Journal of Information Assurance and Security.
ISSN 1554-1010 Volume 10 (2015) pp. 200-208

Efficient and secured data partitioning in the multi cloud environment

Hazila Hasan[1], Suriayati Chuprat[2]

[1] Department of Information Technology and Communication,
Politeknik Sultan Abdul Halim Muadzam Shah, Kedah, Malaysia
hazi1981@polimas.edu.my

[2] Advanced Informatics School (AIS),
Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia
suriayati.kl@utm.my

***Abstract*: Data security and privacy have become the biggest problem in cloud computing and could be solved by adopting data partitioning in the multi cloud environment. Nevertheless, pure data partitioning faces security problems caused by cloud's storage blockage or service outage. Therefore, many researchers have moved and conducted their research on secured data partitioning. However, a little attention is given towards unification of data partitioning process with the security aspect. Most of the researches are more focused on one aspect and have neglected the other one. This leads to insufficient efficiency on data partitioning performance and the security being proposed. Thus, this paper intends to propose efficient and secured data partitioning of multi cloud environment. To achieve this objective, this paper has presented an extensive discussion related to the concept of data partitioning and related works on efficient and secured data partitioning of multi cloud. Lastly, we have proposed an enhanced technique for efficient and secured data partitioning of multi cloud environment.**

***Keywords*:** cloud computing, multi cloud, data security, data privacy, data partitioning, efficient.

I. Introduction

Cloud computing is defined as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [1]. It becomes prevalent in the current age as it possesses unique characteristics such as on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service [1]. In cloud computing there are four models that can be deployed which are private cloud, public cloud, community cloud and hybrid cloud [2, 3]. It also comes in 3 different delivery models which are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) [4].

The users are able to choose the model that is suitable and convenient with their organization and task. These characteristics and models have become a pleasant package to the users and service providers. However the users are still concerned on the reliability and availability of using a single cloud. This concern is due to the fear that a single cloud may not fulfill all users' needs because of its limitation and it might fail to provide its services if it is broken down or during a service outage. In addition, using a single cloud has also exposed to data security and privacy concerns. The concerns related to data security and privacy are being discussed in section II.

II. Data security and privacy in cloud computing

Data security and privacy are being constantly debated as the biggest concern in cloud computing. The reasons for this concern are due to rising of various attacks [5], threats and related issues in cloud computing especially in a solo cloud. According to Roberts II and Al-Hamdani [6], among the potential attacks that can occur or have occurred in cloud computing are wrapper attack in XML signature, phishing, denial of service attack and reputation file sharing caused by multi-tenancy. In addition, Jamsa [7] has discussed a few more potential attacks in cloud computing, namely packet sniffing attacks, man-in-the-middle attack and hypervisor attack. The detail explanation on each attack is mentioned below:

- XML Signature – This attack can occur when the hacker injected illegal code to react as a valid XML signature. The illegal code will be used to perform illegal tasks.
- Browser security – The security of web browser in the cloud is vulnerable towards phishing although it is occupied with Transport Layer Security (TLS). Once phishing has successfully gained the user's password, TLS will not be able to protect the users anymore.
- Flooding – This issue is caused by Denial of Service (DOS) attacks. This attack happened when an infected computer is used to send continues request of service to the servers. The servers will become too busy to handle the requests and thus the genuine request might be neglected and the

server will not perform its task efficiently or stop responding after the attack.

- Reputation Fate Sharing – The use of shared hardware or software to do illegal activities. This can occur if the valid user does not apply a security measure, such as logging out after using the shared hardware or software. Once the hardware or software was suspected to be used for illegal activities, all the people used the shared hardware or software will be the prime suspect.
- Packet sniffing attack - The attacker launches line of codes to examine the packets that travel in the cloud network. The codes known as packet sniffer program will allow the attacker to view and sometimes change the contents of the packet. A wireless network is vulnerable to this type of attack.
- Man-in-the-middle attack – The attacker places himself between the legal user and the cloud system by intercepting the valid communication message between them. Once he placed himself, he then will be able to send and request message and can pretend to be either valid user or the cloud system.
- Hypervisor attack – Through virtualization of cloud server, the operating system of the server will be running on top of the virtualization software. Therefore, the attacker will constantly try to hijack that virtualization software.

The mentioned attacks are not just perceived but they are real. A few cases have been reported by authors such as Kim [8] and AlZain et al. [9]. These attacks undoubtedly can cause breaches towards data security and privacy.

In addition, there are threats which give bad influence towards data security and privacy in cloud computing. The threats are data intrusion [10], malicious insiders [11], [12], data loss or leakage and others [12]. For example, the incident happened in 2009 with Google Docs [13] has caused unauthorized access to confidential data due to a technical glitch. Therefore, the above mentioned threats must be taken into serious precautions so that it can be prevented from happening again.

Lastly, related issue concerning cloud availability is presented by [8], [9], [14]. This issue, which directly concerns on the unavailability of resources and services in cloud computing could happen due to cloud service provider's breakdown or service outage. It can cause distraction to the users' activities and also can lead to data lost. There are incidents happened reported by authors [8], [9] which have proved that service failure are not an unusual situation for cloud service providers. Table 1 shows the service outage that happened to different cloud service providers [15].

Vendor	Service and outage	Outage Duration
Microsoft	Malfunction in Windows Azure	22 hours
Google	• Gmail and Google Apps • Google search outage due to programming error • Gmail site unavailable due to outage in contacts system • Google App engine partial outage	2.5 hours 40 mins 1.5 hours 5 hours
Amazon	• Authentication overload • Single bit error leading to protocol blowup	1 hours 6-8 hours
Flexiscale	Core network failure	18 hours

Table 1. Service outage occurrences [15].

To address the problems as previously mentioned, researchers have proposed the use of virtual private network, encryption and multi cloud as the solution. Virtual private network are benefits to handle illegal communication interception, but it does not work when it involves malicious insiders.

Applying the encryption method as proposed by [16] [17] is useful because data that are compromised cannot be retrieved and restored if the person does not have the knowledge of the encryption key. However, encryption does not protect the data from being deleted and also from malicious insiders. Malicious insider is the internal threat which is the most dangerous and difficult threat, even though security solution such as passwords and encryption are implemented. This is because malicious insiders have more opportunity to obtain passwords and encrypted key without being noticed.

Since virtual private network and encryption method have their limitations, this research will later focus on multi cloud as one solution towards protecting data security and privacy. Extensive discussion on multi cloud will be presented in the next section.

III. Multi cloud environment

According to Vukolic [18], multi cloud is similar to the terms "interclouds" or "cloud-of-clouds". It is an environment that offers several clouds as illustrated in figure 1. Each cloud has its own power of computation, storage and framework, and performs tasks independently to the other clouds. Multi cloud is known to provide the users with benefits such as being able to divide and share the data/ information; fast access on the infrastructures, applications and services from different cloud providers without the need to worry if one fails to provide its services.

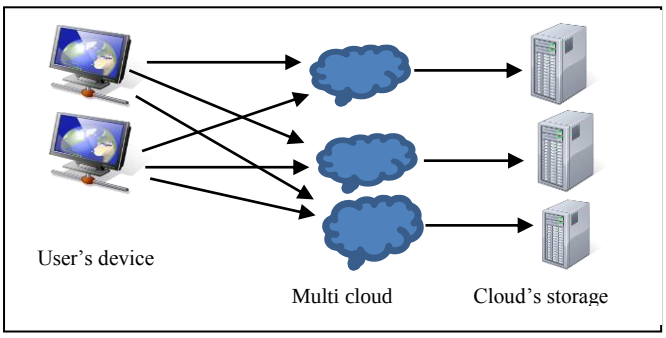

Figure 1. Example of multi cloud environment

The reasons of shifting to multi cloud are various such as for resource and service utilization, costs and service's quality and many others as mentioned in [19]. Adopting multi cloud is also believed to be useful to protect the user's data, promote the user's privacy and maximize cloud's service efficiency through data partitioning. Therefore, in the next sections we will study and analyze the concept of data partitioning, current state of data partitioning in multi cloud and the concepts of efficient and secured data partitioning. Our proposed work will also be presented in the next section.

IV. Concept of data partitioning in multi cloud

A. Processes in data partitioning

The following terms are being used in this paper to describe the processes related to data partitioning. There are:

- Data Separation [20] – this is the process of dividing the data into two or more chunks. This process happens in the user's local machine. During this process, the criteria such as security and size of data are usually being considered. Figure 2 shows the process involved.
- Data Distribution [20] – the process of allocating different data chunks into different clouds through a network. In this process the key factors, e.g.: cost and cloud's quality of services will determine how data chunks will be allocated. Figure 2 shows the process involved.

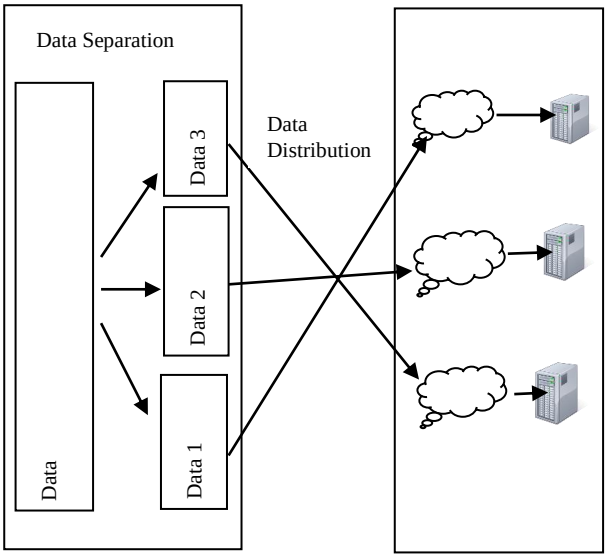

Figure 2. The process of data separation and data distribution

- Data updating [21] – The process of updating the data that only occur if there are any changes in the data.
- Data Retrieval [21] – data retrieval is the reverse process of data distribution and data separation. It's also known as data reconstruction. During data retrieval, security issue regarding cloud's blockage or outage has become the main concern.

V. Data partitioning in multi cloud

In this section, the current state of data partitioning in multi cloud is being explored. The analysis will be done based on researcher's motivation.

Researchers adopted the data partition for several reasons. For example, research done in [22] that is primarily to integrate mobile healthcare with multi cloud's environment has proposed data partitioning in order to increase efficiency of data processing and to save energy cost [22], [23].

Based on similar motivation, Lee et al. [23] are motivated to adopt data partitioning in multi cloud to process big RDF Data. They have proposed a partitioning technique called SPA to increase the efficiency in partitioning big RDF graph data.
Research conducted by Zhao and Wang [21] is mainly due to the factor of maximizing cloud storage resources. In the research, data will be separated into chunks or fragment based on the user's preference. Once the fragments are created, metadata information known as fragment table that consist of fragment id, cloud id, username, password, partition attribute and vector interval are stored in the user's local computer. This table is created purposely to keep track of each fragment and its dedicated cloud storage. After that, the fragmented data will be allocated into different cloud storage based on the query generated. The problem with the query is that, not all queries fit with this model and data partitioning might be skewed if the improper partitioning vector is used. Lastly, during the experimental analysis, the authors have mentioned that the increasing number of fragments will reduce the performance in terms of the space and time of cloud storage. In the paper, the authors have also proposed data replication in order to ensure data availability.

In [24], the authors are focusing on a model to assist decision making during data distribution based on user's budget. The prime result of this model is the minimization of costs needed to be paid to the clouds' provider. This however has put aside other factors that may be critical and prioritized by some users or organization such as performance of service providers, the amount of time data will be stored, security component provided, the ease of use of cloud services and many other user's requirements. In this model, the size of data to be divided into the clouds is at the user's discretion. Therefore, without a proper method to be used, data division will become burdensome for some users. In addition, the absence of updating methods in this model has made the model to be incomplete for the real environment

Other researchers such as in [20], [25], [26] have focused on security reason for adopting data partitioning. They have conducted their research with the aim to ensure data confidentiality [20], [25], [26], [28] and data availability [25]-[27]. The previously mentioned researches [21], [24]

have also integrated security in their proposed works. The detail description of these researches will be explored in the next section.

Table 2 shows the summary of data partitioning in multi cloud based on the motivations and the processes involved.

Ref	Motivation	Data partitioning process			
		Data separation	Data distribution	Data updating	Data retrieval
[20]	Data confidentiality	Yes	Yes	No	No
[21]	Maximize cloud storage resources and data availability	Yes	Yes	Yes	Yes
[22]	Increase efficiency of data processing and save energy cost	Yes	Yes	No	No
[23]	Increase efficiency of data processing and save energy cost	Yes	Yes	No	No
[24]	Minimize the cost and data availability	Yes	Yes	No	Yes
[25]	Data confidentiality and data availability	Yes	Yes	No	Yes
[26]	Data availability	Yes	Yes	No	Yes
[27]	Data availability	No	No	Yes	Yes
[28]	Data confidentiality	Yes	No	No	No

Table 2. Summary of data partitioning in multi cloud.

Table 2 shows the researchers' motivation in adopting data partitioning for the multi cloud environment. Researchers in [22] and [23] have conducted their research with the purpose of increasing efficiency in data processing and saving the energy cost by adopting data partitioning. In their paper, the researchers have explained the process of data separation and distribution that are being conducted in their research.

However, researches done in [20], [21], [24], [25]-[27] and [28] are focusing to increase data security and privacy through the use of data partitioning. The researchers are aimed to protect data confidentiality [20], [25], [27], [28] and ensure data availability [21], [24], [25]-[27]. To protect data confidentiality, researchers in [20] have proposed a new technique called picture shredder which combines image analysis, data separation and data distribution. The process of data updating and data retrieval are not being explored by them. On the other hand, researches conducted in [25] and [26] have included all the processes except data updating. In [27] the authors have only covered the process of data updating and data retrieval. The other processes are not being explored.

Besides the main motivation to maximize cloud storage resources and minimize the cost, the authors in [21] and [24] have also aimed to strengthen data security by ensuring data availability during data retrieval. The authors have adopted security technique in the related process.

Based on the listed motivation, the researches which applied the techniques to any of the data partitioning process and applied security technique to protect data security and privacy will be further analyzed. We will explore the concept of efficient and secured data partitioning in the next section.

VI. Efficient and secured data partitioning in the multi cloud environment

This section will analyze and compare different techniques that have been adopted by the researchers to enhance the efficiency of the data partitioning process and also the techniques adopted for ensuring data security and privacy.

A. Secure Picture Data partitioning

Research done by Leistikow and Tavangarian [20] have explored data partitioning to secure picture sharing in the cloud. They proposed secured techniques called picture shredder which consist of image analysis, data separation and data distribution. The technique used facial recognition and stripping algorithm. Firstly, the image that is captured will be analyzed and sensitive information were identified. Secondly, images will be separated into two separate data (sensitive information and non-sensitive information). Finally, sensitive information will be distributed to Private Cloud and non-sensitive information will be distributed to the Public Cloud. Figure 3 shows the process involved [20].

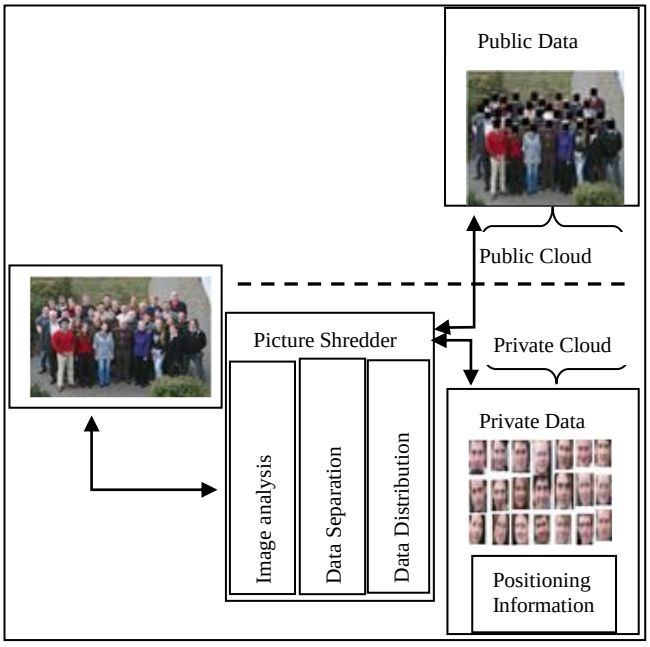

Figure 3. Secure picture data partitioning in multi cloud [20]

B. Data replication data re-partition

Zhao and Wang [21] have implemented the algorithms for all data partitioning process and proposed a model that allows each data chunk/fragment to be replicated and stored in the other cloud storage in order to ensure twenty four hours (24) availability of data during the data retrieval process. This model was introduced to prevent data cloud's server blockage or server failure. However, according to Ye et al. [27] data replication was a difficult approach, especially when it involves data updating. Furthermore, data replication has also required more storage space and increase processing time if big data involves. The process of data replication is shown in figure 4.

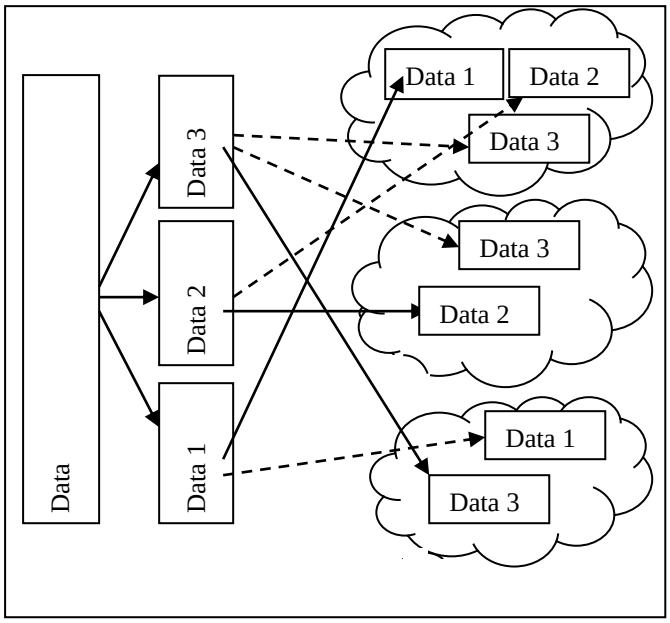

Figure 4. A chunk of data has multiple copies in different cloud

The model has also included data re-partition for data updating. Data updating will occur when the size of each chunk has grown. Nevertheless, the authors mentioned that "re-partition may lead to the division skew, which will lower efficiency of traversal query".

C. Data Availability by using Shamir's Secret Sharing

The research conducted by Singh et al. [24], has implemented data separation and data distribution process through considering the cost and quality of service offered by each cloud service provider. For data retrieval, they have considered the problems of denial of service due to cloud service provider failure or security threats. In data partitioning, if one or more cloud storage failed to provide its service, the stored data cannot be reconstructed. Hence, denial of service may occur. Therefore, the authors have adopted a Shamir's secret sharing technique [29] in their model to ensure data availability during data retrieval. According to the authors, the adoption of the technique has allowed "at least q number of cloud service providers out of p number of service providers must take part to ensure a successful data retrieval". Figure 5 shows the technique that is being used.

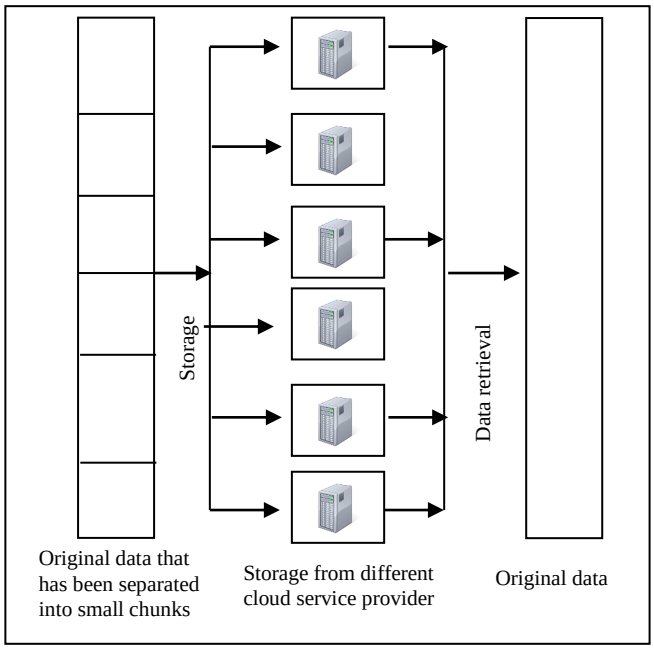

Figure 5. Data retrieval using Shamir's Secret Sharing

In this paper, the experiment that has been conducted to evaluate the technique has shown a successful result. However, during the experiment, data storage for service providers that have low quality of services have been treated as the failed service providers and will not be used during data retrieval. Thus, this does not reflect the real situation that might actually happen. Denial of service attack might occur in any cloud's storage and thus mapping of quality of services with service failure is considered as not accurate.

D. Data Encoding and Data Availability

In paper [25], the authors discussed the concept of encoding techniques to enhance data security of data before they are being distributed over different cloud storage. Firstly, the data was divided into small chunks by adopting information dispersal algorithm. By using the algorithm, the chunks will then be encoded into encoded symbols before they are stored in the multiple cloud storage. Once the data have been encoded, they will be stored in different clouds. To ensure the secrecy of data distribution, the authors have applied erasure coding techniques. To reconstruct the data, data that have been stored will be retrieved from the clouds. The retrieved data will then be decoded to get their original symbol. Lastly, the data will be combined to be the original file. This paper is definitely focusing on security aspects and none of the evaluation is conducted on the data partitioning process performance.

In the data retrieval process, the same technique as implemented in [24], [29] was being used. The technique is prevalent since it does not require data to be retrieved from all cloud's storage, parts of the storage are sufficient to be used to reconstruct the data into its original form. However, according to Jonathan and Chinya [30] this scheme is not practical for real environment unless the users can determine the number of servers that can collude. Figure 6 shows the scheme proposed by the authors.

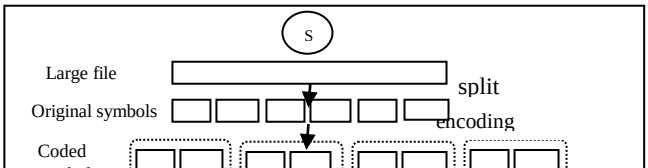

Figure 6. Data partitioning in the multi cloud with data encoding [25]

E. Data Replication and parallel queries

Research in [26] focused on ensuring data availability. This research proposed a model that takes advantage of partition-based cloud data storage. The researchers have come out with queries to communicate with clouds. It contains three processes of data partitioning which are data separation, data distribution and data retrieval. The data update method has yet to be explored further. Security technique solely implemented at the data retrieval process which is used to guarantee data availability. Data fragment has a master replication and the other clouds may store several different replications. This technique is the same technique applied in [21]. Thus, the same weaknesses as mentioned in [21] do exist in this model.

F. Data Updating using lazy updates

This research [27] has been implemented to address the problems of data updating using lazy updates and consistency of verification in data partitioning. First, the storage servers were divided into server groups based on their location information. Within each group, the authors have applied short secret sharing to each data object and distribute the shares to servers in the group. Then the data shares are replicated to different groups.

In this approach, lazy update can be applied by updating shares only in one group and propagating the updates to other groups. Also, the consistent share verification can be performed within each group independently. Thus, according to the authors "the involved of server-to-server communications can be constrained within the group and the cost can be significantly reduced". However, the lazy updates technique which used lazy-group replication can perform well when it involves few clouds with simple transactions, but may become unstable if the system scales up [31].

G. Vertical data partitioning algorithm

This model [28] has adopted vertical data partitioning algorithm to aid the separation process. The vertical partitioning algorithm works by dividing the data into different fractions by splitting the columns or attributes of the database. According to [32], a simple vertical data partitioning algorithm is not suitable for sensitive data. Therefore, the authors have adopted an encryption technique in their proposed model. However, the encryption technique is only useful for protecting data confidentiality. Data integrity and data availability are not being protected. Table 3 below shows the summary of the related works.

Related work	The technique applied to data partitioning process/increase the performance:				The security technique adopted to ensure:			
	Data separation	Data distribution	Data updating	Data retrieval	Confidentiality /Privacy	Integrity	Availability	Authenticity
[20]	Shredding algorithm	Distribute between public and private cloud	×	×	√	×	×	×
[21]	Horizontal algorithm (Range method)	Data storing algorithm	Data fragment update and re-partition algorithm	Data query and connection algorithm and data replication	×	×	√	×
[24]	Algorithm based on rules (cost and Qos)	Algorithm based on rules (cost and Qos)	×	Shamir Secret Sharing	×	×	√	×
[25]	Information Dispersal algorithm	Erasure coding technique	×	Shamir Secret Sharing	√	×	√	×
[26]	Horizontal algorithm (Range method)	Data storing algorithm	×	Data query and integration algorithm and data replication	×	×	√	×
[27]	×	×	Lazy updates	Data replication	√	×	√	×
[28]	Vertical algorithm	×	×	×	√	×	×	√
Proposed technique	Information Dispersal algorithm	CEC algorithm	×	Proactive secret sharing	√	√	√	√

Table 3. Summary of related works.

Table 3 summarizes the techniques adopted to perform or to increase the performance of the data partitioning process and the security techniques that are used to ensure data confidentiality, integrity or availability.

From the related works, it is found that a little attention is given to enhance and evaluate data partitioning process performance. Therefore, this leads to insufficient efficiency of the data partitioning process.

Besides that, most of the researchers do not adopt any security techniques for data integrity. Without a proper verification of data integrity, the integrity of data might not be preserved.

On the other hand, the process of data retrieval for ensuring data availability has caught a great attention from the researchers. Most of the researchers [21], [24]-[27] have explored and proposed security technique for this process. This is due to the reason of solving the problem related to cloud storage's blockage and service outage. However, the proposed techniques have limitation such as not practical for adoption, require big storage size and increase the processing time if data is large.

VII. Proposed work

Figure 6 and figure 7 present the proposed technique of our work.

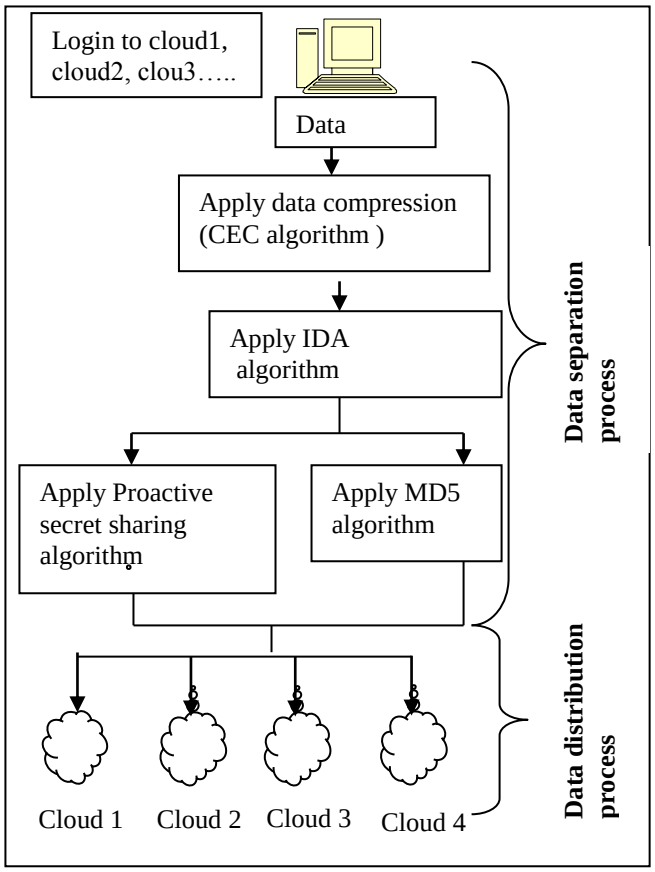

Figure 6. The proposed technique for data separation and data distribution process

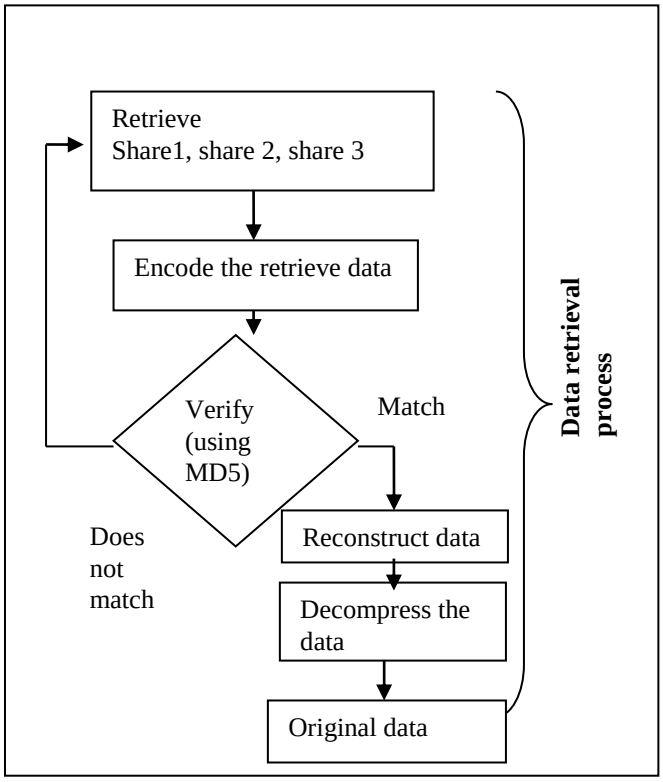

Figure 7. The proposed technique for data retrieval process

In this section, we have proposed an efficient and secured data partitioning technique. This technique is being proposed to achieve efficiency of the data partitioning process and at the same time to protect data security and privacy. Therefore, we have proposed a data compression algorithm to compress the data to make it smaller for efficiency in terms of data size, speed and cost during data distribution. For data separation, we have adopted IDA algorithm because this algorithm is effective to split the data into smaller sizes.

In the data retrieval process, proactive secret sharing is being used because by using this technique, data can be reconstructed without the need to access all cloud storages that have stored the data. Only a few parts of the cloud storage that stored the data are required to retrieve the data. This technique is the extension of Shamir secret sharing techniques and it is different in terms of the flexibility to renew the shares that are stored in the cloud storage. The renewal process can be done weekly, monthly or yearly based on user's discretion. For the security purposes, proactive secret sharing is able to ensure the availability of the stored data even though there is a cloud storage failure case. Besides that, the combination of IDA algorithm and proactive secret sharing are useful to ensure data confidentiality. In addition, the adoption of the MD5 hash algorithm is beneficial to protect the integrity of data. The retrieved data will be verified to check its integrity through the verification of the assigned hash value.

VIII. Future work

Data updating process which is not included in the proposed work because of its complexity will be considered for our future work.

IX. Conclusion

This paper has shown that data security and privacy are the main issues in cloud computing. The use of pure data partitioning alone to address the issue is not sufficient for pure data partitioning approaches may bring potential performance and scalability problems when used in widely distributed systems [27] and also still lingering with security issues such as cloud's storage blockage or service outage [13], [24]. And the existing secured data partitioning researches have given less attention on the unification of data partitioning process with the security aspect**.** Therefore, we presented an extensive discussion related to the concept of data partitioning and related works on efficient and secured data partitioning of multi cloud. Lastly, the enhanced technique on efficient and secured data partitioning of multi cloud environment has been proposed.

References

[1] P. Mell, and T. Grance. "The NIST Definition of Cloud Computing". *National Institute of Standards and Technology Special Publication 800-145*, National Institute of Standards and Technology, Gaithersburg, USA, 2012.

[2] R. Balasubramanian, and M. Aramudhan. "Security Issues: Public vs Private vs Hybrid Cloud Computing", *International Journal of Computer Applications (0975 – 8887*), vol. 55, pp.35-41, 2012.

[3] J. Dykstra, and A. T. Sherman. "Understanding Issues in Cloud Forensics: Two Hypothetical Case Studies", *Journal of Network Forensics 3*, 1 (2011), pp. 19–31, 2012.

[4] P. Bala. "Intensification of Educational Cloud Computing and Crisis of Data Security in Public Clouds", *International Journal on Computer Science and Engineering*, vol. 02, No. 03, pp. 741-745, 2010.

[5] F. Shaikh, and S. Haider. "Security threats in cloud computing". In *Proceedings of the 2011 International conference for Internet Technology and Secured Transactions (ICITST)*, pp. 11-14. 2011.

[6] C. John Roberts II, and W. Al-Hamdani. "Who can you trust in the cloud?: A review of security issues within cloud computing". *Proceedings of the 2011 Information Security Curriculum Development Conference*, pp. 15-19, 2011.

[7] K. Jamsa. *Cloud Computing SaaS, PaaS, IaaS, Virtualization, Business Models, Mobile, Security, and More*, Burlington, MA: Jones & Bartlett Learning, 2013.

[8] W. Kim, "Cloud Computing: Today and Tomorrow", *Journal of object technology*, Vol 8 (1), pp. 65–72, 2009.

[9] M. A. AlZain, S. Ben, P. Eric. "Cloud Computing Security: From Single to Multi-clouds". *2012 45th Hawaii International Conference on System Sciences*, pp. 5490–5499, 2012.

[10] S. L. Garfinkel. "An evaluation of amazon's grid computing services: EC2, S3, and SQS". *Technical Report TR-08-07*, School of Engineering and Applied Sciences, Harvard University, USA, 2007.

[11] P. Boampong, and L. Wahsheh. "Different facets of security in the cloud". *Proceedings of the 15th Communications and Networking Simulations Symposium*, pp. 5:1 -5:7, 2012.

[12] D. Hubbard and M. Sutton. "Top Threats to Cloud Computing V1.0". *Cloud Security Alliance*, 2010.

[13] J. Kincaid, "MediaMax/TheLinkup Closes Its Doors". available on Techchrunch, 2008.

[14] D. Sinanc, and S. Sagiroglu. "A review on cloud security". *Proceedings of the 6th International Conference on Security of Information and Networks - SIN '13*, pp. 321–325, 2013,

[15] L. Wang, R. Rajiv, C. Jinjun, B. Boualem. *Cloud Computing Methodology, Systems, and Applications*, Boca Raton, FL.: CRC Press, 2012.

[16] J. Yang, and Z. Chen. "Cloud computing research and security issues". *International Conference on Computational Intelligence and Software Engineering (CiSE)*, pp. 1-3, 2010.

[17] W. Liu. "Research on cloud computing security problem and strategy". *2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)*, pp. 1216–1219, 2012.

[18] M. Vukolic. "The Byzantine empire in the intercloud". *ACM SIGACT News* 41 (3), pp. 105-111, 2010.

[19] P. Dana. "Multi-Cloud: expectations and current approaches". *Proceedings of the 2013 international workshop on Multi-cloud applications and federated clouds*, pp. 1-6, 2013.

[20] R. Leistikow and D. Tavangarian. "Secure Picture Data Partitioning for Cloud Computing Services". *27th International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, pp. 668 – 671, 2013.

[21] Yawei Zhao and Yong Wang. "Partition-based cloud data storage and processing model". *IEEE 2nd International Conference on Cloud Computing and Intelligent Systems (CCIS)*, vol. 1, pp. 218 – 223, 2012.

[22] Huaming Wu, Qiushi Wang and K. Wolter. "Mobile Healthcare Systems with Multi-cloud Offloading". *IEEE 14th International Conference on Mobile Data Management (MDM)*, vol. 2, pp. 668 – 671, 2013.

[23] Kisung Lee, Ling Liu, Yuzhe Tang, Qi Zhang and Yang Zhou. "Efficient and Customizable Data Partitioning Framework for Distributed Big RDF Data Processing in the Cloud". *IEEE Sixth International Conference on Cloud Computing (CLOUD)*, pp. 327 – 334, 2013.

[24] Y. Singh, F. Kandah and Weiyi Zhang. "A secured cost-effective multi-cloud storage in cloud computing". *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 619 – 624, 2011.

[25] P.F. Oliveira, L. Lima, T.T.V. Vinhoza, J. Barros and M. Medard. "Coding for Trusted Storage in Untrusted Networks", *IEEE Transactions on Information Forensics and Security*, vol.7 (6), pp. 1890 – 1899, 2012.

[26] Ping Ren, Wu Liu and Donghong Sun. "Partition-based data cube storage and parallel queries for cloud computing". *Ninth International Conference on Natural Computation (ICNC)*, pp. 1183 – 1187, 2013.

[27] Yunqi Ye, Liangliang Xiao, I-Ling Yen and F. Bastani. "Cloud Storage Design Based on Hybrid of Replication and Data Partitioning". *16th International Conference on Parallel and Distributed Systems*, pp. 415 – 422, 2010.

[28] S. Subbiah, S. Selva Muthukumaran, and T. Ramkumar. "An approach on enhancing secure cloud storage using vertical partitioning algorithm", *Middle-east Journal of Scientific Research*, vol. 23(2), pp. 223-230, 2015.

[29] A. Shamir. "How to share a secret", *Communication of the ACM*, vol. 22 (11), pp. 612-613, 1979.

[30] L. D. Jonathan, and V. R. Chinya. "Security Limitations of Using Secret Sharing for Data Outsourcing". *26th Annual WG 11.3 Conference on Data and Applications Security and Privacy (DBSec'12)*, pp. 145 – 160, 2012.

[31] J. Gray, P. Helland, P. O'Neil, and D. Shasha. "The dangers of replication and a solution". *Proceedings of the 1996 ACM SIGMOD international conference on Management of data*, ACM [Online]. vol.25(2), pp. 173 – 182, 1996.

[32] R. Veena. "Reducing failure probability of cloud storage services using multi-cloud", *Dissertation for master degree*, Department of Computer Science and Engineering, Rajasthan Technical University, Kota, India, 2013.

Author Biographies

Hazila Hasan was born in Kedah, Malaysia, on May 01, 1981. She received her B.IT in Information Systems Engineering from Multimedia University, Malaysia in 2003 and Master of Computer Science in Information Security from Univerrsiti Teknologi Malaysia in 2012. She is currently pursuing her Ph.D in Information security. Her research interests are in cloud computing security and encryption.

Suriayati Chuprat was born in Sabah, Malaysia, on February 12, 1973. She received her Degree in Computer Science from Universiti Teknologi Malaysia in 1995, Master in Real-Time Software Engineering from Universiti Teknologi Malaysia in 2000 and Ph.D in Mathematics from Universiti Teknologi Malaysia in 2009. Presently, she is working as a senior lecturer at Universiti Teknologi Malaysia. Her research interests are in distributed file systems, dynamic load balancing, heterogeneous distributed systems, high performance scientific computing, parallel architectures, parallel processing, scheduling, and distributed data mining.