Storage Architecture for Network Security in Cloud Computing

Qusay Kanaan Kadhim[1], Hamid Sadeq Mahdi[2] and Haitham A. Ail [3]

[1,3] Department of Computer Science, Al Yarmouk University College, Iraq
[2] Department of Computer, University of Diyala, Basic Education College, Iraq

[1]qusaykn@gmail.com

[2]hamid.sadeq.mehdi@basicedu.uodiyala.edu.iq

[3] haithamlaz9@gmail.com

Received: 27 March 2017 **Accepted: 11 June 2017**

Abstract

Cloud Computing is seen as greatly accessible computing resources as an outward service granted from the world wide web. As an economical view, the cloud computing key is that consumers are free to use whatever they want, and pay for the services they want. The accessibility of the resources from the cloud is obtainable whenever users want and wherever they are. Therefore, users are free to purchase the IT service that they want and they do not have to be concern more about the manner that maintainable things can be beyond the positions. New model for data storage computing which considers as a web-based generation utilizes remote servers. The challenging needed to be undertook in cloud computing is the safety of information of service sources' site. Thus, this study suggests that designing new construction for the security of information storage with variety functions where information encrypted and split into many cipher blocks and disseminated between a large number of services suppliers locations instead of merely relying on only one supplier for information storage. Proposed based in the new architecture, it is applicable to ensure a better security, availability and reliability.

Keyword: Storage, Architecture, Network Security, Cloud Computing.

معمارية أمن التخزين في الحوسبة السحابية

قصي كنعان كاظم[1] ، حامد صادق مهدي[2] وهيثم عبد الكريم[3]

[1،3]قسم علوم الحاسوب ، كلية اليرموك الجامعة - العراق
[2]قسم الحاسوب ، جامعة ديالى – كلية التربية الاساسية – العراق

الخلاصة

تعتبر الحوسبة السحابية موارد يمكن الوصول إليها بشكل كبير كخدمة ممنوحة من الشبكة العالمية كما وجهة نظر اقتصادية، السمة الرئيسية في الحوسبة السحابية هو أن المستهلكين أحرار في استخدام كل ما يريد. إمكانية الوصول إلى الموارد من السحابة يمكن الحصول عليها المستخدمين كل ما يريدون وأينما كانوا. ولذلك فأنا المستخدمين أحرار في شراء خدمات تكنولوجيا المعلومات التي يرغبون بها ،هي تقنية الجيل الجديد على شبكة الإنترنت تقدم تخزين البيانات في السحابية و ايضا يستخدم خدمة المناطق النائية. من التحديات التي تواجها الحوسبة السحابية هي أمن المعلومات من موقع مزودي الخدمات. وبالتالي تقترح هذه الورقة تصميم هيكل جديد للأمن تخزين المعلومات مع وظائف متنوعة حيث المعلومات مشفرة وتنقسم إلى عدة كتل وتشفيرها ونشرها بين اكثر من مزود واحد من مزودي الخدمات المواقع الحوسبة السحابية بدلا من مجرد الاعتماد على مزود واحد فقط لتخزين المعلومات. المقترح هوبناء الهيكل للنظام الجديد ينطبق على ضمان أمن أفضل وأتاحتها وموثوقية.

الكلمات المفتاحية : التخزين ، الهندسة المعمارية ، شبكة ، الآمن ، الحوسبة السحابية .

Introduction

Since the past decade, information technology has been changed dramatically and developed gradually. For example, the internet replaced the old-fashioned software models which has gradually increased the momentum of its services. Recently, the Old-style of business requests have been recognized to be obsolescence due to their complexity in the process and costly. Besides that, the volume and types of hardware as well as software that need to operate them are creepy. The new generation of cloud computing bridged the gap of information technology and eliminated the traditional system limitation through handling hardware and software shifts from users to proficient Service Supplier [1]. Cloud computing considered as a modern computational archetype that proffers on creative model of business for institution to embrace it in absence of direct investment. Both of database and software applications in

cloud computing are transformed into vast center of data such that data service and management cannot be wholly valuable [2]. The premature classical storage system is less more useful and benefits than cloud storage particularly in price decrease, scalability, movability and applicatory condition [3]. The description of cloud storage is a service to administrate, and preserve the remote of data [4]. The user can find this service over the internet (as an example). The user has a permission for storing and retrieving files online from any site using the internet [5]. The user can obtain files online if the uploaded files are kept by the supplier firm on an outward server. Cloud storage services can be enabled for using easily and comfortably by the firms, but probably it can be costly. The backup of users' data is still prerequisite if cloud storage services are applied due to data retrieving from cloud storage that is less faster than locally backup [6]. In cloud storage, dividing data to small parts and saving them to variant locations makes the data secure, therefore if any smash happened to data parts in one data center or a disk, then left blocks makes data to be resumed [7]. In cloud computing, storing the data as public in-service supplier's locations makes the data to have a low security [8]. Cloud computing makes the benefits more attractive than ever, however many challenging security topics also brought for users' data. The essential safety challenge is that there is no supervision on the location of the owners' data. In cloud computing, it is not safe to rely on one service supplier for data storage [9]. Any network or hardware problem in the service supplier location makes the data to be lost, so by using a distributed parity scheme data can be retrieved in this structure and by using Redundant Array of Inexpensive Disks (RAID) storage scheme. The distribution of data over several clouds was discussed in [10] in a method that if an opponent is capable to interrupt in one network. The principal of RAID storage technology in cloud computing was discussed in [11]. Cryptographic quota single-handedly cannot encounter the confidentiality needed via cloud computing facilities [12] [13] because it is inadequate for guaranteeing information confidentiality in cloud computing. The notion of information distribution over numerous cloud service supplier's location instead of central dissemination of information was put [14]. The cloud storage system structure contains admission layer, use interface layer [15]. The combination between cloud storage and private cloud was discussed by [16]. The structure of

cloud storage, hiding complication of hardware and software from its operators were suggested in [17] [18]. the benefit and viability of the technology of secrecy cloud storage centered on Hadoop was analyzed. In [19], Service Level Agreement (SLA) was used as the common standard amongst services suppliers and services' users to guarantee information safety in cloud storage structure. In [20]. The construction to firmly store user information in open cloud and secluded cloud finished employing encryption was suggested [21] [22]. The safety subjects in cloud storage analyzed based on cloud computing perceptions and landscapes in [23]. Figure (1) displays the information loading construction with the host machine represented as user and service suppliers manifest as SP1 to SPn.

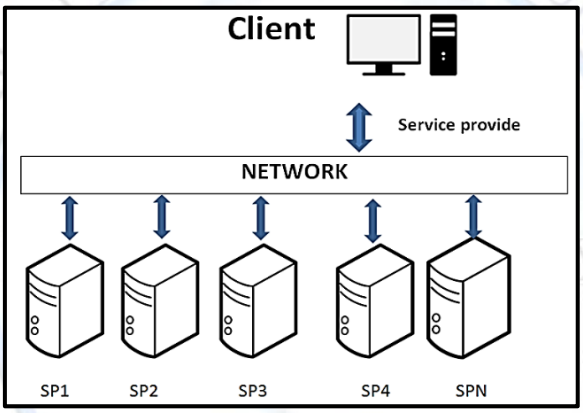

Figure 1: Suggested construction for cloud information storing

Related Work

(Bisong, A. & Rahman, S.) in [24] discussed security risks and concerns in cloud computing and enlightened steps that an enterprise can take to reduce security risks and protect their resources. They have also explained cloud computing strengths/benefits, weaknesses, and applicable areas in information risk management. (Zissis, D. & Lekkas, D.) in [25] presented a paper to evaluate cloud security by identifying unique security requirements and secondly to attempt to present a viable solution that eliminates these potential threats. The paper proposed introducing a Trusted Third Party, tasked with assuring specific security characteristics within a cloud environment. The proposed solution calls upon cryptography, specifically Public Key Infrastructure operating in concert with SSO and LDAP, to ensure the authentication, integrity

and confidentiality of involved data and communications. The solution, presents a horizontal level of service, available to all implicated entities, that realizes a security mesh, within which essential trust is maintained. (Rosado, D. G. et al.) in [26] justified the importance and motivation of security in the migration of legacy systems and they carried out an analysis of different approaches related to security in migration processes to cloud with the aim of finding the needs, concerns, requirements, aspects, opportunities and benefits of security in the migration process of legacy systems. (Hashizume, K. et al.) in [27] presented a categorization of security issues for Cloud Computing focused in the so-called SPI model (SaaS, PaaS and IaaS), identifying the main vulnerabilities in this kind of systems and the most important threats found in the literature related to Cloud Computing and its environment.(Ahmed, M. & Hossain, M. A.) in [28] presented a review on the cloud computing concepts as well as security issues inherent within the context of cloud computing and cloud infrastructure. (Harfoushi, O. et al.) in [29] discussed various security issues and challenges, and presented a conceptual study of the data security issues and challenges in cloud computing. (Hussain, I. & Ashraf, I.) in [30] presented a review of different security issues like trust, confidentiality, authenticity, encryption, key management and resource sharing along with the efforts made on how to overcome these issues. (Srivastava, H. & Kumar, S. A.) in [31] proposed a governing body framework which aims at solving the security and privacy issues by establishing relationship amongst the service providers in which the data about possible threats can be generated based on the previous attacks on other service providers. The Governing Body was responsible for Data Center control, Policy control, legal control, user awareness, performance evaluation, solution architecture and providing motivation for the entities involved.

Network Security

Networks become more complex practically in terms of offered services such as electronic commerce. As a result, networks are more and more subject to various kinds of complex security attacks. Existing security system responses have reached their limits in detecting and defending against various network attacks because current attacks are decentralized, automated and intelligent and these systems are passive in response to network attack in that

they are limited to being local; and there is no automated, network wide response against detected attacks. Some drawbacks of existing systems reveal the necessity of designing a new generation of systems adapted to dynamical environment. Described an active network approach that provided interesting characteristics to deal with these requirements [32]. The security of computer networks plays a strategic role in modern computer systems. In order to enforce high protection levels against malicious attack, a number of software tools have been currently developed. Intrusion Detection System (IDS) has recently become a heated research topic due to its capability of detecting and preventing the attacks from malicious network users. Proposed a pattern matching IDS for network security [33]. The three primary goals of network security which are confidentiality, integrity and availability can be achieved by using firewalls. Firewalls provide security by applying a security policy to arriving packets these policy called security rules and also firewalls can perform other functions like Gateway Antivirus, Gateway Monitor Program to monitor the traffic which pass. [34]. The development of the Web technologies and services increases the level of threats to data security in companies and enterprises day by day information systems about its daily businesses, increases its risk to become vulnerable to security breaches. introduced a comprehensive network security approach for an online retail company which suffers from security breaches [35].

Cloud Computing

Cloud Definitions

Cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This definition is provided by U.S. NIST (National Institute of Standards and Technology) [36]. Another definition is according to Wikipedia which define Cloud computing as it is the delivery of computing as a service rather than a product, whereby shared resources, software, and information are provided to computers and other devices as an over a network (typically the Internet) [37]. Cloud computing is a general term for anything that involves delivering hosted services over the Internet. Instead of a static system

architecture, Virtualization technology allows cloud vendors to convert one server into many virtual machines, [38].

Public Cloud

Public cloud allows users to access the cloud publicly via interfaces using web browsers. Users need to pay only for the time duration they use the service, i.e., pay-per-use. This can be compared to the electricity system which receive at our homes same concept applies here [39]

Private Cloud

A private clouds operation is within an organization's internal enterprise data center. The main advantage here is that it is easier to manage security, maintenance and upgrades and also provides more control over the deployment and use. [40].

Cloud Architecture

Cloud computing system can be divided into two sections as front end and back end. They both are connected with each other through a network, usually the internet. Front end is what the client (user) sees whereas the back end is the cloud system. Front end has the client's computer and the application required to access the cloud (Browser) and the back has the cloud computing services like on-demand computing and data storage from various servers. The figure below shows the cloud computing system architecture [41].

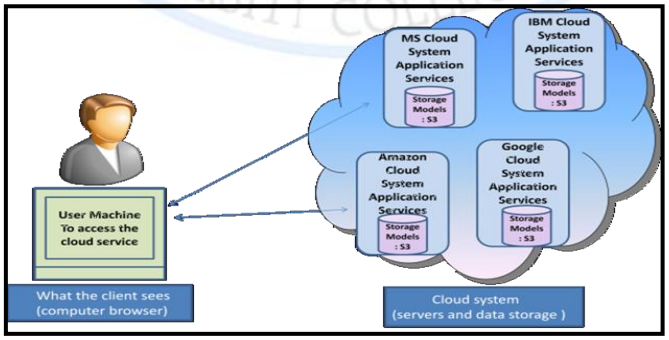

Figure 2: Cloud Computing System Architecture

Security in Cloud Computing

Cloud computing is internet based service paradigm where users access various services from Cloud service provider (CSP) through internet. Whenever user logs in a cloud and start accessing various services. As far as security of information exchanged is concerned, only cloud storage is not concerned. There are in fact various levels where security breach may take place and integrity of information may be compromised. Figures 3 and 4 below illustrate various levels of security concerns in cloud environment respectively [42].

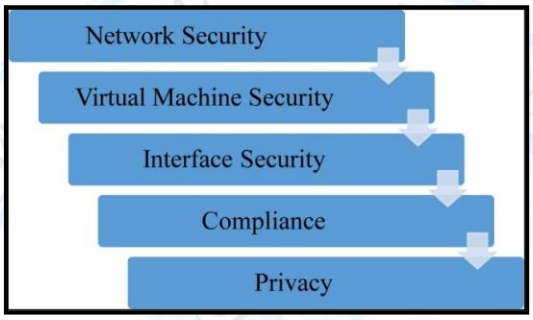

Figure 3: Various Levels of Security Concerns in Cloud Computing

Cloud computing is suffering from severe security threats from user point of view, one can say that lack of security is the only worth mentioning disadvantage of cloud computing. [43]. One of the biggest security worries with the cloud computing model is the sharing of resources. If there was private/sensitive information being stored on a private cloud then there is a high chance that someone could view the information easier than many might believe. The customer is advised to only give their data or use the cloud providers system if they trust them [44].

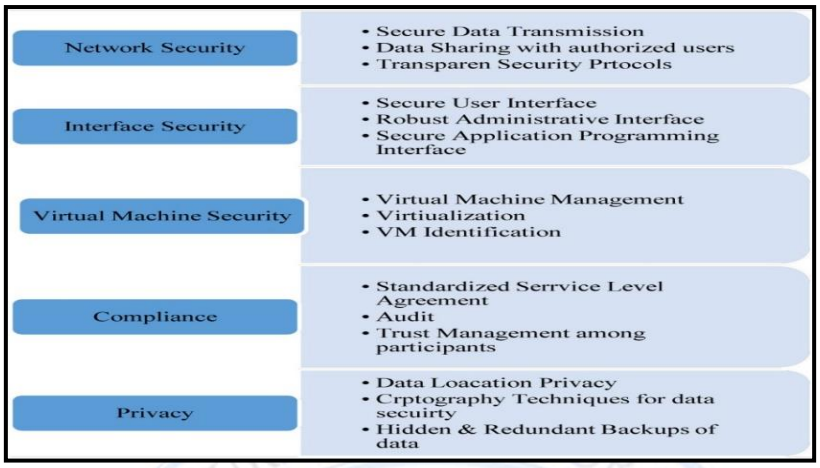

Figure 4: Various Levels of Security Concerns in Cloud Computing

Proposed System Storage Architecture

The encrypted blocks of the information, and the equality data associated with the disseminated information are deposited in the service supplier's information server. This equality of data is not deposited on only service supplier server, but it is dispersed between the obtainable service suppliers for the well-organized re-establishment of information from the obtainable information blocks. To obtain the better availability of data, RAID level implementation will be adopted by each data server in the service provider premises. The suggested RAID level for implementation is RAID 10 based on the performance assessment of several RAID stages. Large arrays with high performance in most uses and superior fault tolerance are generated using RAID 10 because it syndicates the top features of striping and reflecting. Once hard disks turn out to be cheaper, RAID 10 has been melodramatically increasing in acceptance. Conjoining the speed of RAID 0 with the redundancy of RAID 1 minus demanding parity calculations will provide very good to excellent overall performance. Figure 5 characterizes the full architectural illustration of the suggested construction through six service suppliers' information.

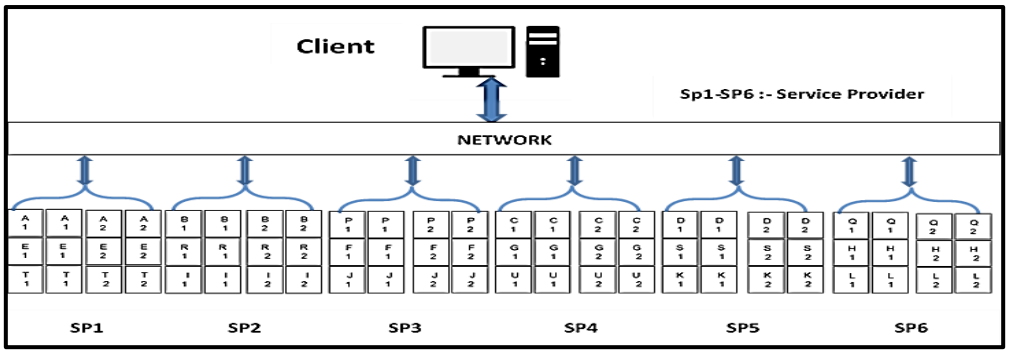

Figure 5: Suggested construction through six service suppliers

Service suppliers 'site, storage server procedures Raid level 10 for data storage. Assume that (Z) is the original data to be deposited in the cloud storage by client. (Z) is then encrypted to (Z') and is split into variant cipher blocks (A, B, C, D, E, F, G, H, I, J, K and L). and is deposited in service suppliers sites successively. Assume that, SP1 stores data block (A), SP2 stores data block (B), SP4 stores data block (C) and SP5 stores data block (D) then to rebuild the data blocks (A and B) or to rebuild the information blocks (C and D) owed to any system or network breakdown, SP3 and SP6 store the parity information (P and Q) related with data blocks (A and B) and (C and D) respectively. Likewise, SP2 and SP4 stores the parity information (R and S) linked with blocks (E and F) and (G and H) respectively, and (T and U) connected to blocks (I and J) and (K and L) is stored in SP1 and SP5 correspondingly. Here, distributed parity scheme is used. Separately statistics block and equality blocks are barred and reflected since RAID 10 will be employed. Information block A on SP1 is striped into dual blocks as A1 A2 and reflected copy also deposited on SP1.Likewise the information blocks and equality blocks on additional service suppliers site are also barred and reflected. An even number of disks are required in RAID 10 packing system revealed in Figure 6.

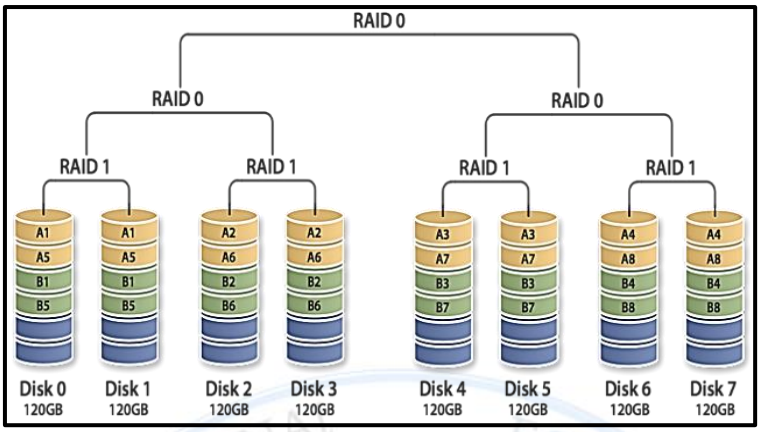

Figure 6: RAID 10 storage system with four service providers

In each disk array there is a replica disk array that is mirrored set of the former. To implement RAID 10, minimum of four disks are needed. There is an ability to handle single disk failure because dual disk stores a mirrored copy of striped data. In the case of double disk failure, it is impossible to recover the data in RAID 10. So, in the proposed architecture, a parity scheme is introduced. Figure 6 shows RAID 10 storage scheme. Assume that customer data are distributed among six service providers SP1, SP2, SP3, SP4, SP5 and SP6.The parity information (P) related to data block (A) stored in SP1 and (B) stored in SP2 is stored in SP3 and the parity information (Q) related to data block (C) stored in SP4 and (D) stored in SP5 is stored in SP6. If any data is lost on data blocks (A) in SP1 or (C) in SP4, then data blocks (A) or (C) can be reconstructed with the help of other data block (B) in SP2 and parity information (P) in SP3 or data block (D) in SP5 and parity information (Q) in SP6, as shown in figure 7.Similarly, if data blocks (B) in SP2 or (D) in SP5 are corrupted, then it will be recovered with the help of data blocks (A) in SP1 and parity (P) on SP3 or data block (C) in SP4 and parity (Q) in SP6. Therefore, it is effectively to reconstruct the data with the help of this parity scheme, if double disk failure occurs. The problems related to hardware are rectified and the data loss due to network issues in any of the service provider's site are sorted out using this scheme. So, the reliability of the proposed architecture is ensured. Although the service supplier might be truthful, many mischievous users always create security problem. Thus, it is undecorated hazard for critical data such as medical or financial records, as cloud service provider employees has physical access to the hosted data. The risk of a single point

of failure, which caused by management of computing resources as a service by a single service provider suggests and the failure owes to number of causes such as hardware, software or network failure. The corrupting or losing the entrusted information from some suppliers, which effects on recovering information appropriately. The cloud storage will have the ability to improve the efficiency through:

- Ensuring the security of the data stored in the cloud storage, and tackling the security issue by encrypting the original data and later by distributing the fragments transparently across multiple service providers.
- Achieving the principal of availability by storing the data on several cloud storage providers whereby no single entire copy of the data resides in one location, and only a subset of providers needs to be available in order to reconstruct the data.
- Achieving the principal of reliability by the parity scheme, by enabling the application to retrieve data correctly even if some of the providers corrupt or lose the entrusted data.

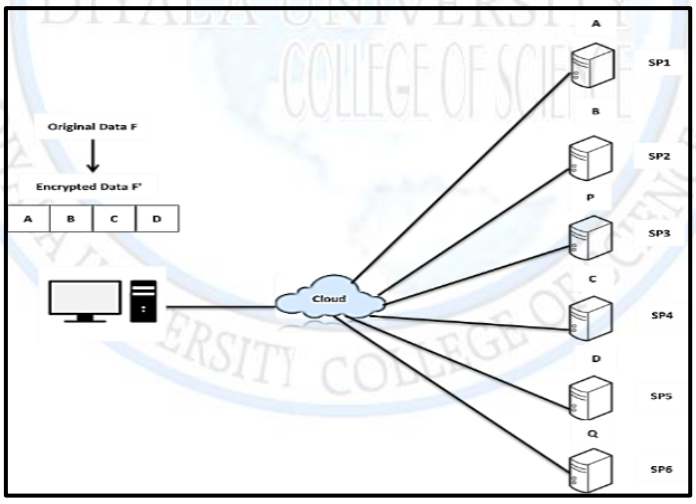

Figure 7: Parity scheme with six service providers

Conclusion

The proposed system encrypts and divides information into cipher parts. Then it allots the cipher parts amidst obtainable service provider's site. The Advanced Encryption Standard (AES) will apply the encryption process. The algorithm of AES may be utilized to protect electronic information. This algorithm can apply both of encryption and decryption processes

for user information, i.e. this algorithm is symmetric. User information can be changed to a non-understandable form called cipher-text using the encryption process, while the cipher-text can be changed back into its original form called plaintext using the decryption process. This algorithm can be used by three variant main distances that are (AES-256), (AES-192), and (AES-128). In addition to use AES algorithm for security, it can be used for excessive speed. After all that mentioned, both of software and hardware applications are still faster. The security of the information can be confirmed by distributing the operators' information between obtainable service providers instead of storing the whole information on a single service provider location. Suppose that, customer data (F) is to use outside sources. The whole data are stored on one service supplier in the centralized storage scheme. So, data will not be safe in this scheme. In the proposed architecture, original information (F) will be encrypted to (F') and then broken off into cipher parts (A, B, C and D), depending on the security perspective. Suppose that, there are four cloud service suppliers available that are SP1, SP2, SP3 and SP4. The encrypted information are dispersed among service suppliers and the cipher part (A) is stored on SP1, (B) is stored on SP2, (C) is stored on SP3 and (D) is stored on SP4 respectively. The proposed architecture uses RAID 10 for storage. Thus parts (A, B, C and D) are striped and mirrored (A: A1, A2, B: B1, B2, C: C1, C2, D: D1, D2). It is important to take into account that the information cannot be recovered from the information stored in the network of a single service provider. Furthermore, the cloud service providers may conspire together for recovering and restructuring the customer's stored data. In this supposed architecture, both of the encryption and distribution processes are accomplished with taking into account the rebuild of information is hard, even though couple of service supplier (A and B) or (C and D) will conspire each other, and this will make the proposed architecture safe. Data getting will be accomplished if the stored data on any storage device are redundant which depends on how fast the access. The bandwidth of network station is impacted by the obtained data. Therefore, a high-speed network cables are employed to retrieve the information.

References

1. Wang, C. et al., 2013. Privacy-preserving public auditing for secure cloud storage. *IEEE Transactions on Computers*, 62(2), pp.362–375.
2. Zhao, L., Sakr, S. & Liu, A., 2015. A framework for consumer-centric SLA management of cloud-hosted databases. Services computing, IEEE Transactions on, 8(4), pp.534–549. Available at: http://ieeexplore.ieee.org /lpdocs/epic03/wrapper.htm?arnumber=6461875.
3. Sr., D.J. & Sharma, Y., 2016. Cloud Computing with ERP - A Push Business Towards Higher Efficiency. Social science research network, 4, p.pp– 140–155
4. Kuo, Y.H., Jeng, Y.L. & Chen, J.N., 2013. A hybrid cloud storage architecture for service operational high availability. In Proceedings - International Computer Software and Applications Conference. pp. 487–492.
5. Daman, R. & Tripathi, M.M., 2015. Encryption Tools for Secured Health Data in Public Cloud. IJISET - International Journal of Innovative Science, Engineering & Technology, 2(11), pp.pp. 843–848.
6. Coyne, L. et al., 2016. Security and Security and Privacy Issues in Cloud Computing – arXi.
7. Sahu, Y., Pateriya, R.K. & Gupta, R.K., 2013. Cloud server optimization with load balancing and green computing techniques using dynamic compare and balance algorithm. In Proceedings - 5th International Conference on Computational Intelligence and Communication Networks, CICN 2013. pp. 527–531.
8. Behl, a & Behl, K., 2012. An analysis of cloud computing security issues. Information and Communication Technologies (WICT), 2012 World Congress on, pp.109–114.
9. Ali, M., Khana, S.U. & Vasilakos, A. V, 2015. In cloud computing, it is not secure to depend on one service provider for data storage. Information Sciences, 305(1), pp.pp. 357–383.
10. Singh, Y., Kandah, F. & Zhang, W., 2011. A secured cost-effective multi-cloud storage in cloud computing. In 2011 IEEE Conference on Computer Communications Workshops, INFOCOM WKSHPS 2011. pp. 619–624.
11. Chen, P.C. et al., 2010. Implementing RAID-3 on cloud storage for EMR system. In ICS 2010 - International Computer Symposium. pp. 850–853.
12. Dijk, M. Van & Juels, A., 2010. On the Impossibility of Cryptography Alone for Privacy-

Preserving Cloud Computing. Proceedings of the 5th USENIX Conference on Hot Topics in Security, pp.1–8. Available at: http://www.usenix.org/event/hotsec10/tech/full_papers/vanDijk.pdf.

13. Yang, J.J., Li, J.Q. & Niu, Y., 2015. A hybrid solution for privacy preserving medical data sharing in the cloud environment. Future Generation Computer Systems, 43-44, pp.74–86.

14. Rao, R.V. & Selvamani, K., 2015. Data Security Challenges and Its Solutions in Cloud Computing. Procedia Computer Science, 48, pp.204–209. Available at: http://www.sciencedirect.com/science/article/pii/S1877050915006808.

15. Jun, S. & Sha-Sha, Y., 2011. The application of cloud storage technology in SMEs. In 2011 International Conference on E-Business and E-Government, ICEE2011 - Proceedings. pp. 1679–1683.

16. Deng, J. et al., 2010. Research and Application of Cloud Storage. 2010 2nd International Workshop on Intelligent Systems and Applications, pp.1–5. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5473373.

17. Wu, J. et al., 2010. Cloud storage as the infrastructure of Cloud Computing. In Proceedings - 2010 International Conference on Intelligent Computing and Cognitive Informatics, ICICCI 2010. pp. 380–383.

18. Zhang, D.W. et al., 2011. Research on Hadoop-based enterprise file cloud storage system. In Proceedings of 2011 3rd International Conference on Awareness Science and Technology, iCAST 2011. pp. 434–437.

19. Shaikh, F.B.F. & Haider, S., 2011. Security threats in cloud computing. 2011 International Conference for Internet Technology and Secured Transactions, (December), pp.214–219. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6148380.

20. Singh, G., 2013. A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security. International Journal of Computer Applications, 67(19), pp.975–8887.

21. Koletka, R. & Hutchison, A., 2011. An architecture for secure searchable cloud storage. In 2011 Information Security for South Africa - Proceedings of the ISSA 2011

Conference.

22. Liu, W., 2012. Research on cloud computing security problem and strategy. In 2012 2nd International Conference on Consumer Electronics, Communications and Networks, CECNet 2012 - Proceedings. pp. 1216–1219.

23. Sari, A., 2015. A Review of Anomaly Detection Systems in Cloud Networks and Survey of Cloud Security Measures in Cloud Storage Applications. Journal of Information Security, p.PP. 142–154.

24. With, Y.W., Chen, I.-R. & Wang, D.-C., 2014. A Survey of Mobile Cloud Computing Applications: Perspectives and Challenges. Wireless Personal Communications, 80(4), p.pp 1607–1623.

25. Angadi, A. et al., 2013. Security Issues with Possible Solutions in Cloud Computing-A Survey. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, 2(2), pp.pp. 652-661.

26. Sushmitha, Y. et al., 2015. A Survey on Cloud Computing Security Issues. International Journal of Computer Science and Innovation, 2015(2), pp.pp. 88-96.

27. Kumar, S. & Goudar, R., 2012. Cloud Computing-Research Issues, Challenges, Architecture, Platforms and Applications: A Survey. International Journal of Future Computer and Communication, 1(4), pp.pp. 356-360.

28. Deepika, C. et al., 2015. A Survey on Cloud Computing Security Issues. *International Journal of Advanced Research in Computer Science and Software Engineering*, 5(6), pp.pp. 992-998.

29. Bisong, A. & Rahman, S., 2011. An Overview of the Security Concerns in Enterprise Cloud Computing. *International Journal of Network Security & Its Applications (IJNSA)*, 3(1), pp.pp. 30-45.

30. Zissis , D. & Lekkas, D., 2012. Addressing Cloud Computing Security Issues. The International Journal of eScience, 28(3), pp.pp. 583-592.

31. Rosado, D. G. et al., 2012. Security Analysis in the Migration to Cloud Environments. Future Internet Journal, 4(2), pp.pp. 469-487.

32. Hashizume, K. et al., 2013. An Analysis of Security Issues for Cloud Computing. Journal of Internet Services and Applications, 4(5), pp.pp. 1-13.

33. Ahmed, M. & Hossain, M. A., 2014. Cloud Computing and Security Issues in the Cloud. International Journal of Network Security & Its Applications (IJNSA), 6(1), pp.pp. 25-36.

34. Harfoushi, O. et al., 2014. Data Security Issues and Challenges in Cloud Computing: A Conceptual Analysis and Review. Communications and Network Journal, 6(1), pp.pp. 15-21.

35. Srivastava, H. & Kumar, S. A., 2015. Control Framework for Secure Cloud Computing. Journal of Information Security, 6(1), pp.pp. 12-23.

36. Eddaoui, A. & Mezrioui, A., 2006. An Active Network Approach for Security Management. International Journal of Computer Science and Network Security, 6(5B), pp.pp. 203-210.

37. Khalil, R. et al., 2010. A Study of Network Security Systems. International Journal of Computer Science and Network Security, 10(6), pp.pp. 204-212.

38. Jahanirad, M. et al., 2012. Comprehensive Network Security Approach: Security Breaches at Retail Company-A Case Study. International Journal of Computer Science and Network Security, 12(8), pp.pp. 107-112.

39. Dillon, T. et al., 2010. Cloud Computing: Issues and Challenges. 24th IEEE International Conference on Advanced Information Networking and Applications, pp.pp. 27-33.

40. Ahmed, M. et al., 2012. An Advanced Survey on Cloud Computing and State-of-the-art Research Issues. International Journal of Computer Science Issues, 9(1), pp.pp. 201-207.

41. Nazir, M., 2012. Cloud Computing: Overview & Current Research Challenges. IOSR Journal of Computer Engineering (IOSR-JCE), 8(1), pp.pp. 14-22.

42. Sahu, Y. & Pateriya, R., 2013. Cloud Computing Overview with Load Balancing Techniques. International Journal of Computer Applications, 65(24), pp.pp. 40-44.

43. Singh A. & Malhotra M., 2015. Security Concerns at Various Levels of Cloud Computing Paradigm: A Review. International Journal of Computer Networks and Applications, 2(2), pp.pp. 41-45.

44. Hassan N. & Khalid A., 2016. A Survey of Cloud Computing Security Challenges and Solutions. International Journal of Computer Science and Information Security (IJCSIS), 14 (1), pp.pp. 52-56.

45. Varsha et al., 2015. Study of Security Issues in Cloud Computing. International Journal of Computer Science and Mobile Computing, 4(6), pp. pp. 230-234.