International Journal of Engineering & Technology, 7 (3) (2018) 1172-1176

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i3.13676
Research paper

Implementation of key-cryptosystem for efficient data sharing in cloud environment

Jumana Waleed [1] *, Taha Mohammed Hasan[1], Ahmed Brisam[2], Roaa Falih Mahdi [3]

[1] Department of Computer Science, College of Science, University of Diyala, Iraq
[2] College of Agriculture, University of Al-Qadisiyah, Iraq
[3] Faculty of Engineering, Department of Computer Engineering, University of Kashan, Iran
**Corresponding author E-mail: jumanawaleed@sciences.uodiyala.edu.iq*

Abstract

The distributed storage based on data recovery administration is a promising innovative way that mounts market actively sooner rather than later. However, in spite of the various studies which have been done in terms of secure information recovery over encoded information in cloud administrations, the majority of these studies concentrated on the strict security given to information in an outside space. Those methodologies oblige dynamite expenses to unify on cloud administration supplier that can be an important hindrance to accomplish productive information recovery in distributed storage. In this paper, a proficient information recovery plan utilizing property based encryption was proposed. The proposed plan is most appropriate for distributed storage frameworks with the gigantic measure of infor-mation. Affluent expressiveness as access control and quick pursuits with straightforward examinations of looking elements were given. Additionally, the plan ensures information security and client protection among information recovery process.

Keywords: *Key-Cryptosystem; Data Sharing; Distributed Computing; Cloud Environment*.

1. Introduction

Cloud Computing is located of assets which are being specified on benefit. Distributed Computing presents preferable methods to allow management; these methods, evaluate open doors acquire modifies the manner business worked. Distributed Computing is a unique working invention and it is another fingerprint to an old concept that is a combination of assets and overhauled gave by cloud management provider over the web. Cloud management or Administrations are carried from information lopes sited anywhere over the world. Distributed Computing produces reasonable for its clients to use the true assets by means of web depending on requirements. It took the publicity in a little time. Common states of Cloud Administrations are Google Engine, Oracle Cloud, Office 365. The development of Distributed Computing requires additional concerns such as security. The loss of security is the major limitation in enormous Distributed Computing appropriation. The quick evolution of Distributed Computing has yielded different security challenges to the clients and suppliers [1].

While cost and convenience are the main principle solid interests of the distributed computing, several significant disturbing issues need to be referenced when permitting moving discriminating application and touchy information to open and imparted cloud environment. Primary angle depicting an accomplishment of any new figuring, the invention is the height of security it gives if the information spotted in the cloud is secured in such a way that it can stay far from any type of security issues. Therefore, the security and protection are the main challenges in the distributed computing. One of the important security issues; is the information security issue which represents the limits access or area reservation on particular sets of data; so in cloud, the information dwell freely so the security issue refers to, client's information and processing task are to be preserved distributing from both cloud supplier and different clients who are using the management. The client's private data must be verified ought not to be gotten by anybody in the distributed computing framework, including application, stage, CPU and physical memory. It is passing that client's classified information is revealed to administration supplier on the accompanying circumstance just. Lots of situations because, a supplier of service is capable of collecting or getting access to the user's data, the supplier of service should have a knowledge about the data location in the cloud computing and is authorized for accessing the data of the user. As it's known, recently, the cloud computing includes three layers; First, software layer which supplied an interface to the user for using the provided services working on the cloud infrastructure; Second, the platform layer supplies the platform like operating environment for software to work with the help of the resources of supplied framework; Third, the infrastructure layer which supplied the hardware resources to compute, storage, and network. In spite of every supplier of service has own software, platform, and infrastructure layer, but when the user utilizes the application of cloud supplied via supplier of service, obligatory, the user must utilize the platform and the infrastructure supplied via the supplier of service. So, the supplier of service should be knowing the location and the accessibility of the user's data. When storing the data in a faraway location that is held via others, the owners of data could meet the issue of system weakness of the supplier of service. If the cloud stops running, the data won't available. There are different types of attacks on the data availability which cause a denial of service, and direct-indirect threat.

The cloud computing provides considerable user appropriateness by releasing users from the necessity to know the working details, but it requires them to trust by cloud services supplier, and this may lead users to worry. So, cloud supplier's must process privacy and security problems as a problem of big and meaningful necessity.

Recently, the realization of cloud computing problems is heavily weighted across privacy and security problems. In order to deal with these problems, a lot of works in information hiding [2], [3], [4], [5] and cryptography can be utilized. In this paper, the problem statement is to implement security architecture in cloud computing and to collect the data from different sources and to analyze and present the program in Java. This paper is constructed as follows; the next section contains an explanation of the newly existing related works and the third section presents the design of the system. The experiential analysis is given in section 4. the conclusion and perspective works are drawn in the last section.

2. Related work

When work is linked to security, the cloud has many limitations. The suppliers should guarantee that the client will not find any trouble like losing the data. In addition, there are probabilities that a malignant user can penetrate the cloud out of impersonating an authorized user or through infecting the whole cloud and this has an effect on numerous customers who are participating the infected cloud. There are several limitations faced the researchers such as the research limits in analyzing the cloud computing in networking and the data collection for the research and practical programming may not be accurate.

The motivation behind the research of Ramgovind et al. [6], is to give a general security point of view of cloud processing with expect to highlight the security worries that ought to be appropriately tended to and figured out how to understand the maximum capacity of cloud registering. As indicated by Okuhara et al. [7]; Moving computing into the "Cloud" makes PC preparing considerably more helpful for clients additionally give them new security issues about wellbeing and unwavering quality. To take care of these issues, administration suppliers must make and give security architectures to Cloud processing. This work depicts household and worldwide patterns in security prerequisites for Cloud computing, for example, access convention, verification and identity administration, and security visualization. Subashini et al. [8] introduce a study of the diverse security hazards that represent a danger to the cloud and displayed a review of more particular to the diverse security issues. Houidi et al. [9] present a work in advancement of the cloud administration provisioning crosswise over different cloud suppliers. The work accepts the development of cloud brokers in the middle of clients and cloud suppliers. The representatives part client demands and guarantee provisioning from different suppliers. A careful part calculation is produced to proficiently part the cloud demands among the numerous cloud stages with the point of diminishing the expense for clients. From a security viewpoint, various unchartered dangers and difficulties have been acquainted from this migration with the mists, falling apart a great part of the viability of customary assurance systems. Zissis et al. [10] present a work of twofold; firstly, to assess cloud security by distinguishing special security prerequisites and also to endeavor to present a practical arrangement that takes out these potential dangers. This work proposes presenting a Trusted Third Party, tasked with guaranteeing particular security qualities inside a cloud situation. The proposed arrangement calls upon cryptography, particularly Public Key Infrastructure working together with SSO and LDAP, to guarantee the validation, respectability and secrecy of included information and correspondences. The arrangement shows a flat level of administration, accessible to all involved elements, that understands a security network, inside which fundamental trust is kept up. Server farm and cloud architectures keep on advancing to address the needs of expansive scale multi-occupant server farms and mists. These needs are based on seven measurements: adaptability in figuring, stockpiling, and data transfer capacity, versatility in system administrations, effectiveness in asset usage, nimbleness in administration creation, cost productivity, administration unwavering quality, and security. The authors C. K. Chu et al. [11], P. Gharjale and P. Mohod [12], and V. Swathy et al. [13], present new public-key cryptosystems with effective, secure and flexible data sharing in the cloud that produce constant-size cipher texts in which effective distribution of deciphering rights to any set of cipher texts are realizable. Here, the user or the secret key holder can share more files with a constant-size key at a time. Snata Choudhury and Kirubanand V.B [14] present an efficient implementation of a multi-encryption for protecting the data which will store in public cloud.

3. System design

3.1. Input design

The connection between the user and information system is done by the design of the input. It includes the improving steps and specifications for preparing data and these procedures are required for putting the transaction data into an applicable shape of handling that can be completed by examining the computer to read data from a written document or it can happen by possessing people keying the data straight into the system. The input design concentrates on managing the required number of input, managing the mistakes, averting the delay, averting additional steps and making the process uncomplicated. The design of input is done just like that it supplies a secure and easy usage with keeping the reliability. So the goal of design the input is to produce an input layout which is easy to follow. Figure 1 represents the Architecture of the System.

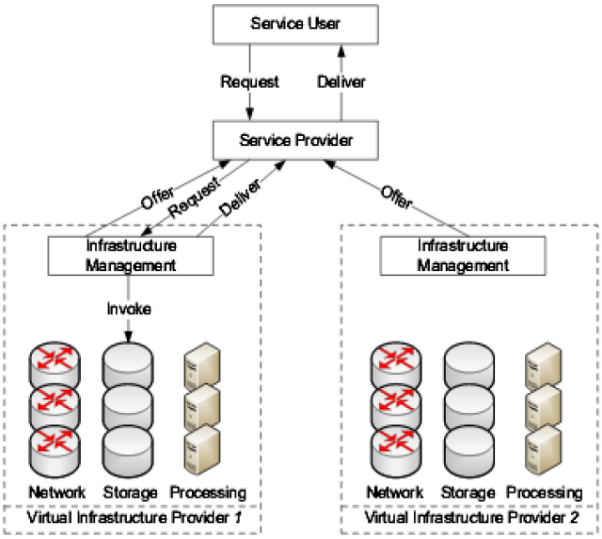

Fig. 1: System Architecture.

3.2. UML diagrams

3.2.1. Data flow diagram

The diagram of the data flow is named a bubble chart which is an easy graphic form; It can be utilized for representing the system in term of the data input for the system, different processing carried out on these data, and the data output is produced via the system. Figure 2 shows a diagram which represents the steps of user login, and these steps firstly, include the name and password insertion for the user. Secondly, if the login is correct, then the home-page (user page) will be opened and this process will enable the user to view account, edit account, change password to ensure that the file is downloaded through sending a request to service provider to offer the VIP and select the virtual resource. On the contrary, if the login is not correct then the user should do the registration.

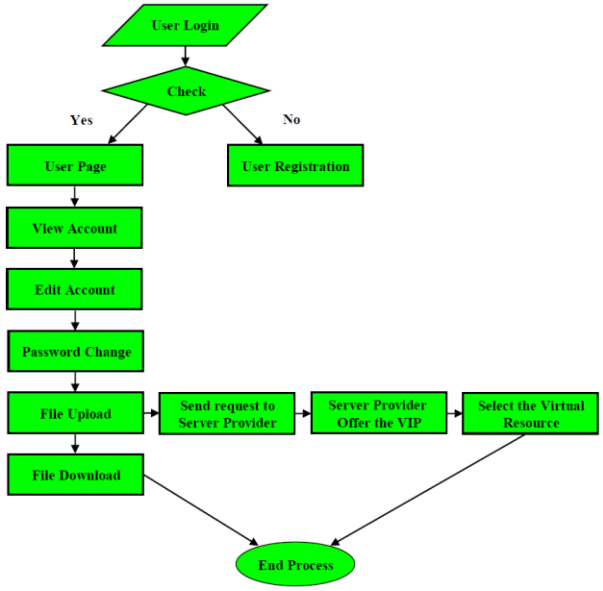

Fig. 2: User.

The diagram in figure 3 refers to the process of the special Admin in which if the login is correct (authorized person), then this will allow the Admin to view all user details, receive the request, offer virtual infrastructure provider and view service list and delete the user and so on. The user list explains to the Admin all the details such as user-ID, username, Email-ID, DOB, mobile number, location, gender and so on. Otherwise, if the login is incorrect then this person is unauthorized.

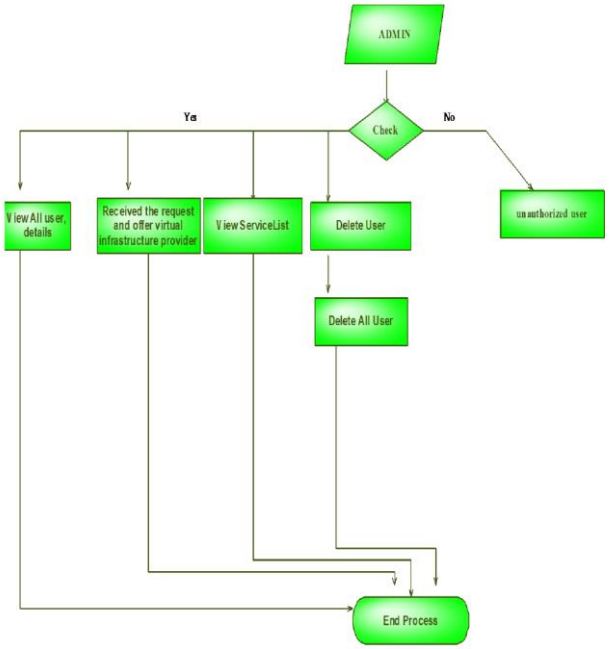

Fig. 3: Admin Dataflow.

3.2.2. Component diagram

This diagram explains a working mechanism of User Login, Service Provider (ADMIN) and Virtual Infrastructure Provider (VIP). Each mechanism includes a few steps of entering the username and password, displaying all user details, receiving the service and clearing the account for full access to the correct image to download the file within the file list.

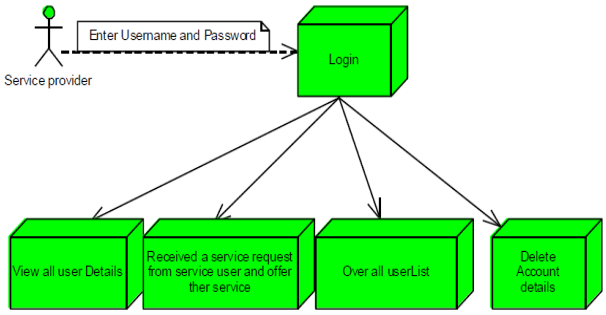

Fig. 4: Service Provider (ADMIN).

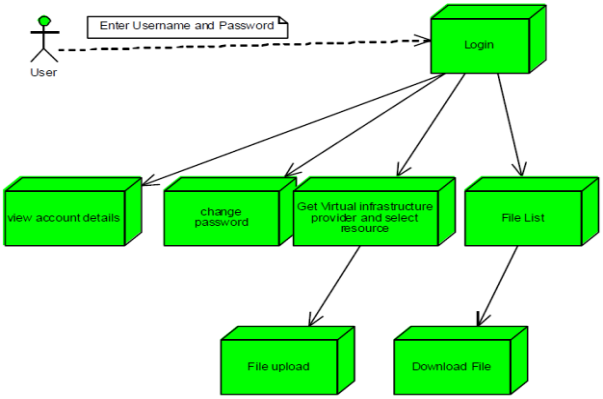

Fig. 5: User Login.

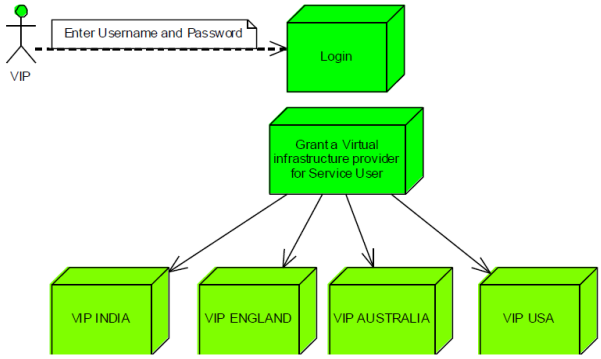

Fig. 6: Virtual Infrastructure Provider (VIP).

3.2.3. Activity diagram

This diagram represents the structural components (architectural) for each of the Admin, Virtual Infrastructure Provider, and Service User. The Admin is capable of viewing all the users, offering the VIP list to service user and deleting the user account. While, Virtual Infrastructure Provider is able to select a current location from (VIP) list such as VIP INDIA, VIP England, VIP USA, and so on.

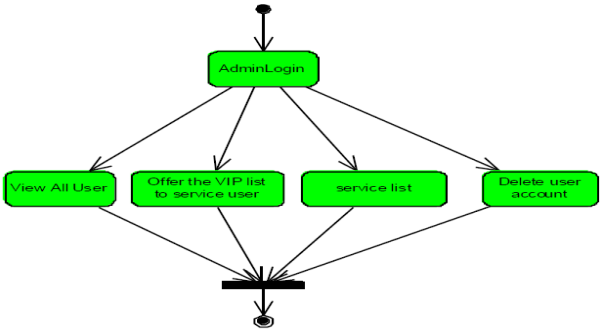

Fig. 7: Admin Login.

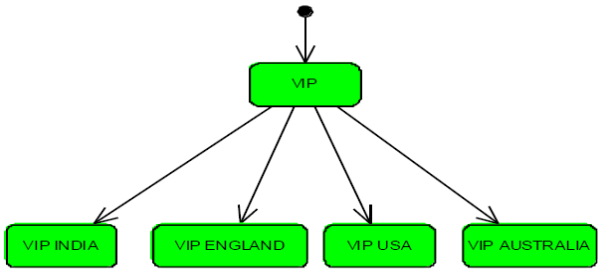

Fig. 8: Virtual Infrastructure Provider.

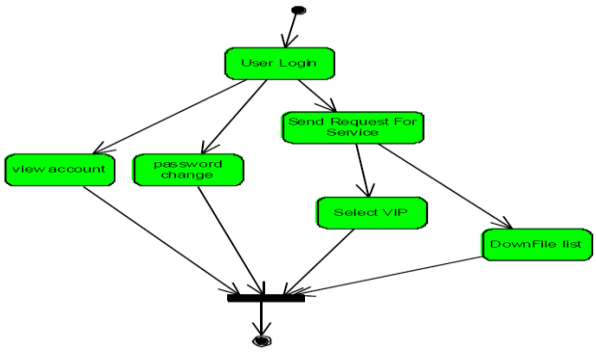

Fig. 9: Service User.

3.2.4. Sequence diagram

The diagram in figure 10 demonstrates the registration mechanism in a sequential manner. And Shows that the user will enter the program using the username and password that was previously recorded in the field sign up. And then goes through several options that can update his personal information (such as user ID, username, Email –ID, DOB, Mobile Number, country, Gender and so on) through the following functions:

- View account: This option Its function displays (user's personal information) that is already registered.
- Edit account: This option has the function of correcting or updating (user's personal information) such as modifying the DOB or changing the Email and others.
- Password change: This option changes its password value to other value fit the user. Such as the password (1111111) that the user changes to (0009999) etc.
- File Upload: This option is to browse the file to be encrypted with one of the specified cryptographic algorithms by reviewing it by hard drives (such as disk D) and saving it in the program.
- File Download: This option is its function to load the user's file from the practical program directly by the user. With consideration. Approval (Director of Administration) responsible for the program.

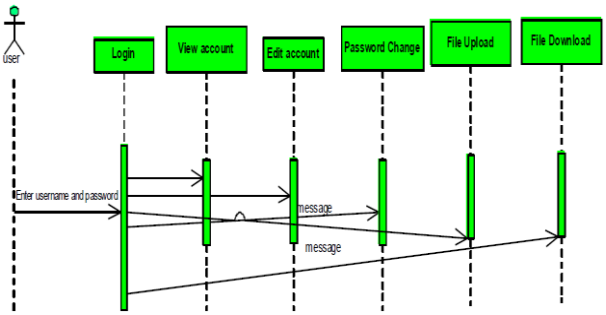

Fig. 10: Service User (Sequence Diagram).

Figure 11 demonstrates how the service provider login and received a request from the service user and offer the virtual infrastructure provider Using one of the encryption algorithms and passing through some security questions, the request is successfully passed. Displays (User Details) and returns (registration steps) repeatedly in other fields of the program. For Example, Fill in fields (date of birth, password and mobile number) for more than once during the program execution steps. In order to maintain the privacy and confidentiality of the program. Non-hacking (user data) and stopping the program from running. It also can delete the user by entering the manager (or ADMIN) into the list User and deleting the unwanted user in the program.

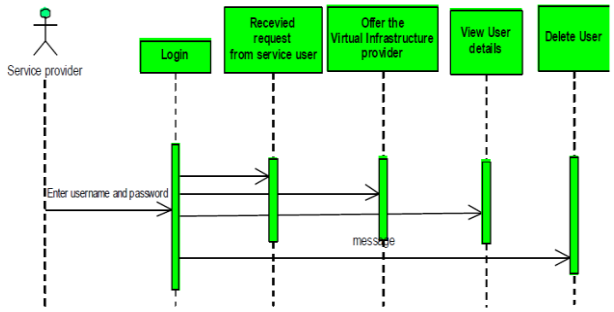

Fig. 11: Service Provider (Sequence Diagram).

In figure 12, the diagram demonstrates how the Virtual Infrastructure Provider gets a request from the service provider and determine the request location from the country list. When VIP receives the request from the service provider, the user enters their username and password until the message passes through a series of country options. Therefore, when the user chooses the appropriate option in the appropriate country location field in the program, this option will then display a list of countries to ensure confidentiality in the user's location. And facilitate the process of discrimination in the case of another user from another country to avoid confusion in the information. Examples of countries used in the diagram will be presented in a sequential format (India, Iraq, Iran, USA, England etc.).

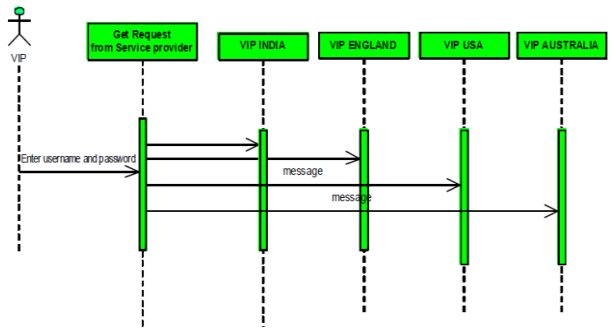

Fig. 12: Virtual Infrastructure Provider.

4. Test program results

In terms of Implementation, when we record new user information (personal information for the user) in the field (SIGN-UP), we must fill in the fields gradually with correct information, for Example the password field should print the numbers correctly and completely copied in confirm password in order to maintain confidentiality in the implementation and then design security question in the practical program and repeated it several times in the program ensures the privacy of user data. This is an important step in the process of testing.

Program input must be correct to ensure correct output. For example, when we enter input data for the user (personal information for the user), Represented. Name, Telephone number, Email address and other data. It will ensure accurate output of the data and display it in the user list.

Fig. 13: Input and Output Program.

To test the program, we need to use one of the algorithms either Data Encryption Standard (DES) or Advanced Encryption Standard (AES). Which is used to encrypt user data in the program. And its usefulness to save the user's private information with a high quality of accuracy and efficiency so as not to be hacked by another user trying to steal data, and penetration of the user file (which contains confidential data from the pictures, videos, and information of large capacity). Therefore, (an algorithm AES) ensures that the user file is encrypted accurately and efficiently while maintaining privacy. The test code (a Java programming code), which is included in the HTML language, is successful completion of the test, Using test functions.

5. Conclusion

The technology of cloud computing represents the effectiveness in time, cost, and performance. This paper showed the basics of using cloud computing with the issues of security. The issues of security represent the most important matter in the cloud computing; essentially, the data integrity and privacy. The data are stored in the cloud publically, and the correct location for storing these data cannot be identified, so, through the process of during storage and transmission, this may lead to a high degree of danger via the access to the data by an untheorized user. The proposed system provides the security for the service users while at the same time benefiting from the flexible and dynamic placement of virtual resources at different virtual infrastructure providers.

References

[1] Antonopoulos, N., & Gillam, L, (2010), "Cloud computing: Principles, systems and applications", Springer Science & Business Media, p. 1-4. https://doi.org/10.1007/978-1-84996-241-4.

[2] Jumana Waleed, Huang Dong Jun, and Saad Hameed, (2014), “A robust Optimal Zero-Watermarking Technique for Secret Watermark Sharing," International Journal of Security and Its Applications Vol.8, No.5, pp.349-360. https://doi.org/10.14257/ijsia.2014.8.5.31.

[3] Jumana Waleed, Huang Dong Jun, Saad Hameed., (2015), "An optimized digital image watermarking technique based on cuckoo search (CS)", ICIC Express Letters, Part B: Applications, Vol. 6, No. 10, pp. 2629-2634.

[4] Jumana Waleed, Huang Dong Jun, Saad Hameed and May Kamil, (2015), "Optimal Positions Selection for Watermark Inclusion based on a Nature Inspired Algorithm", International Journal of Signal Processing, Image Processing and Pattern Recognition, Vol. 8, No. 1, pp. 147-160. https://doi.org/10.14257/ijsip.2015.8.1.15.

[5] Jumana Waleed, Sarah Saadoon Jasim, Thekra Abbas, "The inclusion of watermarks based on QR Code analysis", (2018), International Journal of Engineering and Technology(UAE), Vol. 7, No. (2.9), pp. 97-101.

[6] Ramgovind S., Eloff M. M., and Smith E., (2010), "The management of security in cloud computing", IEEE, In Information Security for South Africa (ISSA), pp. 1-7. https://doi.org/10.1109/ISSA.2010.5588290.

[7] Okuhara, M., Shiozaki, T., and Suzuki, T., (2010), "Security architecture for cloud computing", Fujitsu Sci. Tech. J, 46(4), pp. 397-402.

[8] Subashini, S., and Kavitha, V., (2011), "A survey on security issues in service delivery models of cloud computing", Journal of network and computer applications, 34(1), p 1-11. https://doi.org/10.1016/j.jnca.2010.07.006.

[9] Houidi, I., Mechtri, M., Louati, W., and Zeghlache, D., (2011), "Cloud service delivery across multiple cloud platforms", In Services Computing (SCC), 2011 IEEE International Conference on, p. 741-742. https://doi.org/10.1109/SCC.2011.107.

[10] Zissis, D., and Lekkas, D., 2012, "Addressing cloud computing security issues", Future Generation computer systems, 28(3), pp. 583-592. https://doi.org/10.1016/j.future.2010.12.006.

[11] C. K. Chu, S. S. M. Chow, W. G. Tzeng, J. Zhou and R. H. Deng, (2014), "Key- Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage", in IEEE Transactions on Parallel and Distributed Systems, 25(2), pp. 468-477. https://doi.org/10.1109/TPDS.2013.112.

[12] P. Gharjale and P. Mohod, (2015), "Efficient public key cryptosystem for scalable data sharing in Cloud storage", 2015 International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC), pp. 0325-0329. https://doi.org/10.1109/ICCPEIC.2015.7259485.

[13] V. Swathy, K. Sudha, R. Aruna, C. Sangeetha and R. Janani, (2016), "Providing advanced security mechanism for scalable data sharing in cloud storage", 2016 International Conference on Inventive Computation Technologies (ICICT), pp. 1-6. https://doi.org/10.1109/INVENTIVE.2016.7830237.

[14] Snata Choudhury and Kirubanand V. B, (2018), " Data encryption in public cloud using multi-phase encryption model", International Journal of Engineering and Technology(UAE), Vol. 7, No. 1, pp. 223-227. https://doi.org/10.14419/ijet.v7i1.9309.