SECRET SHARING SCHEME FOR KEY MANAGEMENT OF SECURE DATA SHARING IN CLOUD

NOORHAFEZAN BIN ABD MAJID

FSKTM 2019 43

SECRET SHARING SCHEME FOR KEY MANAGEMENT OF SECURE DATA SHARING IN CLOUD

By

NOORHAFEZAN BIN ABD MAJID

Thesis submitted to the Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, in fulfillment of the requirements for the Master of Information Security

JUNE 2019

COPYRIGHT PAGE

DEDICATIONS

"Many of life's failures are people who did not realize how close they were to success when they gave up."

Thomas Edison

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfillment of the requirement for the degree of Master of Information Security

SECRET SHARING SCHEME FOR KEY MANAGEMENT OF SECURE DATA SHARING IN CLOUD

By

NOORHAFEZAN BIN ABD MAJID

JUNE 2019

Supervisor: Dr. Sharifah Md Yasin

Faculty: Faculty of Computer Science and Information Technology

Cloud computing is no longer a new phenomenon in the industry. Cloud storage is an important milestone in the cloud computing industry and one of the security features that were introduced in cloud storage is via cryptographic methods to control the access only to authorized users.

One of the known issues in cloud storage is the high key generation time for large-scale users and limiting the use of cryptography for data encryption. This problem can be overcome by using cryptography uses a single key, but another problem will arises is the potential for a single point of vulnerability if the key fell in the hands of unauthorized persons, then the whole secret and information can be compromised.

The objectives of this study were to execute and analyze key generation times for large-scale users using the AES-256 method and Shamir's Secret Sharing Scheme, which both are still using a single key concept and prove Shamir's Secret Sharing Scheme is more suitable for large-scale users. Further testing proves that Shamir's Secret Sharing Scheme is more appropriate for large-scale users covering key generation and thresholds to ensure data is completely secure.

There are five (5) phases for this study, identify problems and requirement analysis, design and analysis, design an algorithm, code development and result analysis, and documentations.

The test run in localhost by using PHP platform and there are additional components such as the Composer for the implementation of Shamir's Secret Sharing Scheme and the comparison will be recorded based on the two data types, number of users and file size. Based on the results of the tests, it can be proved that Shamir's Secret Sharing Scheme provides key generation times faster than AES-256, and strengthen by the control of key threshold to ensure that the stored data is more secure. Shamir's Secret Sharing Scheme has also denied the problem of point the vulnerability exist in the AES-256.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia Sebagai memenuhi keperluan untuk Ijazah Sarjana Keselamatan Maklumat

SKEMA PERKONGSIAN RAHSIA UNTUK PENGURUSAN KUNCI BAGI KESELAMATAN DATA DI DALAM PERKOMPUTERAN AWAN

Oleh

NOORHAFEZAN BIN ABD MAJID

JUNE 2018

Penyelia: Dr. Sharifah Md Yasin

Fakulti: Fakulti Sains Komputer dan Teknologi Maklumat

Pengkomputeran awan bukan lagi satu fenomena baru di kalangan industri. Storan awan merupakan salah satu tonggak penting dalam industri pengkomputeran awan dan salah satu daripada ciri keselamatan yang diperkenalkan di dalam storan awan adalah melalui kaedah kriptografi bagi mengawal capaian hanya untuk pengguna yang dibenarkan sahaja.

Salah satu masalah yang dapat dikenalpasti di dalam storan awan adalah masa janaan kunci yang tinggi bagi pengguna yang berskala besar dan masalah membataskan penggunaan kriptografi bagi penyulitan data. Masalah ini boleh diatasi dengan menggunakan kriptografi menggunakan kunci tunggal sahaja, namun masalah lain yang timbul adalah potensi satu titik kerentanan di mana sekiranya mana-mana kunci jatuh di tangan orang yang tak dibenarkan, maka keseluruhan rahsia dan maklumat boleh diceroboh.

Objektif kajian ini dibuat adalah untuk menguji dan menganalisis masa janaan kunci bagi pengguna berskala besar menggunakan kaedah AES-256 dan juga Shamir's Secret Sharing Scheme di mana kedua-duanya masih menggunakan konsep kunci tunggal. Pada pengujian seterusnya juga membuktikan bahawa Shamir's Secret Sharing Scheme adalah lebih bersesuaian untuk pengguna berskala besar merangkumi masa janaan kunci dan kawalan kunci ambang bagi memastikan data benar-benar selamat.

Terdapat lima (5) fasa bagi kajian ini iaitu, mengenalpasti masalah dan menganalisis keperluan, analisis rekabentuk pengujian, rekabentuk algorithm pengujian, pembangunan kod dan analisis keputusan, dan dokumentasi keseluruhan pengujian.

Pengujian ini dilaksanakan dalam komputer peribadi menggunakan platform PHP dan terdapat komponen tambahan seperti Composer bagi implementasi pengujian Shamir's Secret Sharing Scheme dan perbandingan yang dibuat adalah daripada janaan masa kunci yang dibuat oleh kedua-dua kaedah yang dinyatakan di atas menggunakan jenis data yang berbeza seperti bilangan pengguna dan juga saiz fail. Berdasarkan keputusan pengujian yang dilaksanakan, dapat dibuktikan bahawa Shamir's Secret Sharing Scheme memberikan masa janaan kunci yang lebih pantas berbanding AES-256 dan diperkukuhkan lagi dengan kawalan kunci ambang bagi memastikan data yang disimpan adalah lebih selamat dan Shamir's Secret Sharing Scheme juga telah menafikan masalah satu titik kerentanan yang wujud di dalam AES-256.

ACKNOWLEDGEMENT

First of all, I would like to thank Allah SWT for His grace and mercy so that I can complete this thesis. To my parents, Abd Majid Ali and Faridah Mohd Said, who have given much encouragement and support. To my beloved wife, Lilly Aizura Mohd Azmi and my daughters, Nur Arissa Damia and Nur Afrina Inara, done a lot of sacrifice with patience throughout my process of completing my thesis.

Do not forget to thank my supervisor, Dr. Sharifah Md Yasin for her guidance and patience. I am very grateful for the guidance and encouragement she has given me throughout this journey. I am indebted to my sponsor, Jabatan Perkhidmatan Awam Malaysia for giving me the opportunity to conduct this research.

I would like to dedicate this thesis special to my late sister, Norhayati Abd Majid who always gives me full support and strength in whatever I did. Without her, I cannot stand where I am now.

To all my lecturers, friends and classmates who always give ideas and suggestions to improve this thesis, thank you very much for all of you. There are no words that can be described every love, patience, joyfulness, strengths, dreams and hope that you gave me during this journey.

APPROVAL FORM

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfillment of the requirement for the degree of Master Information Security. The members of the Supervisory Committee were as follows:

DR. SHARIFAH MD YASIN

Faculty of Computer Science and

Information Technology Universiti Putra

Malaysia

(Supervisor)

Date: June 2018

DECLARATION FORM

Declaration by graduate student

I hereby confirm that:

- This thesis is my original work
- Quotations, illustrations, and citations have been duly referenced
- This thesis has not been submitted previously or concurrently for any other degree at any other institutions
- Intellectual property from the thesis and copyright of thesis are fully-owned by Universiti Putra Malaysia (UPM)
- Written permission must be obtained from supervisor and Deputy Vice- Chancellor (Research and Innovation) before thesis is published in book form
- There is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity was upheld as according to Rule 59 in Rules 2003 (Revision 2013- 2014). The thesis has undergone plagiarism detection software

Signature:_____ Date: _____

Name and Matric No.: NOORHAFEZAN BIN ABD MAJID (GS 49326)

TABLE OF CONTENTS

LIST OF TABLE

LIST OF FIGURE

LIST OF ALGORITHM

LIST OF CODING

CHAPTER 1

INTRODUCTION

1.1 Background

Cloud computing is a method in which data can be stored and accessible regardless of time and place as long as the user device can access to the Internet. Users can also store a personal data or for the working purposes in the cloud storage that provided by the Cloud Service Provider (CSP) and this approach will provide a greater convenience to the user or to a company to save costs without having to buy and maintain a physical storage. It will enhance the cost efficiency of an organization by reducing the logistic to place data centre on premises and hiring the skillful manpower to configure, monitoring the machine. It also reduces the cost of buying high-end appliances or machines and a renewal fee every year.

Cloud computing will generate more comprehensive positive impact by supporting improvements in information technology innovation, support the mission and vision of the business, accelerate the development of fast, mass solutions faster, reducing the time constraints to market new products, and reduce daily operating costs.

Referring to the report produces by Forbes [6], it has shown a significant increase for organizations using cloud computing services as an option for data centre facilities. According to the illustration, it can be shown that the increase in subscriptions to cloud computing services is very high. Analysts predict that

by 2020, the cost and spending of cloud computing will increase almost by 3 times compared to 2015. The graph as shown as Figure 1.1:

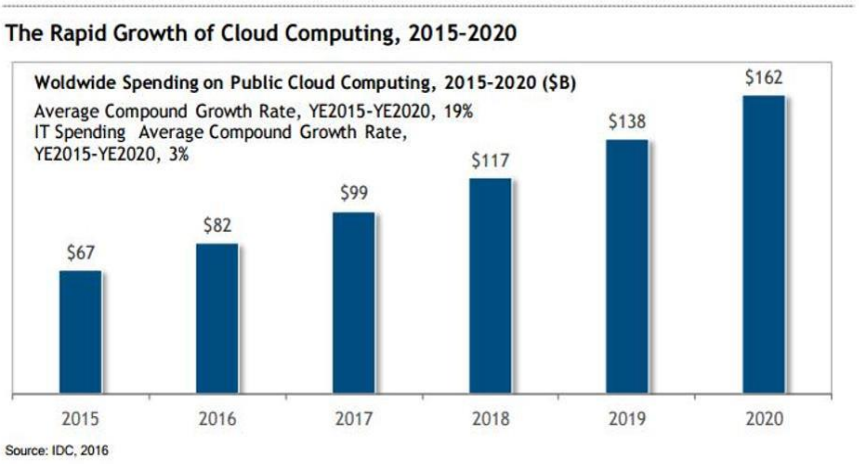

Figure 1.1: The Rapid Growth of Cloud Computing, 2015 -2020 [6]

Referring to the reports from Market Research Future (MRFR) 's report [16], based on Figure 1.2 shows an impressive annual increase as high as 14% for the compound annual growth rate (CAGR) projected from the year 2017 to 2023. Graphs also show global expectations for the cloud object storage market can reach up to USD 6 Billion by 2023. The graph as shown in Figure 1.2

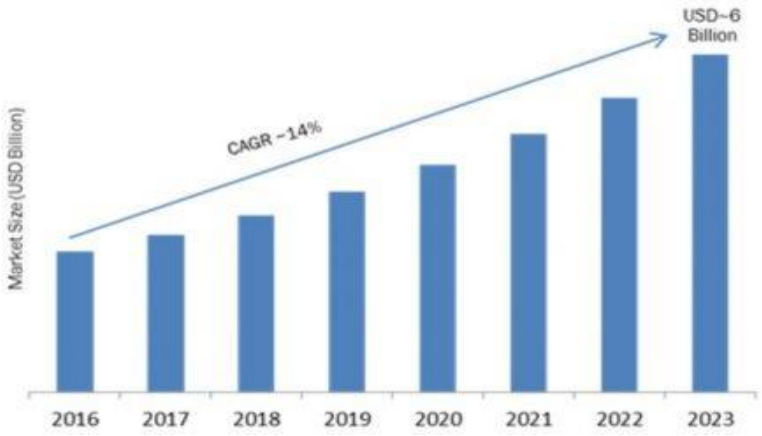

Figure 1.2: Global Cloud Object Storage Market, 2016 -2023 [16]

This significant development is due to several factors such as follow:

a) **Usability:** Ease to use the Cloud Storage for sharing information such as document, music, photo, files and many more.

b) **Bandwidth:** Normally Cloud Service Provider (CSP) will provide sufficient bandwidth to handle their user and client.

c) **Accessibility:** Cloud Storage can be accessed from anywhere and at any time as long as the user can access the internet or Virtual Private Network (VPN).

d) **Disaster Recovery:** Cloud Service Provider (CSP) will enhance their services by getting ready with the disaster recovery plan either for process and infrastructure.

e) **Cost Saving:** Cloud Service Provider (CSP) will provide a cloud storage service that is appropriate and meets the needs of the customer cost.

However, there are still weaknesses and disadvantages in the cloud storage service that can be improved from time to time. Among the shortcomings that often serve as a benchmark for a Cloud Service Provider (CSP) as follows:

a) **Lack of Control:** User or client cannot fully control of the service.

b) **Unknown Location:** Client will be bound to the rules and laws of different countries and pose a risk to data security.

c) **Internal Attack:** Internal attacks can occur either from the Cloud Service Provider (CSP) or any third parties which together exist and share resources in the same cloud storage.

d) **Shared Data Among Group:** Control of internal users who have been removed or departed or future staff that will join the company in the future.

In Naresh *et. al* (2016), emphasize the cloud security challenge in eight (8) different pillars such as below :

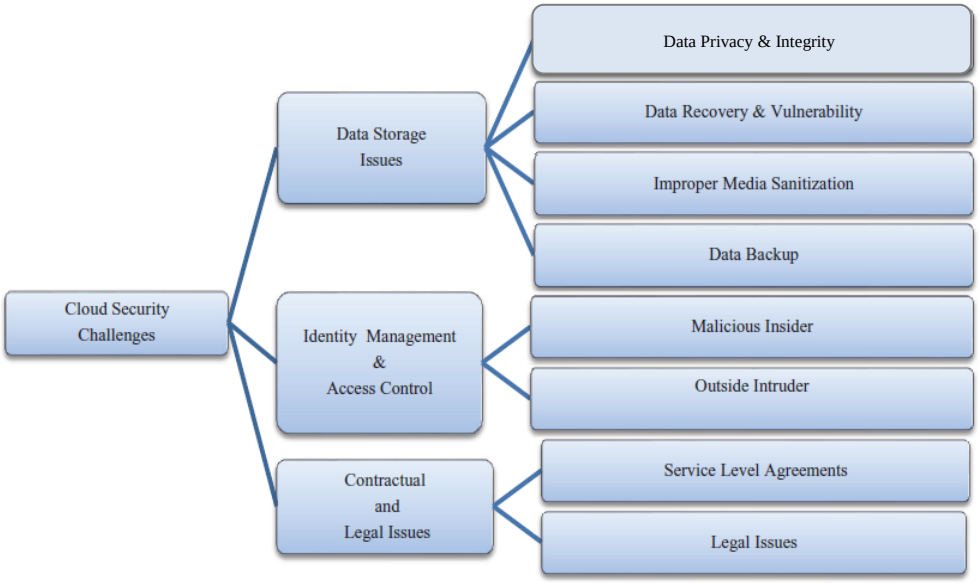

Figure 1.3: Cloud Security Challenges [19]

Based on Figure 1.3, malicious insiders and outsider intruders [19] are categorized as Cloud Security Challenges. Details of the both issue are briefly described as follows:

a) Malicious Insider

An insider threat can be executed from multiple factors such as internal user/staff, vendor, partner, and other organization. In the cloud environment, one of the main issues is multi-tenancy and this approach can create a side

channel attack based on the vulnerability among others. In Figure 3, this issue can be mitigated by implementing an Identity Management and Access Control and based on both of this category, the current research in Ali *et al.* (2017) [2] using a similar method to control the security breaches among the internal users by implementing the access control list.

b) Outside Intruder

The outside attacker usually will use the vulnerability of the network architecture or from the application to penetrate the system and retrieve the data. Based on the Confidentiality, Integrity, and Availability (CIA) concept, the confidentiality can be control by implementing user management and access control but for the availability, it involved the physical security appliances like firewall, intrusion prevention and many more.

1.2 Problem Statement

In Ali *et al.* (2017) Secure Data Sharing in Clouds (SeDaSC) is related to enhance the security control to mitigate the insider attack to access and manipulate the data that was stored in public cloud storage.

Based on this paper, the problem that can be enumerated as per follows:

a) Tests implemented by Ali *et al.* (2017) are conducted from 10 to 100 users only. Therefore, there is no record mentioned for key generation time for users exceeding 100 whether the time increment is directly proportional or exponential (numerous time differences) based on user

additions. If the time recorded is unusually large for increment number of users, then there must be a limitation on the number of users.

b) In P. Singh *et al.* (2018) Secure Data Deduplication Using Secret Sharing Scheme Over Cloud mention in the normal approach, the plaintext with be decrypted with the convergent key and then for each different user, the convergent key will be decrypted with a master key. The master key is different for each user. The number of master key will follow the number of user and if the master key is compromised by the attacker then the data will be lost and cannot to be recovered. Hence this method presents the single point of vulnerability. Same issue can be happened in AES encryption because AES encryption uses a single key only and secret information can be decrypted by using the same key. Secure information can be abused by attackers when the key falls to unauthorized person because of the negligence either by intentionally or unintentionally. This method also will present the single point of vulnerability in the key management. Furthermore the key and the data will be stored in the third party servers that have a potential in compromise in security. The approach to using a single key for decryption may be appropriate for low and medium level secret information. For high-level information, there are two ways either through the asymmetric key or using a method of secret sharing scheme where more than one key is required to decrypt the information. But in order to remain the single key encryption concept, secret sharing scheme is more appropriate to be tested in this research.

1.3 Research Objectives

Based on the problem statement listed in section 1.2, the objectives of this thesis are:

a) To re-execute existing algorithms to prove functionality and to compare the results in terms of key generation times. The algorithm will follow exact algorithms from Ali *et al.* (2017) including random number generator, hash function using SHA-256, and hash based message authentication code (HMAC) on each encrypted file. This test will produce key generation times for 10 to 100 users and the number of users will be enhanced to 500 users for getting the key generation times for large-scale users.

b) To analyze and compare the results between both or these method using the same number of users. Analysis of key generation times in AES and secret sharing scheme are compared. If the time generated by the secret sharing scheme is faster than AES then the secret sharing scheme is more suitable for high secrecy information with large-scale users because secret sharing scheme can control threshold number of key to reconstruct back the ciphertext to the original information. This is also one way to minimize the risk of one single point of vulnerability because if there is a key that leaked into the hands of unauthorized person, the ciphertext is still safe because the threshold is dynamic and can be controlled depending on the degree of secrecy and the number of shares the secrets and keys. In R. Shor *et al.* (2018) also mention that

encrypting the data and dispersing the keys with an efficient secret sharing scheme is optimal for multi-cloud environments.

1.4 Scope and Limitation

The scope of this research is to analyze the key generation times generated by the existing method and to improve the performance by using the secret sharing scheme. The limitation of this project is to conduct the same testing environment as existing method by using High Level Petri Nets, SMT Library, Z3 solver and external cloud storage such as Amazon Web Services (AWS). In this thesis, testing has been implemented using localhost as the role of Cryptographic Server (CS) and does not involve any Cloud Service Provider (CSP) because the service is payable and needs an additional cost.

1.5 Thesis Structure

The structure of this thesis consists of six chapters as follows:

Chapter 1 is about the background of this thesis including problem statement and research objectives. This chapter will be described briefly about the growth of cloud storage, the challenging issue in cloud storage, the existing security approaches in cloud storage and the relevancies of using the cryptographic method in cloud storage.

Chapter 2 will describe a literature review related to this thesis. A literature review is a source of research article and journal that being used to give more understanding about the related topic. From the literature review, it will be as a guideline in the specific research environment. Based on the findings of the previous researcher, it will be helped to generate new idea in this thesis and try to make this research applicable in the industry.

Chapter 3 will discuss the phase of the research methodology involved in this research including the comparison between current research algorithms and the new proposed algorithm. It also acts as a framework to ensure this thesis complete accordingly and follow the objectives mention above.

Chapter 4 will discuss the project implementation and development. In this chapter, the approach used is being explained in detail including the flow chart and algorithm that been used. This chapter also will be discussing the tools, the software and hardware requirement and also the step of running the testing.

Chapter 5 is explaining the result. In this chapter, all the results and findings related to this project will be provided here. An evaluation of the result and the discussion will be explained in this chapter.

Chapter 6 is the conclusion of this thesis. This chapter will describe the achievement, conclusion, suggestion, limitation and future enhancement from this work.

REFERENCES

[1] Keith M. Martin (2017). Two types of cryptosystem. Everyday Cryptography: Fundamental Principles & Applications. 2nd Edition.

[2] M. Ali (2017) "SeDaSC: Secure Data Sharing in Clouds," in IEEE Systems Journal, vol. 11, no. 2, pp. 395-404.

[3] Y. Chen and W. Tzeng (2012). "Efficient and Provably-Secure Group Key Management Scheme Using Key Derivation," in Proc. IEEE 11th Int. Conf. TrustCom. pp. 295–302.

[4] Definition of Cloud Storage. Retrieved from https://www.techopedia.com/definition/26535/cloud-storage

[5] Overview for cloud file sharing. Retrieved from https://searchstorage.techtarget.com/definition/cloud-file-sharing

[6] Cloud Computing Forecast. Retrieved from https://www.forbes.com/sites/louiscolumbus/2017/04/29/roundup-of-cloud-computing-forecasts-2017/#7ddf93431e87

[7] A. N. Khan, M. M. Kiah, S. A. Madani, M. Ali, and S. Shamshir-band (2014) "Incremental Proxy Re-Encryption Scheme For Mobile Cloud Computing Environment," J. Supercomput., vol. 68, no. 2, pp. 624–651.

[8] L. Xu, X. Wu, and X. Zhang (2012). "CL-PRE: A Certificateless Proxy Reencryption Scheme For Secure Data Sharing With Public Cloud," in Proc.7th ACM Symp. Inf., Comput. Commun. Security, pp. 87–88.

[9] S. Seo, M. Nabeel, X. Ding, and E. Bertino. (2013) "An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds," IEEE Trans. Knowl. Data Eng., vol. 26, no. 9, pp. 2107–2119.

[10] Cisco Global Cloud Index: Forecast and Methodology, 2016–2021 White Paper. Retrieved from https://www.cisco.com/c/en/us/solutions/collateral /service-provider/global-cloud-index-gci/white-paper-c11-738085.html

[11]Disadvantages of Cloud Computing. Retrieved from https://cloudacademy.com/blog/disadvantages-of-cloud-computing/

[12] Ramkumar, K.R., & Singh, R.P. (2017). "Key management using Chebyshev polynomials for mobile ad hoc networks." China Communications, 14, 237-246.

[13] 5 advantages and disadvantages of using Cloud Storage. Retrieved from https://bigdata-madesimple.com/5-advantages-and-disadvantages-of-cloud-storage/

[14] Insider Threats as the Main Security Threat in 2017. Retrieved from https://www.tripwire.com/state-of-security/security-data-protection/insider-threats-main-security-threat-2017/

[15] Lim, Bin Yong (2015). "Secret Sharing Schemes and Advanced Encryption Standard" Thesis. Monterey, California: Naval Postgraduate School.

[16] Cloud Object Storage Market 2019 Global Leading Growth Drivers, Emerging Audience, Sales, Profits and Regional Analysis. Retrieved from https://www.reuters.com/brandfeatures/venture-capital/article?id=90456

[17] Roman Shor, Gala Yadgar, Wentao Huang, Eitan Yaakobi, Jehoshua Bruck (2018). "How to Best Share a Big Secret". ACM ISBN 123-4567-24-567/08/06. Association for Computing Machinery.

[18] Priyanka Singh, Nishant Agarwal, Balasubramanian Raman (2018). "Secure data deduplication using secret sharing schemes over cloud". Future Generation Computer Systems. Volume 88, Pages 156-167.

[19] Naresh Vurukonda, B.Thirumala Rao (2016). "A Study on Data Storage Security Issues in Cloud Computing". 2nd International Conference on Intelligent Computing, Communication & Convergence.

[20] M. Bertier, A. Mostefaoui, and G. Tr´edan (2010). “Low-cost secretsharing In sensor networks,” in Proceedings of the IEEE 12th International Symposium on High Assurance Systems Engineering (HASE ’10).

[21] Y.-X. Liu, L. Harn, C.-N. Yang, and Y.-Q. Zhang (2012). “Efficient (n, t, n) secret sharing schemes,” Journal of Systems and Software, vol.85, no. 6, pp. 1325–1332.

[22] S. K. Narad, M. R. Sayankar, S. V. Alone and P. S. Mahiskar (2017). "Secret sharing scheme for group authentication — A review," International conference of Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, pp. 12-16.

[23] S. Pawar, S. El Rouayheb, K. Ramchandran (2011) “Securing Dynamic Distributed Storage Systems Against Eavesdropping and Adversarial Attacks” IEEE Trans. Information Theory, pp.67346753.

[24] K. Iwamura and K. Tokita (2018). "Fast secure computation based on a secret sharing scheme for n < 2k − 1," *2018 Fourth International Conference on Mobile and Secure Services (MobiSecServ)*, Miami Beach, FL, pp. 1-5.

[25] Shingu T., Iwaumura K. and Kaneda K. (2016). “Secrecy computation without changing polynomial degree in Shamir’s (K, N) secret sharing scheme” In Proceedings of the 13th International Joint Conference on e-Business and Telecommunications - Volume 1: DCNET, (ICETE 2016).

[26] A. Waseda and R. Nojima (2012). “Consideration for IT-secure password protected secret sharing, (in Japanese)” IEICE Technical Report 2011-79.

[27] W. Ogata, “Improvement of IT-secure password-protected secret sharing, (in Japanese)” the 30th symposium on cryptography and information security, Jan. 22-25, 2013.

[28] S. Takahashi, H. Kang and K. Iwamura (2014). "Asymmetric secret sharing scheme suitable for cloud systems," 2014 IEEE 11th Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, pp. 784-790.

[29] Abdelrahman, Ahmed & Fouad, Mohamed & Dahshan, Hisham. (2017). Analysis on the AES Implementation with Various Granularities on Different GPU Architectures. Advances in Electrical and Electronic Engineering. 15. 10.15598/aeee.v15i3.2324.

[30]Understanding Shamir’s Secret Sharing. Retrieved from https://medium.com/vault12/understanding-shamirs-secret-sharing-6a4bd27768c9

[31] K. Tsujishita and K. Iwamurra (2018). "Password-protected secret sharing scheme with the same threshold in distribution and restoration," 2018 Fourth International Conference on Mobile and Secure Services (MobiSecServ), Miami Beach, FL, pp. 1-5.

[32] P. R. Kamble and S. Patil (2018). "Exploring secret image sharing with embedding of shares," 2018 2nd International Conference on Inventive Systems and Control (ICISC), Coimbatore, pp. 1090-1093.

[33] Monica G. Charate, Dr. Savita R. Bhosale (2015). "Cloud Computing Security Using Shamir's Secret Sharing Algorithm From Single Cloud To Multi Cloud". International Journal of Advanced Technology in Engineering and Science. Volume No 03, Special Issue No. 01.