PERFORMANCE IMPROVEMENT FOR CRYPTOGRAPHY, COMPRESSION AND DATA TRANSFER IN MULTI-CLOUD STORAGE THROUGH PARALLELIZATION

Mahdi Aza'r, Elankovan Sundararajan

Research Center for Software Technology and Management,
Fakulti Teknologi dan Sains Maklumat, Universiti Kebangsaan Malaysia
43600 UKM Bangi, Selangor Malaysia.

Email: p97093@siswa.ukm.edu.my, elan@ukm.edu.my

ABSTRACT

Cloud computing is rapidly becoming more popular from day to another. It is used for most computing purposes today because it reduces the cost of computing and availability of resources. For better computing, cloud data storage becomes more popular because, nowadays, cloud storage services are used by a wide range of user types including governments, companies, banks, organizations. These users are getting advantage of cloud storage to share data between departments, other system components and among their authenticated end-users. This project is designed to overcome cloud storage performance which is considered one of the most critical aspects in the cloud especially for confidential data which should not be accessed by any unauthorized parties. The confidential data is not secure in one cloud service provider when it could be accessed from the cloud administrator or worker. The objectives of this project are to design and develop an algorithmic way to improve performance of confidential data recovery and data transfer between cloud serves provider and users. By converting data into slices, encrypt each slice with parallel techniques and store them encrypted in more than one cloud services provider storage, the property of data leak will reduce because the data would be meaningless in cloud. By designing this solution that encrypts the data slices before uploading it to different cloud storages, data can only be decrypted in the authenticated user's local machines. Since the encryption performed on local machine it much more saver then the cloud. This solution is improving performance and illuminating any third-party to have a clone of data because it converts the data into chunks of bits that are not useful only in one local machine that has the correct authorization by having the correct encryption and decryption key. The approaches have been used to complete this project are slice, encrypt, shuffle sliced data, compressing sliced data, and then uploaded it into different cloud service storage this will result in more secure data and improvement of performance for the data recovery needs.

Keyword: Cloud computing, Encryption, Slice, Shuffle, Compression, Recovery performance, comma-separated values CSV.

I. INTRODUCTION

Web-based applications generally store static data on the server, enabling the client to mobility, simpler configuration, and manage enhanced data. These applications are increasingly designed for scalability and support the plugin architecture, allowing third-party developers to quickly deliver additional features and provide improved services and customization. However, this design can result in an application bug or a single misconfiguration that affects many users, which may result in data

loss or corruption. Third-party plugins may be poorly tested and can cause problems with other plug-ins, or even worse than corrupt user data.

The cloud is gradually achieving more capacity slowly. The cloud has been in use for many years, with a myriad of things like Flickr, Google Apps, Skype, and MSN Messenger. The idea started during the 1960s, when John McCarthy thought counting was an open aid (Krogstie 2012). Recruiting appeared strewn with affiliations and schools offering in the late 1970s. In the mid-1990s enlistment decided to grant basic access to computer control such as the electric power matrix. In different settings, the expression "cloud" was used to photograph the massive ATMs during the 1990s (Zhang et al. 2010). A huge step was observed during the 1990s due to the rise of the Internet and the evolving speed of Internet affiliations. The reasonableness of virtual private networks (VPN) is found after the precondition for transferring protected and secure data between correspondence between branches. These workflows require weight change according to optimized resource use. VPN is safer than basic dial-up, and any system in the outside world requires additional luxury endeavors (Feilner 2006). Of course, Web 2.0 moved the web instinctively, dynamically and synergistically with social messaging and the full knowledge of its owners and introduced opportunities to influence the web and attract its customers more conveniently. Enterprises were rapidly adopting Web 2.0, which is the second stage in the Web's advancement. Various computing paradigms were presented during the 21st century. The popular ones between them are cluster, grid, and cloud computing. Among the standard names associated with cloud formation, sales control by giving endeavors applications through a website, Amazon with Amazon Web Services (AWS), Amazon's Computing Cloud (EC2), Microsoft and Windows Azure, and Google with its several services, for example, Google Docs which gave the cloud an unimaginable push and public visibility. Eucalyptus, OpenNebula and Nimbuswere shown as basic open source stages for the transmission of special clouds, like the hybrid (Peng et al. 2009). It is arranged around various Cloud-focused professions that enlist parallel engagement, appropriate planning and virtualization structures to give virtual machines (VMs) to customers on demand. The prominent variant relationship, for example, IBM, Oracle, Dell, Fujitsu, Tera, HP, Yahoo, and other huge names displaying the cloud that prepares after that.

The method of data recovery fluctuates, depending on the conditions of data misfortune and the programming of data recovery used to create the reinforcement and oriented reinforcement media. For example, various work area and workstation enhancement stages in programming allow customers to recover lost documents themselves, while restoring a harmed database from tape enhancement is an increasingly mind-boggling process that requires IT intercession. Data recovery administrations can also be used to restore documents that have not been supported and are still on your hard circle, coincidentally deleted from the database system of your PC. Records can be recovered since in better places the records and records about that record are being kept. For example,

Windows uses a record portion table to keep track of documents on your hard drive and where they are stored. The assignment table resembles the chapter of the book by chapter list, while the pages in the book resemble the genuine documents on the hard drive. Normally only the record allotment table does not work effectively at the stage where data should be retrieved. There are different approaches to recover it if the record is damaged, lost, or corrupted. On the off chance of physically harming the record, it can be changed at the moment. For example, various programs, Microsoft Office, place institutionalized headers at the beginning of records to suggest that they have a position with this application. Many utilities can be used to physically change the headers of the text, so some records can possibly be retrieved. Some ways of data recovery incorporate development, and organizations do not only collect data by tape. Application recovery and critical data from tape needs some effort, and after a disaster you may need to get to your data. The sharing of tapes is also concerned with hazards. In addition, it may not be necessary to continue activities with all development data in a remote area. It is therefore smart to find out what can be saved and what data should be retrieved.

Transferring data between the cloud provides and users is considered one of the most critical aspects in the cloud because of the sensitive and important information stored in cloud. Cloud services are used by a wide range of user types including governments, companies, banks, organizations and along to the typical social networking users. The leaking of cloud information might cause a disaster based on how critical the data is. To avoid the risk of malicious insider in the cloud and to avoid the failing of cloud services such as, data integrity, data security, data intrusion, and service availability researcher suggested to use multi cloud service provider to store important and confidential data in order to reduce the chance of data leaking and data losing. The problem in current algorithms used in cloud data recovery is that it takes more time to recover lost data. In multiple cloud-based data recovery service, multiple cloud service provider resources can be used collaboratively. Simple and unified interface for end users is exposed to adapt cloud service providers and the internal process between the clouds become invisible to users. The proposed priority of scheduling strategy to balance data recovery goals, such as high data reliability, low backup cost, and short transparent recovery time for users (AlZain et al. 2011; Challagidad et al. 2017; Cidon et al. 2013).

This paper consists of five (5) sections. Section I discuss the background of this study including the issues and problems in data recovery performance. Section II discuss literature review. Section III elucidates process design and research questions in the study. Section IV presents the findings of the work and discussion. Lastly, section IV concludes the paper with a summary of the findings and recommended future work.

II. LITERATURE REVIEW

A. Overview of Cryptography

Encryption is the technology area to secure information. It attempts to secure and encrypt information so that the original information cannot be re-encrypted or decrypted by a third party with access to encrypted hidden data. Practically speaking, encryption methods apply a verified function, algorithm or routine to information with the appropriate key specified before data encryption and the corresponding algorithm, or function or routine for decoding information, as it is no longer accessible as it was original, original information can be retrieved. Encryption is a data encryption technique into a secret code. It is the most effective way to secure data. The data is translated into a type in the process, called a cipher text that is not easily understood by unauthorized individuals. Decryption is the mechanism by which encrypted data is translated into its original form so that it can be understood. Encryption switches data to prevent anyone who does not have a key to access it from intercepting it (Sharma & Gandhi 2012).

i) Secure Hash Algorithm (SHA 256)

SHA-256 is a member of SHA-2 cryptographic hash functions designed by the National Security Agency (NSA). SHA stands for Secure Hash Algorithm. Cryptographic hash functions are mathematical operations that run on digital data; by comparing the calculated "hash" (resulting from the implementation of the algorithm) with a known and predicted hash value, a person can determine the integrity of the data. A one-way hash can be created from any part of the data, but the data cannot be created from the hash.

AlZain et al. (2011) proposed model called Multi-clouds Database (MCDB). MCDB guarantees security and privacy in the cloud computing environment and relies on multi-cloud service providers and the secret exchange algorithm with SHA256 algorithm. These techniques have been used in previous research on database security. MCDB provides a "cloud database" that allows customers different types of database queries, such as aggregation and exact match and range query, with the ability to store any different type of data, such as Videos, images or documents. The purpose of the proposed new model is to avoid the risk of malicious insider information in the cloud and avoid the failure of cloud services. Security risks such as data integrity, data intrusion and service availability have been examined in the model.

Sundarakumar (2019) proposed a model used secure encryption algorithm (SHA-256) technology proposed to control cloud computing access. SHA-256 redefines the encrypted text policy with a well-

defined structure for system users, for secure and flexible access control. In this process, the text is encrypted with the access policy specified by encryption, while the corresponding decryption key is generated for a set of attributes. The attributes associated with the decryption key meet the access policy associated with a given encrypted text, and the key can be used to decrypt the text. With this SHA achieved precise access control and good data access in the cloud in an elaborate manner.

ii) Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES), a symmetric block encryption chosen by the United states (US) government to protect classified information, is implemented in software and hardware worldwide to encrypt sensitive data. The competing algorithms must be judged for their ability to resist attack, compared to the other zeros provided, although the security force is the most important factor in the competition.

Nehe and Vaidya (2016) proposed a middleware-oriented framework that integrates different Infrastructure as a Service (IaaS) storage clouds for data recovery. Depending on the access token of registered users, the middleware performs authentication with IaaS cloud frames. The middleware is based on a service level administrator which decides how to divide a file that is being uploaded, encryption and decryption using Advanced Encryption Standard (AES) followed by merging to download. The middleware supports integrated authentication of all cloud platforms. The evaluation of the framework shows a great improvement in security, since they are distributing the storage and encrypting the data.

Vanitha and Mangayarkarasi (2016) discuss the data security algorithm in the cloud and make a comparison between the different algorithm. Many similar algorithms such as Data Encryption Standard (DES), Triple Data Encryption Algorithm (Triple-DES), Advanced Encryption Standard (AES), and Blowfish also explain an asymmetric algorithm such as Rivest–Shamir–Adleman (RSA). Results that AES and blowfish are algorithms are very safe and good. Using power and speed in AES and Blowfish algorithms is better when compared to other algorithms. When we use an asymmetric encryption algorithm, RSA is protected and able to be used to run the application in a wireless network, due to its speed and security.

Kulkarni et al. (2015) proposed an advanced encryption algorithm (AES) and seed block option (SBA) proposed an advanced encryption algorithm. The proposed method uses AES and SBA. If data is accidentally deleted, can get it from the remote server. This method takes less time to recover data and resolve time-related issues. The method thus provides an effective security mechanism for data stored in the cloud environment.

B. Data Slicing

Slicing refers to a way to segment, display, and understand data in a database. Large blocks of data are cut into smaller segments and the process is repeated until the correct level of detail is achieved for proper analysis. slicing thus presents data in new and diverse perspectives and provides a closer look at them for analysis. For example, the report shows the annual performance of a product. If we want to show quarterly performance, we can use the slicing strategy to move to the quarterly level.

Data slicing is a technique for dividing data into independent pieces. The data can be divided into three ways: horizontal slicing, vertical slicing and hybrid slicing. The main idea behind splitting the data is to divide the entered data into several independent pieces, then encrypt each piece with an algorithm different from the previous one in order to further secure the encrypted data, as it is very difficult for the attacker to decipher all the algorithms with 100% accuracy and in time (Kaur et al. 2018).

Subramanian and John (2017) proposed a system for cloud customers to make their requests. The proposed system called Dynamic Multi-Cloud Data Division (DDS-MC). The DDS-MC system has different components that are responsible for finding the required services from the appropriate service providers. The proposed methodology ensures that the file cutting parts are defined by the owner of the data limited to the available storage locations. The data owner loads the file through the proposed framework interface. The receiver sends the decryption request to the owner. After the successful verification owner acknowledges the decryption request and submits the necessary credentials to download the file. The recipient enters the credentials through the framework interface. The frame retrieves the parts of the file and each part is decrypted and stores the receiver's machine. The receiver or service provider has no knowledge about the number of file parts stored on the multi-cloud server. This method also guarantees that the file cannot be accessed without the knowledge or permission of the owner.

Kaur et al. (2018) proposed a data slicing fragmentation technique horizontal or vertical fragmentation technique to create the information segments. The entire data set is divided into segments, either by mistreatment or horizontal data slicing technique. These slices of segments are encrypted mistreatment 3 completely different cryptography rule. And then transfer this chunk of segments to the cloud. This segment portion uses the cryptography technique before loading a portion of information in the cloud and once it downloads a portion of information from the cloud server. Each fragment is encrypted with a completely different scientific discipline rule.

The secure personal cloud storage system that offers the convenience of connecting and using the portable storage device (PSD) is highlighted.(Mar et al. 2015) The authors demonstrated the accessibility and scalability of cloud storage, using the information dispersion algorithm (IDA) to address the dual requirements for confidentiality and data availability. Its implementation allows sector files to be distributed among multiple Cloud service providers (CSPs). Therefore, the adversary must commit at least two or three cloud providers to be able to reconstruct the data. Similarly, two CSPs must collude to mount any effective attack (Sighom et al. 2017).

Ul Islam Khan et al. (2016) proposed a mechanism to design secure storage and an accessible framework for cloud computing that can provide more privacy, confidentiality and integrity. The framework is called "SSM", which means secure division and storage of information in data centers. The main goal of system design is to develop a robust and secure storage infrastructure to improve cloud accessibility. System design focuses on managing and protecting the secure data store that the customer downloads to a cloud application. The security architecture of cloud computing allows only the right user to download or share data as needed. The cloud computing security architecture provides a multi-cloud security architecture that allows a valid user to store or download data in a distributed cloud environment and keep it for future work. In the current mechanism, there is a need for a large storage capacity which cannot be reached by a personal computer due to limitations in both processing and storage. The unique feature of this system design is that it uses a strange encryption and decryption technology which depends on how the key is distributed. The system design provides many services to prevent vulnerable attacks. The company's goal is to provide a sophisticated security architecture that enables data security in multiple applications in the cloud to authenticate the user against illegal activity.

C. Data Compression

Compression can be divided into two categories, such as lossy and lossless. In lossless compression, rebuilding after compression is numerically identical to the original. In a lost compression scheme, reconstructed data relates to relative degradation. Lost technique degrades quality at every compression or decompression. In general, lossy techniques provide greater compression rates than lossless techniques.

Data compression is a decrease in the number of bits needed to represent data. Data compression can save storage, speed up file transfers, reduce network storage and bandwidth costs. Compression is performed by a program that uses an algorithm to determine how to shrink data. For example, the algorithm may represent a series of bits - or 0s and 1s - with a string smaller than 0s and 1s using a dictionary to convert between them, or the formula may insert a reference or pointer to a

string of 0s and 1s that the program has already seen. Data compression can dramatically reduce the amount of storage the file consumes. For example, in a 2: 1 compression ratio, a 20 MB file takes up 10 MB of space. As a result of the compression, spend less money and less storage time (Crocetti& Sliwa 2017).

Sharma and Gandhi (2012) propose data compression and encoded to reduce storage space, time of transmission and data protection. The data representation size is reduced by the compression algorithm to minimize the storage needed for that data. Compression of data is a desirable way of reducing transmission costs by using the available bandwidth effectively. Over the past decade, an unparalleled increase has occurred in the amount of digital data sent over the Internet, including text, pictures, video, audio, computer software, etc. As this trend continues unexpectedly, research into the development of algorithms that can optimize the productivity of the available network bandwidth by compressing data to the limit makes sense. It is also important to consider the security implications of the data being sent as it is being compressed, since most of the text data transmitted over the Internet is highly vulnerable to many attacks.

Zhou and Zhu (2018) propose a solution to recovering data using cloud storage by creating two clouds, sending text files (pdf, doc, docx) and an image file (jpg, png, gif) from the first cloud to the second cloud. Before storing both files in the second cloud, apply the data integrity algorithm (Keyed-hash message authentication code (HMAC)) to check the integrity of the data on both files, and then apply the data compression algorithm (LempelZiv-Welch (LZW)) to compress data on both files such as Text and image. After verifying the integrity and successfully compress both files, store the compressed files in the second cloud. Remote cloud like Dropbox and Google Drive let you host, edit, share and sync files only. The main cloud called Central Server will run with an operating system designed to support multiple users, multi-user applications, databases, and considerably more.

III. PROCESS DESIGN AND RESEARCH QUESTIONS

The objectives of this study are to improve performance of confidential data recovery for organizations that use cloud as storage and improve data transfer between cloud serves provider and users. The context of the project is slicing, encrypting, shuffling and upload source data securely into number of cloud clusters from different service providers with the ability to download, decrypt and assemble the same data again. That to ensure the objectives of this study. The process design of the project is explained as follows.

A. Data Split

The main reason for splitting the data is to increase security, so, when a cyberattack aims at the data in the cloud or when it's on its way to be uploaded or downloaded, the attacker can only have a small part of the data instead of having all in one. This is not the only security step; however, it reduces the possibility of data leaking.

This process has its own cost, it slows down the entire flow which is sometimes noticeable especially if the inputted data is a big file. However, to speed up this process, getting advantages of multiprocessing programming is an advantage itself whereas it divides the amount of runtime by the number of Central Processing Units (CPU) available cores. Multiprocessing does not solve the slowness completely, however, it reflects noticeable changes.

Splitting the input file is a discussable step, whereas, data will be encrypted and shuffled anyway as shown in the next few sections. However, data will be encrypted by an auto generated Secret-Key which might be spoiled to whom can get advantage of strict data that should be protected. Simply, splitting the input file is a step where if the secret key got spoiled, the sniffer-attack would decrypt a smaller part of the data instead of its all.

Another advantage of splitting the input file is to help shuffling the data and upload it securely as chunks in different cloud service providers. This process is the initial point for generating a compartmentalized data chunks for each cloud storage which is another security step that is discussed in this section.

B. Data Encryption and Data Decryption

This process takes the input from the output of Splitting process that is explained above. Simply, it takes each file and output an encrypted version of the same file by using parallel process. The top advantage of the decryption is keeping the data secure even from cloud service providers. Since the data is uploaded by HTTPS protocol which is based on OpenSSL - an open-source secure library for secure communication - data is already encrypted and it is almost impossible to decrypt the data. However, this process is to add one more layer of encryption to prevent the data which should be highly protected from cloud service providers; because, OpenSSL encrypts the data only when it's on its way to the destination but when the data is uploaded, it is not encrypted anymore which allows the service providers to copy or have unprivileged look though the data.

C. Data Compressing and Data Decompression

The compressing process in this project designed to use GZIP software which is originally a file format standard to reduce file sizes efficiently and quickly. This process is helpful for the project in a way that reducing the uploading and downloading size. Additionally, it also reduces the cost of cloud storage services.

Compressing Data Process is designed to generate a compressed file for each cloud service provider. In other words, it takes the chunks - the output of shuffling process - and generate one compressed file for each cloud service provider.

To enhance the data availability, each file that has been generated for a single cloud service provider is copied to the next file, thus when one of the cloud service providers is down, its data is available in the other cloud service chunks.

D. Downloading and Uploading from or to Cloud Clusters

This is the final step for the whole uploading process. Uploading the compressed chunks to its designated cloud storage. This process is parallelized as other process in this project to enhance the performance and utilize the machine hardware components.

The main functionality of uploading component is to take a copy of the output of compressed data and use the Application Programming Interfaces (APIs) that are provided by service providers to upload these files to their end destination.

In this project five cloud clusters are made which are two clusters from Google Cloud Storage, one cluster from AWS S3 Storage and two clusters from Dropbox. Because of differences between each service provider, each different APIs have different methods to deal with in the programming level. The flow is not unified or standardized which makes adding more clusters or new service provider harder in term of system integrity.

The case for this study to test confidential comma-separated values (CSV) dataset. In general, the study aims to answer the main project question which is, how to reduce the chances of unauthorized access to confidential data stored in the cloud services with keeping the availability and less effect the performance of storing and retrieving?

IV. RESULTS & DISCUSSION

Parallel processing enhances the performance by almost 10000%. Parallel processing utilizes the hardware in the machine so instead of using only single process, all facility of computer's CPU is used. By using comma-separated values (csv) dataset different size of files to test the project after applying the parallelism techniques for the encryption and deception, compression and decompression and uploading and downloading the time consumed of processing as shown below differences between the before and after implementing this prosses is considerable improved.

A. Encryption and Decryption

After implementing the encryption and decryption process in this project, a slowness of the encryption and decryption flow is noticed. Then, a parallelism of encryption and decryption process is implemented which make a tremendous improvement. Below in this section is a table 1 shows the differences between the before and after implementing the sub processes of encryption and decryption processes in parallel.

Table 1: Test Results Before and After implementing Parallel Processing in Encryption and Decryption.

Data Size	Time consumed without parallel processing	Time consumed with parallel processing
18MB	4 Minutes	2.4 Seconds
1GB	222 Minutes	2.3 Minutes
5GB	1120 Minutes	12 Minutes
10GB	2470 Minutes	20.9 Minutes

B. Compression and Decompression

A delay in the compression and decompression flow is observed after implementation of the compression and decompression process in this project. Thereafter, a parallelism of the method of compression and decompression is applied which allows a considerable improvement. Below in this

section is a Table 2 showing the variations between the compression and decompression processes in parallel before and after implementation of the sub processes.

Table 2 : Test Results Before and After implementing Parallel Processing in Compression and Decompression.

Data Size	Time consumed without parallel processing	Time consumed with parallel processing
18MB	1.1 Minutes	3.1 Seconds
1GB	65.9 Minutes	3.09 Minutes
5GB	329.9 Minutes	15.5 Minutes
10GB	659.9 Minutes	31.5 Minutes

C. Uploading and Downloading

A delay in the uploading and downloading flow is observed following execution of the upload and download phase in this project. Thereafter, a parallel process of uploading and downloading is applied which makes a considerable improvement. Below in this section is a table 5.3 which shows the differences between the upload and download processes in parallel before and after implementation of the sub processes.

Table 3 : Test Results Before and After implementing Parallel Processing in Uploading and Downloading.

Data Size	Time consumed without parallel processing	Time consumed with parallel processing
18MB	40 Seconds	19 Seconds
1GB	39.9 Minutes	18.9 Minutes
5GB	199 Minutes	94.5 Minutes
10GB	400 Minutes	190 Minutes

V. CONCLUSION

This study was designed to improve performance of confidential data recovery for organizations that use cloud as storage and improve data transfer between cloud serves provider and users. Furthermore, improving the performance of the proposed solution to increase its usability and efficiency. In general, it was found that the data stored in cloud services are not secure enough especially when the data are confidential and important data and the time consumed for this processing is high. At the end

of this project provides a solution to store this data in clouds for data recovery and backups using different slicing and encryption algorithms and decrease the time consumed for this processing.

There are many trends to expand slides in the future. The first is big data. All tests carried out in this project were on tables with fewer than 100,000 rows. It will be interesting to know whether the cutting efficiency will continue as the number of rows and columns the project handles significantly increases. The next addition that can be made to this project is to apply data recovery to full table groups or databases. So far, the program has focused on slicing, marge, encrypting, and decrypting a single CSV file. If anatomy can be applied to a single file, it can be applied to any number of files. Role key restrictions can also be considered when encrypting multiple files.

ACKNOWLEDGEMENT

Praise and thanks to Allah first and foremost whose blessing enabled me to accomplish this project. I would like to thanks, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia.

REFERENCE

Alshammari, M. M., Alwan, A. A., Nordin, A. & Al-Shaikhli, I. F. 2018. Disaster recovery in single-cloud and multi-cloud environments: Issues and challenges. *4th IEEE International Conference on Engineering Technologies and Applied Sciences, ICETAS 2017* 2018-Janua(November): 1–7. doi:10.1109/ICETAS.2017.8277868

AlZain, M. A., Soh, B. & Pardede, E. 2011. MCDB: Using multi-clouds to ensure security in cloud computing. *Proceedings - IEEE 9th International Conference on Dependable, Autonomic and Secure Computing, DASC 2011* (December): 784–791. doi:10.1109/DASC.2011.133

Benusi, A. & Hyka, D. 2014. A Framework for Secure Data Exchange in Mobile Cloud Computing. *International Electronic Journal of Pure and Applied Mathematics* 7(3). doi:10.12732/iejpam.v8i2.1

Bobde, R. R., Khaparde, A. & Raghuwanshi, M. M. 2015. An approach for securing data on Cloud using data slicing and cryptography. *Proceedings of 2015 IEEE 9th International Conference on Intelligent Systems and Control, ISCO 2015*. doi:10.1109/ISCO.2015.7282356

C.Lakshmi, D. 2014. Impact Study of Cloud Computing on Business Development. *Operations Research and Applications: An International Journal (ORAJ)* 1(1).

Challagidad, P. S., Dalawai, A. S. & Birje, M. N. 2017. Efficient and Reliable Data Recovery Technique in Cloud Computing. *Science Publishing Group* 5: 13–18. doi:10.11648/j.iotcc.s.2017050501.13

Cidon, A., Rumble, S., Stutsman, R. & Katti, S. 2013. Copysets: Reducing the Frequency of Data Loss

in Cloud Storage. *Atc '13* 37–48. Retrieved from http://www.stanford.edu/~skatti/pubs/usenix13-copysets.pdf

Crocetti, P. and Sliwa, C. (2017). What is data compression? [online] SearchStorage. Available at: https://searchstorage.techtarget.com/definition/compression?cv=1.

Drive savers data recovery. 2019. What are the Different Types of Data Recovery Services?. [Online]. [10 November 2019]. Available from: https://drivesaversdatarecovery.com/blog/what-are-the-different-types-of-data-recovery-services/

Feilner, M. 2006. OpenVPN Building and Integrating Virtual Private Networks Learn. *Design*. Packt Publishing. Retrieved from http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:OpenVPN+Building+and+Integrating+Virtual+Private+Networks#0

Garg. 2019. Threats to Information Security. [Online]. [3 November 2019]. Available from: https://www.geeksforgeeks.org/threats-to-information-security/

Hannan, E. and Burton, A. (2017). What is data recovery? [online] SearchDisasterRecovery. Available at: https://searchdisasterrecovery.techtarget.com/definition/data-recovery.

Idexcel technologies. 2019. Data Backup and Recovery in Cloud Computing. [Online]. [10 November 2019]. Available from: https://www.idexcel.com/blog/data-backup-and-recovery-in-cloud-computing/.

Jain, G. 2017. A Survey On Security Using Encryption Techniques In Cloud 5(2): 326–331.

Kaur, R., Singh, P. & Rani, S. 2018. Migrated Encrypted Data in Cloud using Data Slicing Approach. *International Journal of Computer Sciences and Engineering* 6(7): 286–290. doi:10.26438/ijcse/v6i7.286290

Khoshkholghi, M. A., Abdullah, A., Latip, R., Subramaniam, S. & Othman, M. 2014. Disaster Recovery in Cloud Computing: A Survey. *Computer and Information Science* 7(4): 39. doi:10.5539/cis.v7n4p39

Krogstie, J. 2012. Model-Based Development and Evolution of Information Systems: A Quality Approach. *Springer Science & Business Media*, hlm. Vol. 91. doi:10.1017/CBO9781107415324.004

Kulkarni, T., Memane, S., Nene, O. & Dhaygude, K. 2015. Intelligent Cloud Security Back-Up System 3(2): 241–245.

M. E. Whitman, Principles of information security, 6th ed. Boston, MA: Course Technology,2018.

Manion, T., Kim, R. & Patiejunas, K. 2014. Remote Desktop Access Software | BOMGAR. http://www.bomgar.com/products

Mar, K. K., Law, C. Y. & Chin, V. 2015. Secure Personal Cloud Storage 108–113.

Mukundha, C. & Chandar, B. 2018. Identity Based Encryption in Cloud Computing With Outsourced

Revocation Using Ku-CSP 08(8): 12–21.

Nehe, S. & Vaidya, M. B. 2016. Data security using data slicing over storage clouds. *Proceedings - IEEE International Conference on Information Processing, ICIP 2015* 322–325. doi:10.1109/INFOP.2015.7489401

Osorio, G. A., Del Real, C. S., Valdez, C. A. F., Miranda, M. C. & Garay, A. H. 2011. The NIST Definition of Cloud Computing. *Acta Horticulturae* 728: 269–274.

Peng, J., Zhang, X., Lei, Z., Zhang, B., Zhang, W. & Li, Q. 2009. Comparison of several cloud computing platforms. *2nd International Symposium on Information Science and Engineering, ISISE 2009* 23–27. doi:10.1109/ISISE.2009.94

Powell, O. and Rikhi, I. (2019). What is Data Recovery and How It is Helpful for You ?. [online] Stellar Data Recovery Blog. Available at: https://www.stellarinfo.com/blog/know-about-data-recovery.

Pillai, A. & Khurana, A. 2017. Internet of Things: Applications and Future Trends. *International Journal of Innovative Research in Computer and Communication Engineering Internet of Things: Applications and Future Trends* 5(3): 5194–5202. doi:10.15680/IJIRCCE.2017

Ramgovind, S., Eloff, M. M. & Smith, E. 2014. The management of security in cloud computing. *Proceedings of the 2010 Information Security for South Africa Conference, ISSA 2014* (September). doi:10.1109/ISSA.2010.5588290

S, M. & Venkateshkumar, D. S. 2018. Cloud Computing in Data Backup and Data Recovery. *International Journal of Trend in Scientific Research and Development* Volume-2(Issue-6): 865–867. doi:10.31142/ijtsrd18652

Sharma, M. & Gandhi, S. 2012. Compression and Encryption : An Integrated Approach. *International Journal of Engineering Research & Technology (IJERT)* 1(5): 1–7. Retrieved from www.ijert.org

Sighom, J. R. N., Zhang, P. & You, L. 2017. Security enhancement for datamigration in the cloud. *Future Internet* 9(3): 1–13. doi:10.3390/fi9030023

Subramanian, K. & John, F. 2017. Dynamic Data Slicing in Multi Cloud Storage Using Cryptographic Technique. *Proceedings - 2nd World Congress on Computing and Communication Technologies, WCCCT 2017* 159–161. doi:10.1109/WCCCT.2016.46

Sundarakumar, M. R. 2019. Authorization for secured cloud storage through SHA-256 5(1): 1–3.

Ul Islam Khan, B., Baba, A. M., Olanrewaju, R. F., Lone, S. A. & Zulkurnain, N. F. 2016. SSM: Secure-Split-Merge data distribution in cloud infrastructure. *ICOS 2015 - 2015 IEEE Conference on Open Systems* (August): 40–45. doi:10.1109/ICOS.2015.7377275

Vanitha, M. & Mangayarkarasi, R. 2016. Comparative study of different cryptographic algorithms. *International Journal of Pharmacy and Technology* 8(4): 26433–26438.

Wei, J., Liu, W. & Hu, X. 2018. Secure data sharing in cloud computing using revocable-storage identity-based encryption. *IEEE Transactions on Cloud Computing* 6(4): 1136–1148.

doi:10.1109/TCC.2016.2545668

Zhang, Q., Cheng, L. & Boutaba, R. 2010. Cl[1] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: state-of-the-art and research challenges," J. Internet Serv. Appl., vol. 1, no. 1, pp. 7–18, Apr. 2010.oud computing: state-of-the-art and research challenges. *Journal of Internet Services and Applications* 1(1): 7–18. doi:10.1007/s13174-010-0007-6

Zhou, L. & Zhu, Y. 2018. Preprocessing method before data compression of cloud platform. *International Conference on Communication Technology Proceedings, ICCT* 2017-Octob: 1223–1227. doi:10.1109/ICCT.2017.8359830