharing scheme in a multi-cloud environment for data sharing.

Because our approach is combining secret sharing and multi-clouds in developing a cloud-disaster management the need therefore arise to review current method used in cloud-based disaster in a multi-cloud system and their shortcomings.

- **Remus:** Cully *et al* [13] described a system that provides software resilience in the face of hardware failure (VMs) in such a manner that an active system at such a time can continue execution on an alternative physical host while preserving the host configurations by using speculative execution. The strength lies on the preservation of system's software independently during hardware failure.
- **SecondSite**: As proposed by Rajagopalan *et al* [14] is built to extend the Remus high-availability system based on virtualization infrastructure by allowing very large VMs to be replicated across many data centres over the networks using internet. One main aim of this solution is to increase the availability of VMs across networks. Like every other DR systems discussed above, SecondSite is not focused on contending downtime and security of data during cloud outages.
- **DR**-Cloud – Yu *et al* [15] relied on data backup and restore technology to build a system proposed to provide high data reliability, low backup cost and short recovery time using multiple optimisation scheduling as strategies. The system is built of multi-cloud architecture using Cumulus [16] as cloud storage interface. Thus providing the need for further studies on the elimination of system downtime during disaster, provide consistent data availability as there is no provision for such in this work.

III. Our Approach

Our approach is in combining secret sharing scheme with multi-clouds to achieve resilience with the aim of applying same in redefining cloud-based disaster management from recovery from cloud outages to mitigating cloud outages.

A. The architecture

The architecture of as shown in Figure 1 shows key share creation, dispersal and storage, while that of Figure 2 is of shares retrieval and key recovery.

Share creation and Secret recovery.

The diagram above explains our design of key share creation, dispersal and storage using different cloud service providers.

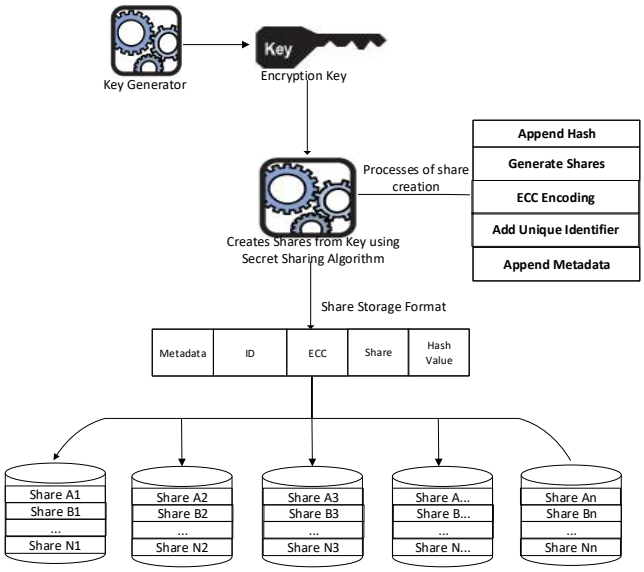

Figure 1: Key Share Creation, Dispersal and Storage

Share Creation: The dealer determines the number of hosts shares combination from which data recovery is possible known as threshold *(t)* and the degree of the polynomial, drived from subtracting 1 from the threshold. In this case, the threshold is 3 and the degree of polynomial is 2. He initiates a secret sharing scheme by generating the polynomial $f(x) = ax^2 + bx + c$, the coefficients *a* and *b* are random values and *c* is the secret, the constant term of the polynomial as well as the intercept of the graph. He generates 5 shares for all the hosts $H_1 \ldots H_5$ and sends the shares to them for $1 \leq i \leq n$ in an equal ratio and weights w_i, and thereafter leaves the scene.

$$\varphi_{ij} = f(\vartheta_{ij}) \qquad [1]$$

Secret Recovery

Just as in Shamir [6] authorised participants following earlier stated rules are able to recover the secret using Lagrangian interpolation once the condition $\sum_{p_i \in \Delta} w_i \geq t$ as stated earlier is met. The participants $P_i \in \Delta$ contribute their shares $\vartheta_{ij} for\ 1 \leq j \leq w_i$ to recover the secret $f(0) = k$.

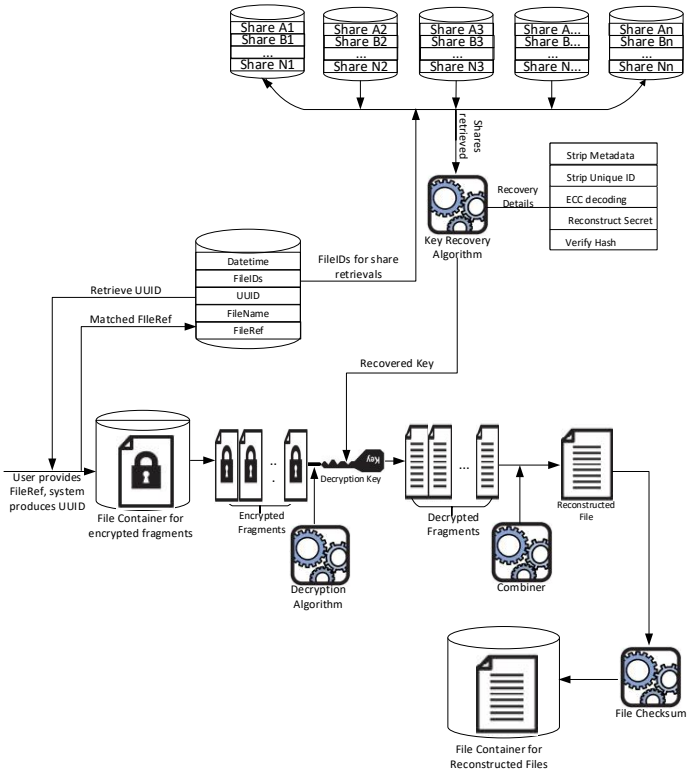

Figure 2: Share Retrievals and Key Recovery

IV. RESULTS AND EVALUATIONS

Test: Cloud Outages against Normal situations.

This test assumes that cloud outage prevents secret recovery.

Table 1: Cloud Outages and Normal Situations

KeyShaFileSize	Key Recovery (Sec)	% Difference (Sec)
1KB, 3 from 5,	7.80	1.28/16.41% 20% failure
1KB, 3 from 5, 1 down	6.52	
10KB, 3 from 5	7.76	4.02/51.80% 40% failure
10KB, 3 from 5, 2 down	3.74	
1KB, 6 from 10	25.67	9.73/37.90% 30% failure
1KB, 6 from 10, 3 down	15.94	
10KB, 6 from 10	25.33	10.89/42.99% 40% failure
10KB, 6 from 10, 4 down	14.44	

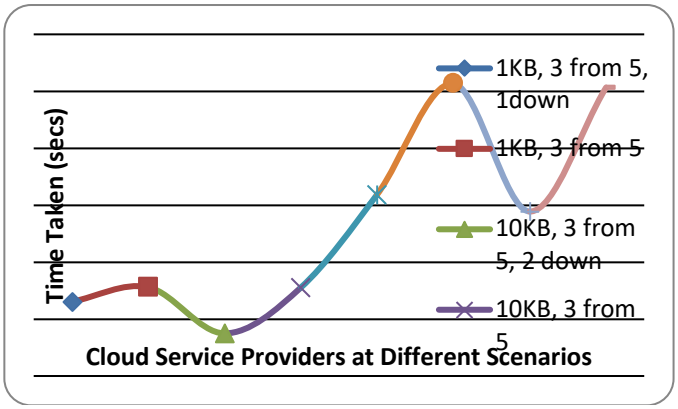

Figure 3: Cloud Service Providers at Different Scenarios

Discussions:

The results above show that cloud outage has no negative effect on key recovery, rather reduces the overhead in comparison with normal situations. It shows the relationship between cloud outage and normal operational conditions. From available results at twenty percent (20%) failure rate using 3 from 5 share policy, the system becomes faster by sixteen percent (16.41%), but at forty percent (40%) failure rate using same share policy, the download speed is faster by a little above fifty one percent (51.80%). Taking a look at a higher share policy of 6 from 10, at thirty percent (30%) failure rate, the system download speed is higher by a little above thirty-seven percent (37.90%), while at forty percent (40%) failure rate, the system performed better by about forty-three percent (42.99%). The implications therefore are that in as much as failure rate is not equivalent or above the threshold, system performance improves as there was no result obtained when the cloud outage exceeds or equal to threshold. These therefore do not support the assumption as above that cloud outage has negative effect in key recovery. There is no significant evidence to show that the size of the share has effect on the key recovery during cloud outages because at forty percent (40%) failure rate using share of 10KB in 3 from 5 shows performance rate of above fifty-one percent while in 6 from 10 share policy approximately forty-three (42.99%) percent performance rate.

V. Conclusions, Lessons Learnt and Future Work

Current cloud-based disaster recovery systems have focused on faster recovery after an outage and the underlying issue has been the method applied, which centred in data backup and replicating the backed-up data to several hosts. This method has proved some major delays in providing a strong failover protection as there has to be a switch from one end to another during disaster in order to bring systems back online, the need thus arises for research to focus on method capable of mitigating this interruptions by providing strong failover protection as well as stability during adverse failures so as to keep systems running. This method we have provided here using this paper. Because, secret sharing schemes are keyless method of encryption, data at rest and in transit are safe as it exists in meaningless format. The recovery of key is done using system memory and share verification is usually carried out using an inbuilt share checksum mechanisms using SHA-512, which validates shares before recovery. Else, share recovery returns error and halts.

We have learnt that cloud outage rather than prevent key recovery, using our method proved that it hastens key recovery from results available. Also, understand that when cloud outage exceeds threshold of the share policy, key recovery becomes impossible and to ameliorate this situation, we propose as future work to use the concept of Self-Organisation as proposed by Nojoumian *et al* in [8] to manage cloud resources though with some modifications so as to maintain share availability from cloud service providers.

VI. References

[1]K. Bill, 'New Study: Cost of Data Center Outages – 2016', 08-Feb-2016. .

[2]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.

[3]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.

[4]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.

[5]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.

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

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

[8]M. Nojoumian and D. R. Stinson, 'Social secret sharing in cloud computing using a new trust function', in *Privacy, Security and Trust (PST), 2012 Tenth Annual International Conference on*, 2012, pp. 161–167.

[9]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.

[10]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.
[11]F. Fabian and B. Fabian, ‘Collaborative and secure sharing of healthcare data in multi-clouds’, *Inf. Syst.*, vol. 48, pp. 132–150, 201503.
[12]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.
[13]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.
[14]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.
[15]Y. Gu, D. Wang, and C. Liu, ‘DR-Cloud: Multi-cloud based disaster recovery service’, *Tsinghua Sci. Technol.*, vol. 19, no. 1, pp. 13–23, 2014.
[16]M. Vrable, S. Savage, and G. M. Voelker, ‘Cumulus: Filesystem backup to the cloud’, *ACM Trans. Storage TOS*, vol. 5, no. 4, p. 14, 2009.