UNIVERSITI PUTRA MALAYSIA

AN EFFICIENT CRIME GROUP OF SECURED DATA SHARING SCHEME IN CLOUD

MUSTAFA NOORI RASHID

FSKTM 2018 57

AN EFFICIENT CRIME GROUP OF SECURED DATA SHARING SCHEME IN CLOUD

By

MUSTAFA NOORI RASHID

Thesis Submitted to the School of Graduate Student, University Putra Malaysia, in Fulfillment of the Requirement for the Degree of Master of Computer Science

2018

COPYRIGHT

DEDICATION

This thesis is dedicated to:

I dedicate this project to God Almighty my creator, my strong support, my source of inspiration, wisdom, knowledge and understanding. He has been the source of my strength throughout this project and on his wings only have I soared.

My father, who taught me that the best kind of knowledge to have is that which is learned for its own sake. It is also dedicated to my mother, who taught me that even the largest task can be accomplished if it is done one step at a time.

I also dedicate this work to my wife; who has encouraged me all the way and whose encouragement has made sure that I give it all it takes to finish that which I have started. To my children, they will be my future. Thank you. My love for you all can never be quantified. God bless you.

ABSTRACT

Abstract of the thesis presented of the Senate of University Putra Malaysia fulfillment of the requirement for the degree of Master of Science.

An Efficient Crime Group of Secured Data Sharing Scheme in cloud

By

Mustafa Noori Rashid

2018

Supervisor: Dr. Ahmad Alauddin Ariffin

Faculty: Computer Science and Information Technology

The importance of cloud computing is the users can accomplish an effective and economical approach for data sharing among group members in the cloud with the characteristics of low maintenance and little management cost. Cloud security is a part of computer security. Data confidentiality requires that unauthorized users including the cloud are incapable of learning the content of the stored data. Maintenance of the availability of data confidentiality for dynamic groups is still an important and challenging issue. The cloud provider cannot be treated as a trusted third party (cloud storage services) because of its semi-trust nature, and thus the traditional security

models cannot be straight forwardly generalized into cloud based group sharing frameworks. We propose a crime group of information sharing framework for cloud, which can effectively take advantage of the cloud servers' help but have no sensitive data being exposed to attackers and the cloud provider. By applying the proxy signature technique, the group leader can effectively grant the privilege of group management to one or more chosen group members. By adopting proxy re-encryption, most computationally intensive operations can be delegated to cloud servers without disclosing any private information. Extensive security and performance analysis shows that our proposed scheme is of high efficiency and satisfies the security requirements for public cloud-based secure groups.

ABSTRAK

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia

Sebagai memenuhi keperluan untuk ijazah Sarjana Sains

An Efficient Crime Group of Secured Data Sharing Scheme in cloud

By

Mustafa Noori Rashid

July 2018

Pengerusi: Dr. Ahmad Alauddin Ariffin

Fakulti: Sains Komputer dan Teknolologi Maklumat

Kepentingan pengkomputeran awan ialah pengguna dapat mencapai pendekatan yang berkesan dan ekonomi untuk perkongsian data di kalangan ahli kumpulan dalam awan tersebut dengan ciri-ciri penyelenggaraan yang rendah dan kos pengurusan yang kecil. Keselamatan awan adalah sebahagian daripada keselamatan komputer. Kerahsiaan data memerlukan agar pengguna yang tidak dibenarkan termasuk awan tidak berupaya mengetahui kandungan data yang disimpan. Pengekalan kerahsiaan data untuk kumpulan dinamik masih menjadi isu penting dan mencabar. Penyedia awan

tidak boleh dianggap sebagai pihak ketiga yang dipercayai (perkhidmatan penyimpanan awan) kerana sifat separa-amanahnya, dan oleh itu model keselamatan tradisional tidak boleh diambil secara terus menerus sebagai anggapan umum ke dalam rangka kerja perkongsian kumpulan berasaskan awan. Kami mencadangkan kumpulan rangka kerja perkongsian maklumat jenayah untuk awan, yang dapat secara berkesan memanfaatkan bantuan pelayan awan tetapi tidak menyebabkan data sensitif terdedah kepada penyerang dan penyedia awan. Dengan menggunakan teknik tandatangan proksi, ketua kumpulan dapat dengan berkesan memberi keistimewaan pengurusan kumpulan kepada satu atau lebih ahli kumpulan yang terpilih. Dengan mengguna pakai penyulitan-semula proksi, kebanyakan pengendalian komputasi yang intensif boleh ditugaskan kepada pelayan awan tanpa mendedahkan apa-apa maklumat peribadi. Analisis keselamatan dan prestasi yang menyeluruh menunjukkan bahawa skim cadangan kami berciri kecekapan tinggi dan memenuhi keperluan keselamatan untuk kumpulan berasaskan-awan yang selamat.

ACKNOWLEDGMENTS

First and foremost, praises and thanks to the God, the Almighty, for His showers of blessings throughout my project work to complete the work successfully.

Apart from the efforts of myself, the success of any project depends largely on the encouragement and guidelines of many others. I take this opportunity to express my gratitude to the people who have been instrumental in the successful completion of this project.

I would like to show my greatest appreciation to Dr. Ahmad Alauddin Ariffin, for his supervision, advice, and guidance, where his office door was always open whenever I confront into a trouble spot or had a question about my research or writing. I feel motivated and encouraged every time I attend his meeting. Without his encouragement and guidance this project would not have achieved. The guidance and support received from Dr. Ahmad was vital for the success of the project. I am grateful for his constant support and help. Thank him from depths my heart.

I must express my very profound gratitude to my dear wife for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of researching and writing this thesis. This accomplishment would not have been possible without her. Thank her.

I am extremely grateful to my parents and my family wife for their love, prayers, caring and Sacrifices for educating and preparing me for my future. My Special thanks goes to my age friend Mohammed Hoobi Mutar for the intense interest shown to complete this project successfully.

Finally, my gratitude to the Malaysian people in general for their perfect hospitability in their blue sky and green land during my study period. Thanks Malaysia.

APPROVAL

This thesis submitted to the faculty of Computer Science and Information Technology of University Putra Malaysia and has been accepted as partial fulfillment of the requirement for the degree of Master of Computer Science.

The member of the Supervisory Committee were as following:

Supervisor: Dr. Ahmad Aladdin Ariffin

Department of Communication of Technology and Network

Faculty of Computer Science and Information Technology

University Putra Malaysia

Date and Signature: _____

Assessor: Dr. Amir Rizaan Rahiman

Department of Communication of Technology and Network

Faculty of Computer Science and Information Technology

University Putra Malaysia

Date and Signature: _____

DECLARATION

I declare that the thesis is my original work except for quotation and citations which have been duly acknowledge. I also declare that it has not been previously, and is not concurrently, submitted for any other degree at University Putra Malaysia or other institution.

Mustafa Noori Rashid

Data_____

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

TSGSF	Traditional Secure Group Sharing Frame work
CDSGSF	Crime Dynamic Secure Group Sharing Frame work
API	Application Programming Interface
CSP	Cloud Service Provider
SaaS	Software as a Service
VM	Virtual Machine
VMs	Virtual Machine Services
RAM	Random Access Memory
CIS	Cloud Information Services
PRE	Proxy Re-Encryption
DH	Diffie-Hellman
IBM	International Business Machines Corporation
DEK	Data Encryption Key
CP-ABE	Ciphertext Policy Attribute-Based Encryption
EABDS	Efficient Attribute-Based Secure Data Sharing Scheme

SAPA	Shared Authority Based Privacy Preserving Authentication
UC	Universal Composability
ID-Based	Identity-Based
TGDH	Tree Based Group Diffie-Hellman
TGKM	Time-based Group Key Management
CIBPRE	Conditional Identity-Based Broadcast Proxy Re-Encryption
AES	Advanced Encryption Standard
SHA algorithm	Secure Hash Algorithm
MD-5	Message Digest
IT	Information Technology
IDE	Integrated Development Environment
MySQL	My Structured Query Language
CA	Certificate Authorities
CPU	Central Processing Unit
LR	Literature Review

CHAPTER 1

INTRODUCTION

1.1. Overview

In this Chapter, We Introduce a review of cloud computing, a brief background about the scope of this thesis, an idea about our research problem and how it has been addressed our objective, and the outline of the thesis chapters.

1.2. Cloud Computing

Cloud computing is a general term used to describe a new class of network based computing that takes place over the Internet, basically a step on from utility computing a collection/group of integrated and networked hardware, software and Internet infrastructure (called a platform).Using the Internet for communication and transport provides hardware, software and networking Services to clients these platforms hide the complexity and details of the underlying infrastructure from users and applications by providing very simple graphical interface or Applications Programming Interface (API).In addition, the platform provides on demand services that are always on, anywhere, anytime and anyplace. Pay for use and as needed, elastic, scale up And down in capacity and functionalities. The hardware and software services are available to general public, enterprises, corporations and businesses markets [40].

The cloud computing provides on demand services over the Internet with the help of a large amount of virtual storage. The main features of cloud computing is that the user does not have any setup of expensive computing infrastructure and the cost of its services is less. In the recent years, cloud computing integrates with the industry and many other areas, which has been encouraging the researcher to research on new related technologies. Due to the availability of its services &

scalability for computing processes individual users and organizations transfer their application, data and services to the cloud storage server. Regardless of its advantages, the transformation of local computing to remote computing has brought many security issues and challenges for both consumer and provider [41].

Cloud offers massive opportunity for new innovation, and even disruption of entire industries. Cloud computing is the long dreamed vision of computing as a utility, where data owners can remotely store their data in the cloud to enjoy on demand high-quality applications and services from a shared pool of configurable computing resources. Identity privacy is one of the most significant obstacles for the wide deployment of cloud computing. Cloud systems can be used to enable data sharing capabilities and this can provide several benefits to the user and organization when the data shared in cloud. Since many users from various company contribute their data to the Cloud, the time and cost will be less compared to manually exchange of data. By migrating the local data management systems into cloud servers, users can enjoy high-quality services and save significant investments on their local infrastructures [33] [39].

Due to the benefits of cloud computing, increasingly more users have been using public cloud storage for data storing and sharing. However, for the widespread adoption of public cloud storage services, public cloud storage should solve the critical issue of data confidentiality. That is, the sensitive data must be secured from the unauthorized accesses. To protect the confidentiality of the sensitive data, a common approach is to encrypt the data before uploading them to the cloud. Since the Cloud Service Provider (CSP) does not know the keys used to decrypt the encrypted data, the confidentiality of the data is assured. However, traditional encryption technique brings many inconveniences for data sharing between different users. To share the encrypted data with a friend, a data owner has to download his data from the storage server, decrypt them, re-encrypt them using

his friend's public key and then send the re-encrypted data to his friend or re-upload the re-encrypted data to the cloud. Obviously, this strategy is extremely inefficient due to the heavy overhead at the data owner. In addition, it loses the merit of the public cloud storage. Therefore, how to flexibly share the encrypted data stored in clouds becomes a challenge [4].

Cloud computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services. The services themselves have long been referred to as Software as a Service (SaaS). The datacenter hardware and software is what we will call a Cloud. When a cloud is made available in a pay-as-you-go manner to the general public, we call it a public cloud; the service being sold is utility computing. We use the term private cloud to refer to internal datacenters of a business or other organization, not made available to the general public. Thus, cloud computing is the sum of SaaS and utility computing, but does not include private clouds. People can be users or providers of SaaS, or users or providers of utility computing [43].

The importance of Cloud Computing is the users can accomplish an effective and economical approach for data sharing among group members in the cloud with the characters of low maintenance and little management cost. Cloud security is a part of computer security. It describes set of policies, technology, and control that is helpful to protect the data and services .The threats and attacks directly or indirectly affect the cloud system. Integrity, availability and confidentiality of the cloud resources as well as service of different layers are breach that may be raised new security concern. Cloud Computing means more than simply saving on Information Technology (IT) implementation costs. One of the most fundamental services offered by cloud providers is data storage. A company allows its staffs in the same group or department to store and share files in the cloud. By utilizing the cloud, the staffs can Cloud Computing, Data Sharing, Dynamic Groups, Integrity, Privacy-

preserving, Reliability, Scalability be completely released from the troublesome local data storage and maintenance. However, it also poses a significant risk to the confidentiality of those stored files [7] [10].

1.3. Cloud Computing Applications

There are various applications of cloud computing in today's network world. Many search engines and social websites are using the concept of cloud computing like www.amazon.com, hotmail.com, facebook.com, linkedln.com etc. the advantages of cloud computing in context to scalability is like reduced risk , low cost testing ,ability to segment the customer base and auto-scaling based on application load [46].

The applications of cloud computing are practically limitless. With the right middleware, a cloud computing system could execute all the programs a normal computer could run. Potentially, everything from generic word processing software to customized computer programs designed for a specific company could work on a cloud computing system. Clients would be able to access, their applications and data from anywhere at any time. They could access the cloud computing System using any computer linked to the Internet. Data wouldn't be confined to a hard drive on one user's computer or even a corporation's internal network. It could bring hardware costs down [16].

Cloud computing systems would reduce the need for advanced hardware on the client side. You wouldn't need to buy the fastest computer with the most memory, because the cloud system would take care of those needs for you. Instead, you could buy an inexpensive computer terminal. The terminal could include a monitor; input devices like a keyboard and mouse adjust enough processing power to run the middleware necessary to connect to the cloud system. You wouldn't need a large hard drive because you'd store all your information on a remote computer. Corporations that rely on

computers have to make sure they have the right software in Place to achieve goals. Cloud computing systems give these organizations company-wide access to computer applications. The companies don't have to buy a set of software or software Licenses for every employee. Instead, the company could pay a metered fee to a cloud computing company [45].

Servers and digital storage devices take up space. Some companies rent Physical space to store servers and databases because they don't have it available on site. Cloud Computing gives these companies the option of storing data on someone else's hardware, removing the Need for physical space on the front end. Corporations might save money on IT Support. Streamlined hardware would, in theory, have fewer problems than a network of Heterogeneous machines and Operating System. If the cloud computing system's back end is a grid computing system, then the client could take advantage of the entire networks processing power. Often, scientists and researchers work with calculations so complex that it would take years for individual computers to complete them. On a grid computing system, the client could send the calculation to the cloud for processing. The cloud system would tap into the processing power of all available computers on the back end, significantly speeding up the calculation [43].

1.4. Cloud storage

Cloud storage is a typical service model of online outsourcing storage where data is stored virtualized pools which are generally hosted by third parties. Companies need only pay for the storage they actually use. But when data is stored into cloud, user simultaneously loses the control of his data. It makes that the unauthorized accesses from hackers even cloud service providers is inevitable. Security is one of the most important problems that should be addressed in cloud storage applications. In recent years, many scholars have proposed the use of encryption methods to protect users' privacy in cloud storage applications.

In cryptographic cloud storage application framework data owner encrypts files before outsourcing to protect his privacy. Because the authorized users have the key, they could decrypt the files after downloading. Obviously, unauthorized users, attackers, even the cloud service provider can't breach user's privacy without authentication. In cryptographic cloud storage, data owner need not only store files on the cloud but also shares these files to some group users. Therefore, group key management is an important in cloud storage [42].

Cloud computing of storage is a modern and unprecedented service that store resources such as data and applications, and share them between various devices via a network by using the concepts of virtualization, storage, connectivity, and processing power .the benefits of cloud computing, such as unlimited storage, automatic software integration, quick deployment and being the most cost efficient method to use, maintain and upgrade resources [1].

1.5. Cloud Deployment Models

There are four deployment models of cloud computing: public, private, community and hybrid as shown in Fig. 1. Each of these models has different characteristics and implications for the customers [16].

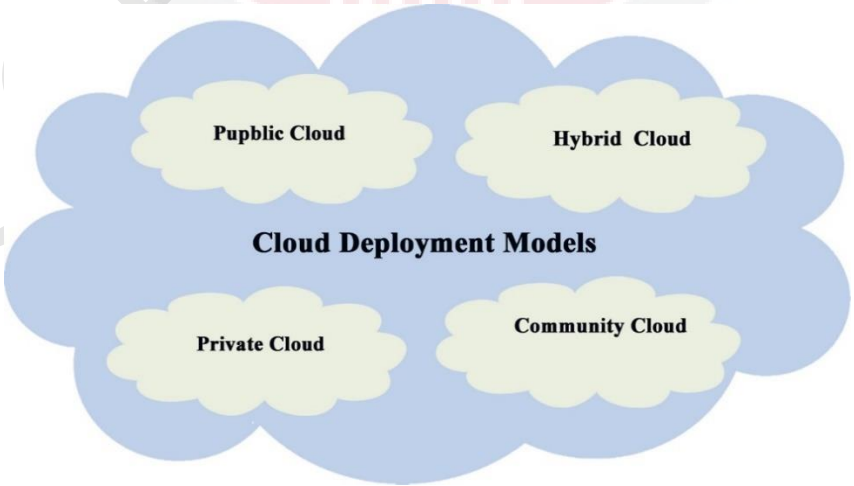

Fig. 1.1. Deployment Models for Cloud Computing.

❖ **Public Cloud**

The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services [16].

Basic Characteristics:

•Homogeneous infrastructure

•Common policies

•Shared resources and multi-tenant

•Leased or rented infrastructure

•Economies of scale

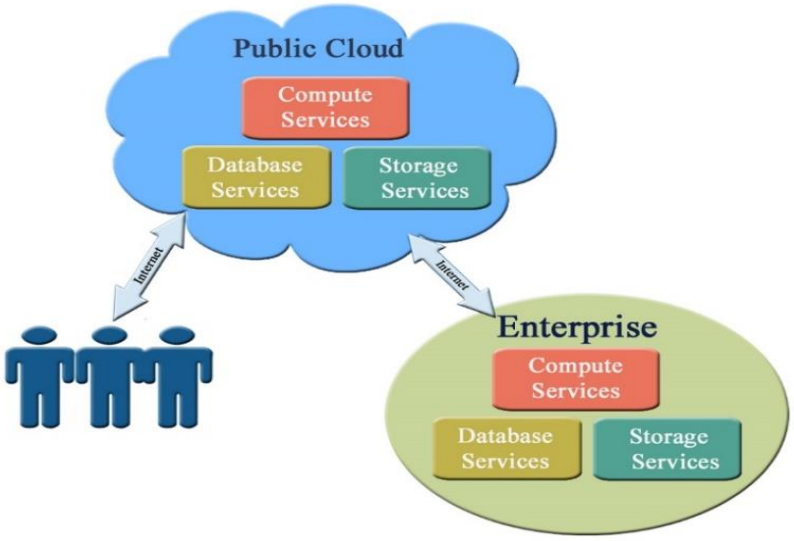

Fig. 1.2. Public Cloud of Computing.

❖ **Private Cloud**

The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise [16].

Basic Characteristics:

•Heterogeneous infrastructure

•Customized and tailored policies

•Dedicated resources

•In-house infrastructure

•End-to-end control

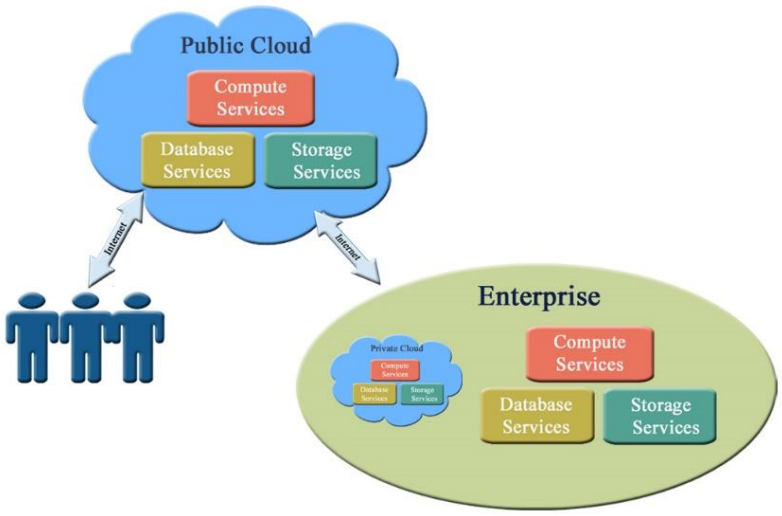

Fig. 1.3. Private Cloud of Computing.

❖ **Community Cloud**

The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy and compliance considerations) [16].

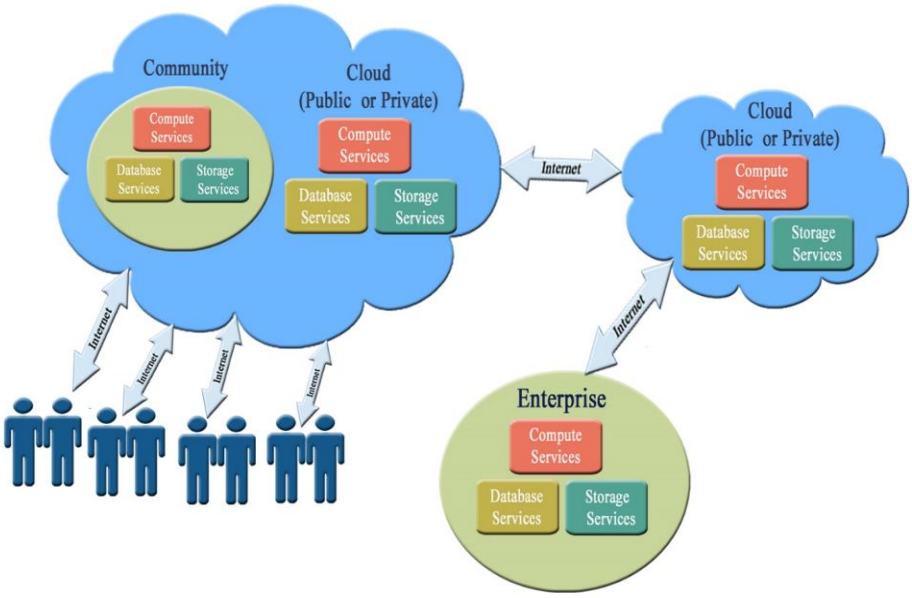

Fig. 1.4. Community Cloud of Computing.

❖ **Hybrid Cloud**

The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds) [16].

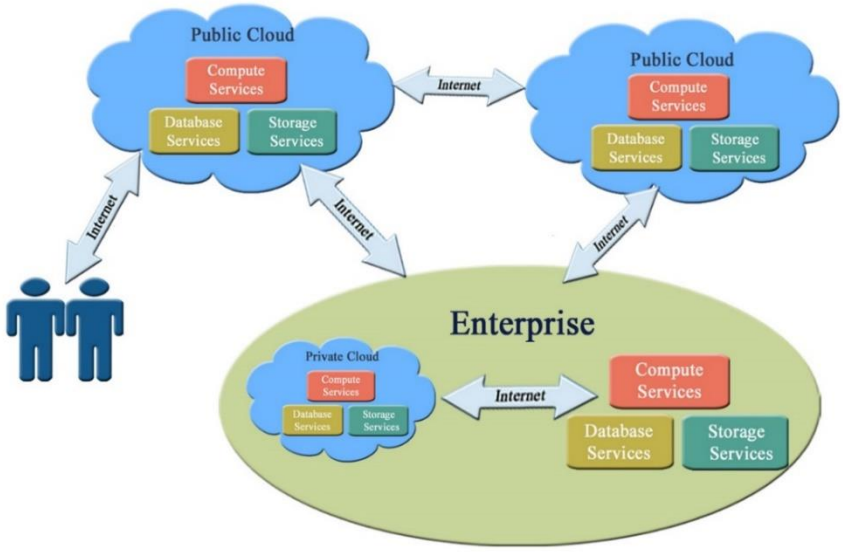

Fig. 1.5. Hybrid Cloud of Computing.

1.6. CloudSim Architecture

CloudSim is simulation software which enables to work on cloud computing experiments. It is a Simulation application which enables seamless modeling, simulation, and experimentation of cloud computing and application services .Due to the problem that existing distributed system Simulators were not applicable to the cloud computing environment. Evaluating the performance of cloud provisioning policies, services, application workload, models and resources Performance models under varying system, user configurations and requirements is difficult to achieve. To overcome this challenge, cloudSim can be used [23].

Motivation: provides a generalized and extensible simulation framework that enables modeling, simulation and experimentation of emerging cloud computing infrastructure application services [44].

User Interface Structure:

Cloudlet: This class models the cloud based application services.

VM: This class models a virtual machine, which is managed and hosted by cloud host component [44].

VM Services:

Cloudlet Execution: Used to support modeling of other performance and composition metrics for applications such as transactions in data base oriented applications.

VM Management: The VM management stands for the Operations control policies related to VM life cycle such as provisioning a host to VM, VM creation, VM destruction & VM Migration [44].

Cloud Services:

VM provisioning: The process of creating VM instances on hosts.

CPU Allocation: CPU is allocated to each of the services.

Memory Allocation: Memory is allocated to the host.

Storage Allocation: Storing of data or service is managed.

Bandwidth Allocation: This is an abstract class that models the policy for provisioning of bandwidth to VMs [44].

Cloud Resources:

Event Handling: This is an abstract class represents the provisioning policy for allocating primary memory (RAM) to the VMs.

Cloud Coordinator: This abstract class extends a cloud based datacenters to the federation .It is responsible for periodically monitoring the internal state of datacenter resources and based on that it undertakes dynamic load-shredding decisions [44].

Sensor: This interface must be implemented to instantiate a sensor component that can be used by a cloud Coordinator for monitoring specific performance parameters.

Applications of Cloudsim:

The growing popularity and importance of cloud computing, several external researchers around the world have started using cloudsim.

Cloudsim Feature: Support for modeling and simulation of large scale cloud computing datacenters. Energy aware computational resources. Support for data center network datacenter topologies and message passing applications. Support for dynamic insertion of simulation elements, stop and resume of simulation. Support for user defined policies for allocation of host to virtual machines and policies for allocation of host resources to virtual machines [44].

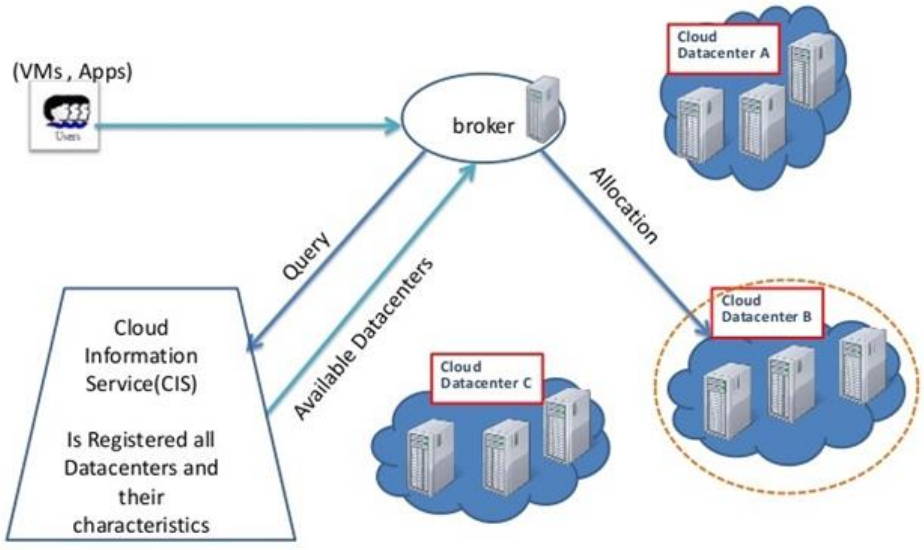

Fig. 1.6. General Overview of CloudSim Process.

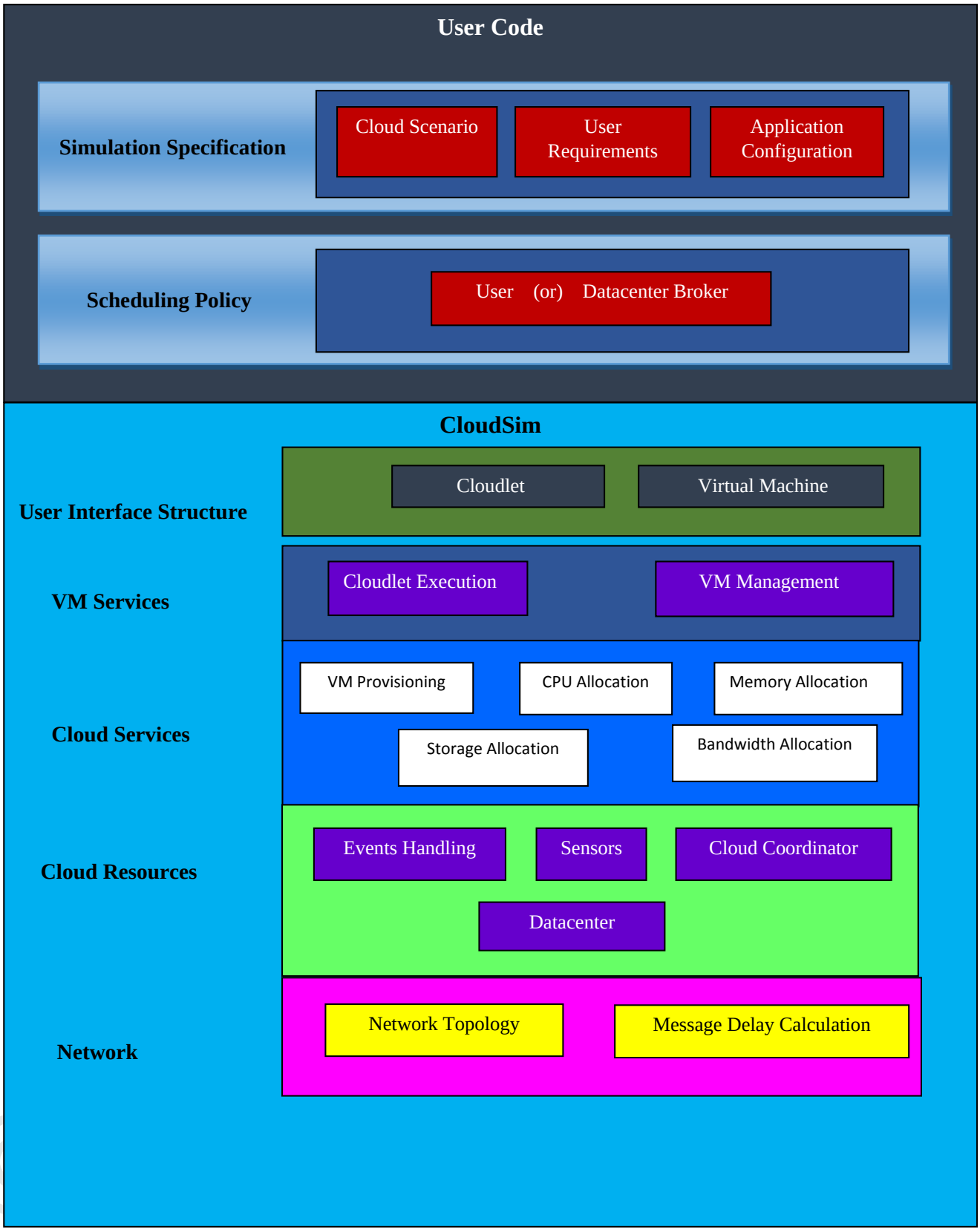

Fig. 1.7. Cloudsim Core Simulation Engine.

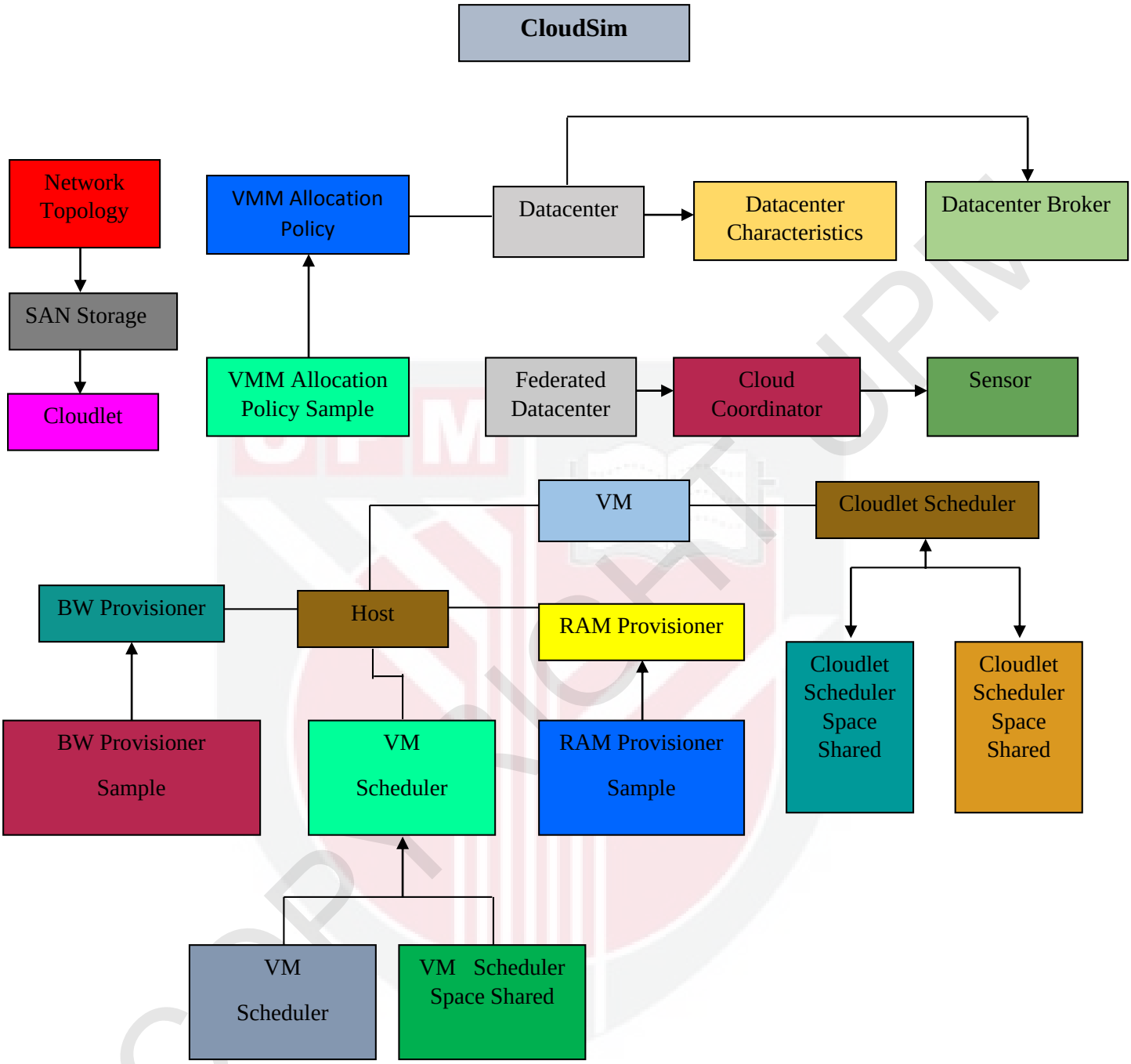

Fig. 1.8. Generation Process

1.7. Problem Definition

Cloud registering is being received at a fast rate in light of the fact that it has an expansive number of upsides for a wide range of organizations and builds effectiveness. Ventures are diminishing stockpiling expenses by utilizing online stockpiling arrangement suppliers. This permits the endeavor to store enormous measures of information on outsider servers. One of the real points of interest is that the stockpiling limit is versatile and therefore, the undertaking pays for the measure of capacity that it needs. Moreover, access to the information is accessible through any Internet association [20].

The isolation and reliability group of apportion information have become two major issues of cloud Computing. [22] The cloud provider cannot be considered as a consign third-party because of its semi-trust nature, and thus the standard reliability models cannot be understood to make a general into cloud based group allocate frameworks. [1] The reliability of the satisfied information increases the encryption charge for the owner. Cryptography is the important to achieving reliability by encrypting/encoding result to make them non understanding information, the Actions of encoding plain text messages into cipher text messages is known as encryption, there are multiple methods to encrypt the data.

Encryption of the data is the method to save the data from harmful and unapproved users, encryption of the record could be more than one layer, many layer of the encryption. Private information needs that unapproved users including the clouds are incapable of learning the contents of the stored data. To keep up the obtained of data private for dynamic groups is still a major and testing issue. [6]Cloud computing, users can reach a powerful and energy saving approach for information sharing among group members in the cloud with the characters requiring little work to keep in good condition and little management cost. Meanwhile, we must provide privacy assurance for the sharing information

files since they are outsourced.[8][12] regrettably, because of the continual make different membership, sharing information while providing isolation-preserving is still a demanding concern, mainly for a untrusted cloud due to the scheming attack? [13]Moreover, conventional privacy sharing framework schemes, the reliability of key distribution is based on the safe communication channel, however, to have such channel is a strong notion and is difficult for practice [5].

1.8. Objective

The data owners want to prevent the server and unauthorized users from learning the contents of their sensitive files. Each of them owns a privacy policy. In particular, the proposed scheme has the following objectives:

Fine grained access control: Dissimilar users can be approval to read different sets of files. This schemes are commonly used in cloud computing. In this type of schemes, each data item is given its own access control policy. The entity that wants to entrance the data item needs to give its quality to a policy obligation. In a cloud environment, normally, the policy obligation is not the admin of the data. The access control policies and the quality might disclose some information that the policy obligation is not entitled to know. This is proposes a fine-grained entry control method. It stops the policy obligation from understand the access control policies and the quality by using cryptographic methods. Compared with the existing schemes, the proposed scheme gives higher level isolation.

Flexible policy specification: The complex data access policies can be specified in a flexible manner. Multiple-owner manner is more workable than single owner manner as multiple owners manners allow every member in the group should be capable to alter their own information. Each part will be ready to examine the information as well as adjust the piece of information in whole information document, though single owner way allow just group admin to store and alter information in the

cloud and individuals can just read the information. The combination of new staff and revocation of current member of staff makes the group active in nature. The common variations of membership make capable and secure data sharing in cloud very complex and hard due to the next two primary reasons: We can decide users not receive to learn the satisfied of data files stored before their present by the unstated system, since it not possible for new accept users to openly contact with data owners and get the complement decryption keys. Second, to reduce the difficulty of key management, it is required to get a methodical membership revocation mechanism without updating the private keys of the present users. There are more than a few security methods that have been planned up-to-date for capable and secure data sharing on untrusted servers. In all of these the encrypted data files are stored in untrusted storage and allocate the complement decryption keys only to approved users by the data owners. But, the concerns of user decision and multiple-owner manner have not been inscribing very expense.

Scalability: To carry a large and random number of users, the system should be highly scalable, in terms of complexity in key management, user management, and computation and storage. We provide a secure way for key distribution without any secure communication channels. The users can securely obtain their private keys from group manager without any certificate authorities due to the verification for the public key of the user.

Our method can reach fine-grained ingress control, with the help of the group user list, any user in the group can use the source in the cloud and revoked users cannot access the cloud furthermore after they are revoked. The proposed method using secure information sharing scheme which can be secure from complicity attack. The rescinded users can not be able to get the original data information once they are rescinded even if they conspire with the untrusted cloud. Our Proposed method can achieve secure user revocation with the help of polynomial function. Our scheme is able

to support dynamic groups' expense when a new user joins in the group or a user is rescinded from the group; the private keys of the other users do not need to be recomputed and updated. We provide security dissection to prove the security of our scheme. In addition, we also perform simulations to demonstrate the efficiency of our scheme.

1.9. Project Scope

Cloud computing, users can achieve an effective and economical approach for data sharing among group members in the cloud with the characters of low maintenance and little management cost. Meanwhile, we must provide security guarantees for the sharing data files since they are outsourced. Unfortunately, because of the frequent change of the membership, sharing data while providing privacy-preserving is still a challenging issue, especially for an untrusted cloud due to the collusion attack. Moreover, for existing schemes, the security of key distribution is based on the secure communication channel, however, to have such channel is a strong assumption and is difficult for practice. We propose an efficient crime secure data sharing scheme for dynamic members. Firstly, we propose a secure way for key distribution without any secure communication channels, and the users can securely obtain their private keys from group manager. Secondly, our scheme can achieve fine-grained access control; any user in the group can use the source in the cloud. Thirdly, we can protect the scheme from collusion attack, which means that revoked users cannot get the original data file even if they conspire with the untrusted cloud. In our approach, by leveraging polynomial function, we can achieve a secure user revocation scheme. Finally, our scheme can achieve fine efficiency, which means previous users need not to update their private keys for the situation either a new user joins in the group or a user is revoked from the group. Our scheme is able to support dynamic groups efficiently, when a new user joins in group or a user is revoked from the group; the private keys of the other users do not need to be.

1.10. Motivation

Proxy Re-Encryption (PRE) schemes are cryptosystems which allow a proxy who has a re-encryption key to convert a ciphertext originally encrypted for one party into a ciphertext which can be decrypted by another party [19].

Proxy signature schemes allow a proxy signer to generate a proxy signature on behalf of an original signer. However, since in previous proxy signature schemes a proxy signature is created on behalf of only one original signer, these schemes are referred to as proxy mono-signature schemes [25].

Diffie-Hellman (DH) schemes for authenticated key exchange are designed to provide a pool of players communicating over an open network or over a public channel with a shared secret key which may later be used to achieve some cryptographic goals [26].

Our motivation is to combine Proxy Signature, Diffie-Hellman (DH) and Proxy Re-Encryption together into a protocol to effectively grant the privilege of group management to negotiate and update the group key pairs to find optimize solution to overcome the limitations.

1.11. Organization of Thesis

The first chapter presents the background of the subject, explains the problem and the purpose of the thesis, and defines the research methodology applied. The second chapter starts with presenting Literature Review (LR) in the cloud and evaluating their features and security approaches. The third chapter starts with presenting methodology for file sharing in the cloud and evaluating their features and security approaches. The **f**ourth chapter presents the results of evaluation and analysis of the proposed system in terms of two measurements; Number of Data and Execution Time. The fifth chapter presents the Conclusion and Future work.

REFERENCES

[1] F. F. Moghaddam, S. D. Varnosfaderani, I. Ghavam, and S. Mobedi, "A client-based user authentication and encryption algorithm for secure accessing to cloud servers based on modified Diffie-Hellman and RSA small-e," in *Proceeding - 2013 IEEE Student Conference on Research and Development, SCOReD 2013*, vol. 16–17, no. December, I. Ghavam, Ed. kuala lumpur: human press, 2015, pp. 179–180.

[2] S. Jain, C. W. Hutchings, Y. T. Lee, and C. R. McLean, "A knowledge sharing framework for homeland security modeling and simulation," *Proc. - Winter Simul. Conf.*, no. CI, pp. 3460–3471, 2010.

[3] S. Chandrasekhar, A. Ibrahim, and M. Singhal, "A novel access control protocol using proxy signatures for cloud-based health information exchange," *Comput. Secur.*, vol. 67, no. 27–62016, pp. 38–41, 2017.

[4] Y. Lu and J. Li, "A pairing-free certificate-based proxy re-encryption scheme for secure data sharing in public clouds," *Futur. Gener. Comput. Syst.*, vol. 62, pp. 140–147, 2016.

[5] K. Liang *et al.*, "A secure and efficient Ciphertext-Policy Attribute-Based Proxy Re-Encryption for cloud data sharing," *Futur. Gener. Comput. Syst.*, vol. 52, pp. 95–108, 2015.

[6] Z. Zhu and R. Jiang, "A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud," *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 1, pp. 40–50, 2016.

[7] J. Dangur and S. M. Jaybhaye, "Public Cloud Secure Group Sharing and Accessing in Cloud Computing," vol. 8, no. 15, pp.1-7 2015.

[8] S. I. S. Hussain, D. F. A. Based, and F. Proxy, "an Assessment on Various Secure Data Sharing Methods in Public Cloud," vol. 1, no. 8, pp. 694–697, 2015.

[9] J. Pingat and S. Mandwade, "An Efficient And Secure Data Sharing By Preventing Collusion Attack In Cloud," no. February, pp. 1–5, 2017.

[10] A. Singh and K. Chatterjee, "Cloud security issues and challenges: A survey," *J. Netw. Comput. Appl.*, vol. 79, no. November 2016, pp. 88–115, 2017.

[11] Jueeli Dangur and S. M. Jaybhaye, "Framework for Secure Data Sharing In Dynamic Group Using Public Cloud," vol. 12, no. 10, pp. 199–204, 2016.

[12] M. Caroline Kayalvizhi and R* Vinupriya "Group Key Management for Dynamic Groups in Public Cloud." vol. 2, no. 1, pp. 22–26, 2016.

[13] R. Sandhu, R. Krishnan, J. Niu, and W. H. Winsborough, "Group-centric models for secure and agile information sharing," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 6258 LNCS, pp. 55–69, 2010.

[14] J. R. Aparna and S. Ayyappan, "Image watermarking using Diffie Hellman key exchange algorithm," *Procedia Comput. Sci.*, vol. 46, no. Icict 2014, pp. 1684–1691, 2015.

[15] G. K. Pradhan, S. Biswas, and B. Puthal, "P Roposed Information Sharing Security Approach for Security Personnels , Vertical Integration , Semantic Interoperability Architecture and," *Int. J. Comput. Sci. Inf. Technol.*, vol. 3, no. 3, pp. 120–139, 2011.

[16] R. Krishnan, "Security and Privacy in Cloud Computing" Master's Thesis from ScholarWorks at WMU" 2017.

[17] H. Sunghyuck, "Secure and efficient tree-based group Diffie-Hellman protocol," *KSII Trans. Internet Inf. Syst.*, vol. 3, no. 2, pp. 178–194, 2009.

[18] M. Ruby and K. Venkatarao, "Secure Group Communication by Establishing a Novel Trust Relationship Model and Detecting Malicious nodes in Peer to Peer Systems," vol. 4, no. 12, pp. 2058–2062, 2015.

[19] Ryotaro Hayashi and Tatsuyuki Matsushita, "A Proxy Re-Encryption Scheme with the Unforgeability of Re-Encryption Keys against Collusion Attacks,", pp. 1–26, 2014.

[20] Sheetal Mahalle, Ranjeet Jaiswal, "Cloud Computing Security :A Survey", vol. 115, no. 6, pp. 21–25, 2015.

[21] M. P. Rewagad and M. Y. Pawar, "Use of digital signature with diffie hellman key exchange and aes encryption algorithm to enhance data security in cloud computing," *Proc. - 2013 Int. Conf. Commun. Syst. Netw. Technol. CSNT 2013*, pp. 437–439, 2013.

[22] X. Huang, J. K. Liu, S. Tang, Y. Xiang, and S. Member, "Cost-Effective Authentic and Anonymous Data Sharing with Forward Security," vol. 64, no. 4, pp. 971–983, 2015.

[23] Rodrigo N. Calheiros, Rajiv Ranjan, Anton Beloglazov, C´esar A. F. De Rose and Rajkumar Buyya, "CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms", pp. 23–50, 2010.

[24] Liu, H., Member, S., Ning, H., Member, S., Xiong, Q., & Yang, L. T. "Shared Authority Based Privacy-preserving Authentication Protocol in Cloud Computing" , vol. 26, no. 1, pp. 241–251, 2015.

[25] Lijang Yi, Guoqiang Bia and Guozhen Xian, "Proxy multi-signature scheme: A new type of proxy signature scheme, vol. 36, no .6, pp. 527–528, 2000.

[26] Emmanuel B., Olivier Ch., David P., Jean-Jacques Q., "Provably Authenticated Group Diffie-Hellman Key Exchange, vol. 36, no .6, pp. 225–264, 2001.

[27] H. Qinlong, M. A. Zhaofeng, Y. Yixian, F. U. Jingyi, and N. I. U. Xinxin, "EABDS : Attribute-Based Secure Data Sharing with Efficient Revocation in Cloud Computing ∗," vol. 24, no. 4, pp. 862–868 ,2015.

[28] K. Xue and P. Hong, "A Dynamic Secure Group Sharing Framework in Public Cloud Computing," vol. 2, no. 4, pp. 459–470, 2014.

[29] P. G. Sonar et al, "A Novel Approach for Secure Group Sharing in Public Cloud Computing, vol. 127, no. 11, pp. 47–50, 2015.

[30] Prashant Rewagad and Yogita Pawar, "Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing," vol. 3, no. 13, pp. 437- 439, 2013.

[31] A. Kalaskar et al., "Secure Information Sharing for Dynamic Groups in Cloud Computing : Survey," vol. 2, no. 3, pp. 171–175, 2015.

[32] S. Sathya, B. Vanathi, and K. Shanmugam, "Secure-Sharing-of-Data-for-Dynamic-Group-in-Cloud-Storage-Application," vol. 7, no. 3, pp. 812–817, 2016.

[33] Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yan "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," vol. 24, no. 6, pp. 1182–1191, 2013.

[34] Yunchuan Sun, Junsheng Zhang, Yongping Xian, and Guangyu Zhu, "Data Security and Privacy in Cloud Computing," Sage Journal, International Journal of Distributed Sensor Networks, China, pp. 1–9, July 2014.

[35] A. Avi˘zienis, J. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing,"IEEE Transactions on Dependable and Secure Computing, vol. 1,no. 1, pp. 11–33, 2004.

[36] Z. Mahmood, "Data location and security issues in cloud computing," in Proceedings of the 2nd International Conference on Emerging Intelligent Data and Web Technologies (EIDWT'11),pp. 49–54, IEEE, September 2011

[37] D. Sun, G. Chang, L. Sun, and X. Wang, "Surveying and analyzing security, privacy and trust issues in cloud computing environments," in Proceedings of the International Conference on Advanced in Control Engineering and Information Science (CEIS'11), pp. 2852–2856, chn, August 2011.

[38] Umadevi. R, Velumani.V, "Security Enhancement of Health Information Exchange Based on Cloud Computing," vol. 2, no. 9, pp. 89-93, 2017.

[39] B.V.Varshini, M.Vigilson Prem, J.Geethapriya, "A Review on Secure Data Sharing in Cloud Computing Environment," vol. 6, no. 3, pp. 224-228, 2017.

[40] Salah M El-Sayed, Hatem M. Abdul Kader, Mohie M. Hadhoud , Diaa Salama AbdElminaam, "Mobile Cloud Computing Framework for Elastic Partitioned/Modularized Applications Mobility," vol. 1, no. 2, pp. 53-63, 2014.

[41] Ashish Singh, Kakali Chatterjee, "Cloud security issues and challenges: A survey," vol. 79, no. 1, pp. 88–115, 2017.

[42] Yihui Cui, Zhiyong Peng, Wei Song, Xiaojuan Li,Fangquan Cheng, and Luxiao Ding,"A Time-Based Group Key Management AlgorithmBased on Proxy Re-encryption for Cloud Storage , pp. 117–128, 2014.

[43] Rehan Saleem, "Master's Thesis, Cloud computing's effect on enterprises in terms of cost and security", pp. 1–9, 2011.

[44] Ass. Prof. Kirit J. Modi," CLOUDSIM" form "www.uvpce.ac.in/content/m-tech-admission-inquiry", pp. 1–29, 2017.

[45] Jonathan Strickland," How Cloud Computing Works" form "www. computer.howstuffworks.com/cloud-computing", 2008.

[46] Kuliya Muhammed, Isma'il Zaharaddeen, Kabir Rumana, Abdulkadir M. Turaki, "Cloud Computing Adoption in Nigeria: Challenges and Benefits", vol. 5, no. 7, pp. 89-93, 2015.