International Journal of Academic Research in Computer Engineering
Print ISSN: 2476-7638 and Online ISSN: 2538-2411
Vol. 1, No. 2, Pages. 44-49, November 2016

International Journal of Academic Research in Computer Engineering
Volume 1, Number 2, Pages 44-49, November 2016
www.ijarce.org
IJARCE

Data Storage Security in Cloud Computing: A Brief Review

Seyyed Keyvan Mousavi[1*], Davoud Shafiei[2] , and Mitra Khanjari Japelaghi[3]

1. Department of Computer Engineering, Miandoab Branch, Islamic Azad University, Miandoab, Iran.
2. Department of Computer Engineering, Meybod Branch, Islamic Azad University, Meybod, Iran.
3. Department of Computer Engineering, Central Tehran Branch, Islamic Azad University, Tehran, Iran.

Receive Date 2016.09.01; Accepted Date: 2016.11.10, Published Date: 2016.11.15

*Corresponding Author: S.K.Mousavi (k.mousavi2016@gmail.com)

Abstract
With the development of computer networks and in particular cloud computing and fast-moving organizations into unified information, the need for a secure environment for managing data in the Data Storage (DS) is felt. What distinguishes the cloud space for organizations in terms of security from traditional models is the lack of direct control of information and the probability of their improper management by cloud servers that can be considered the most important threat in the cloud computing model. DS plays a strategic role in the development of applications and communications in a cloud environment. As you know, the data can be in the form of text, audio, video, and etc. DS is used by combining a set of hardware and software instruments to store information and databases on the Web. The type of hardware used in DS and type of backup, the operating system and certain security and commercial applications set on it, will endow security and functionality to customers. The most important discussion in DS and its relationship with cloud environment is security; in this article, we will study data security in DS.

Keywords: Cloud Computing, Data Storage, Security.

1. Introduction

IT world is advancing rapidly, and the world's large servers known as DS are getting connected to the cloud computing technology. Implementation of servers based on features such as costs of design, installation, implementation, configuration, monitoring, maintenance, backup, and decline of systems' efficiency and difficulty of management and other problems have led IT experts to, designing virtual systems, run storage servers in the cloud environment, and hence, causing reduction in costs and increase of DS space, elasticity, scalability, high processing speed, and protecting the rights of producers [1]. Cloud computing is an approach that gives users the benefits provided by virtualization. In cloud computing, one can be simulated several large servers of DS in an environment and use them for DS [1]. Today, with the growing needs of users to different cloud computing services, DS is designed to involve the information and sensitive applications in a completely safe and expansible space [2]. DS is made of cloud computing infrastructure components that backup the Internet, e-commerce, and telecommunications sectors, and all DS services in the cloud environment must be highly safe [3].

For many organizations, the creation of technology to meet business needs is difficult. Budget, human resources, and constraints on storage devices are effective on the ability to create technologies needed. Cloud computing is a new approach to improve technology capabilities using applications accessible through the Internet. Fast growth of Cloud computing provides an opportunity for organizations to reduce intra-organization technology structures and use the Cloud

environment [4]. The main benefits of cloud computing technology are elasticity and scalability [5]. Cloud computing is elastic in providing the resources requested by the users. And the amount of memory and the number of processors is variable in this technology. Customers only pay for what they use in the cloud environment. Cloud systems have high error tolerability, and services provided by the cloud have higher availability.

When end users use cloud services and store their data in providers' infrastructure, the most crucial security aspects are related to privacy and confidentiality of users' data. End users want to know where their data is saved and who has access and control to their information and also they would like to be given guarantee so that no illegal access is given to their sensitive data by service providers. Other important security challenges related to cloud services are examined including:

Position of resources: End-users use services provided by cloud providers, without precise knowledge of where resources are located. When a security event occurs, it indicates a potential problem which sometimes goes beyond the control of cloud providers. Data stored by providers of cloud services providers are not only influenced by policy providers, but affected by the law of provider resident countries. When using these services, users must agree to the terms and requirements, according to which it grants the right to disclose user information by the adoption of laws and law enforcement requests to providers. For example, we can refer to the recent terms of Dropbox service. European Union has issued instructions to secure users' private information. According to the directive, the transfer of personal data to countries that do not show the appropriate level of protection and security is prohibited. The transfer of personal data outside the European Union countries is legally possible if this is done with the consent of the owner of the information. And this is done for a country that has security agreements of European Union.

Multi rent: This represents a challenge to protect users' data against unauthorized access by other users' processes running on similar physical servers, as there were previously shared hosting services. However, with the widespread use of cloud computing and by the fact that users store more important data in the cloud. This needs more serious examination.

Authentication and trust in the information: When important data is placed in the infrastructure of cloud providers, this data can be changed without the consent of the owner of the information. Modified data may be retrieved again and processed by the owner of information for performing key decisions. Authenticity of the data, in this case, is very important, and therefore, this should be guaranteed by the provider. However, there are no common standards to ensure the accuracy of the data.

Large organizations using cloud computing will be able to reduce their costs, and using cloud computing, they could easily eliminate the problems of storage and data integrity. Cloud computing because of low cost, high accessibility, and efficiency and many other facilities is a revolution in the IT industry. Cloud computing provides a large volume of data and quick computation for customers on the Internet. Although cloud computing provides a great range of facilities, but companies and organizations, due to security issues, are reluctant to distribute their information and applications in the cloud environment and cloud service providers [6]. Data security in the cloud is one of the main challenges to be considered as a barrier to run cloud computations. Cloud computing is often classified based on server models or extensibility. Models for cloud computing are classified as private, public, group, and hybrid cloud [7].

Private cloud: the ownership of a private cloud is on an organization or its rent. All major sources of private cloud are transferred to the organization. An example of this model is applied to use commercial and financial applications software's that contain sensitive and vital information of the organization.

- Public Cloud: public cloud ownership is on the service provider, and its resources are sold to the public. End users can rent parts of the resources and can often manage the cloud-based resources based on their need. Amazon, Google, and Microsoft are examples of public cloud providers.
- Group Cloud: group cloud is similar to private cloud. The difference is that cloud resources are established between members of a group or several private organizations with shared data. Also, group cloud can be run by a third party.
- Hybrid Cloud: hybrid cloud is a combination of two or more cloud infrastructures which may be private, public, or group. The main purpose of the hybrid cloud is usually allocation of additional resources for high demands.

The overall structure of this paper is organized as follows: In the Section 2, we examine the DS in cloud computing; in the Section 3, we will have

discussions; in the Section 4, conclusion and future works are explained.

2. Data Storage

With the development of web and addition of users to the environment, the volume of documents increases day by day. Therefore, Internet lines and servers are not able to respond to the huge amount of users' data. With the increase in the volume of users and documentations and also easy distribution of information on the Internet, business concepts have entered the Internet arena. Business firms need to have servers that give them the possibility to easily and quickly make their data available to their clients and users, and it is not possible that any company or organization that wants to set up its website launch its own server because due to large number of users of these sites and the high traffic volume, there is a need for extremely high-speed connections, Of course, even if this is possible in practice, there is a high price demand. The solution to this problem seems to be setting up special centers under DS. DS is a set of software and hardware equipment's established to host network and communication facilities to provide information services in cloud computing [8]. In Figure (1), DS architecture is shown in relation to a cloud environment.

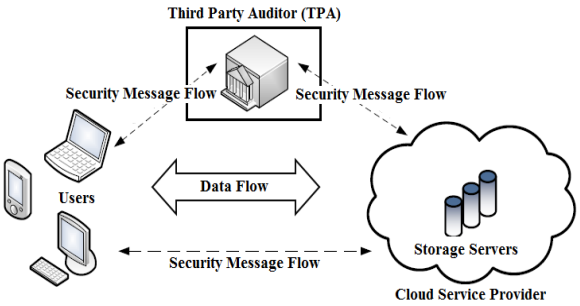

Figure 1: Cloud DS Architecture

Generally, DS is a place for storage, management, processing, exchange of digital information, and providing applications or management services for data processing [8]. The main goal of DS is providing web servers to users. Servers used are set according to the need and possibilities of the data. The design criteria for services provided in the DS include [9]: High Availability, Extensibility, Security, and Ability to manage.

Diversity and complexity of the business needs create competition for the provision of services tailored to enhance the efficiency and security. Organizing and DS operations must be designed to meet the information needs of users. Due to high volume of database, advanced servers are necessary for the operation of DS [9]. Also, a separate metadata database that describe attributes such as type, format, location, and authors of the data stored in the DS is needed to help users and administrators of data.

Role-Based Access Control (RBAC) model has been proposed for data security in Cloud environment [10]. It is applicable for large-scale cloud systems used to encrypt data from Equations (1) and Equation (2).

$$K' = (\hat{e}(C_1, h^{p_{i,M^{(s)}}}).\hat{e}(\frac{S_i}{H_2(K_i)}, C_2).D)^{\frac{1}{\Pi^{m}_{j=1,j\neq i} H_1(ID_{R_j})}}$$

$$where \quad p_{i,M^{(S)}} = \frac{1}{s}.(\prod_{j=1,j\neq i}^{m}(s + H_1(ID_{R_j})) - \prod_{j=1,j\neq i}^{m}(H_1(ID_{R_j})))$$

(1)

$$K_i = (\hat{e}(dkU_k, V_i).\hat{e}(W_i, h^{p_{k,N^{(s)}}}))^{\frac{1}{\Pi^{n}_{j=1,j\neq k} H_1(ID_{U_j})}}$$

$$where \quad p_{k,N^{(S)}} = \frac{1}{s}.(\prod_{j=1,j\neq k}^{n}(s + H_1(ID_{U_j})) - \prod_{j=1,j\neq k}^{n}(H_1(ID_{U_j})))$$

(2)

In Equation (1) using the key K', data encryption can be performed. Data security in the DS environment is done using Steganography technique [11]. Encryption is one of the main mechanisms, showing a strong defense against users' attempts to infiltrate data and attack infrastructure of DS. In the first stage, data are hidden in the image using mapping method, and in the second stage, data recovery is performed from the image. The evaluation results of MATLAB represent the efficiency and security of data using Steganography technique. Elliptic Curve Digital Signature Algorithm (ECDSA) model is used for encrypting data in the DS environment [12]. ECDSA method operates based on signature. In this method, all user data are in security mode.

Pretty Good Verification (PVG) model for data encryption DS has been done using algorithms of AES, RC4, MD5 and SHA1 [13]. The results show that AES algorithm has better performance compared with other algorithms. Secure DS and Processing Framework (SPF) framework is suggested for data security in DS [14]. SDSPF is provided to protect user data and security of static and dynamic data. In this framework, the data are transferred and stored as encryption. In SDSPF model, Attestation Component and Data Processing Security Manager are used. PDDS model is suggested for higher security of data stored in DS [15]. In PDDS model, encryption and decryption of data is done using RSA algorithm. The results show that, in PDDS model, the volume and DS time are reduced. Merkle Hash Tree (MATH) model is suggested for security and control access to data [16]. In this method, the key management is done based on tree

and allows data source to access data by multiple nodes which requires with fewer bits for key length to make key encryption from Elliptic Curve Cryptography (ECC) of ECC algorithm, compared to RSA. The results show that ECC accrues out encryption and decryption operations in less time.
Cloud Data Owner-Cloud Data User (CDO-CDU) model [17] to enhance security and user access to cloud data has been suggested. In the CDO-CDU model, access control has been defined for each user. In the access control section, the data access is in the form of hashing and for access, the digital signature is required. MD5 model is used for encrypting of data. Dynamic Merkle Hash Tree (DMHT) model [18] based on RSA and AES techniques was suggested for dynamic data. In DMHT model, the blocking was used to encrypt data. The results show that AES model has better performance in comparison with the RSA and block the data in less time. Model of MTH-RSA [19, 20] in order to block the data has been suggested in less time. The main purpose of this model is to enhance the security of MTH model reduce the time of data encryption. The results show that MTH-RSA model has better performance in comparison with the MTH and better blocks the data with high-volume. In Table (1), the characteristics of the proposed models has been investigated for the security of the DS.

Table 1: Comparison of Security Models in DS

Model	Encryption Algorithm	Digital Signature	Access Control	Execution Time
RBAC [10]	RSA	√	X	Normal
Steganography [11]	Hash	X	X	High
ECDSA [12]	Hash	√	√	Normal
PVG [13]	AES,RC4, MD5,SHA 1	X	√	Normal
SDSPF [14]	Hash	√	X	Low
PDDS [15]	RSA	X	X	Low
MTH [16]	RSA	√	√	High
CDO-CDU [17]	MD5	√	√	Low
DMHT [18]	RSA,AES	√	X	Normal
MTH-RSA [19]	RSA	√	X	High

3. Discussion

Cloud computing is solution for increasing storage capacity and adding dynamic capabilities to the data, without investment on training new recruits and without spending costs for new software's. In the past few years, cloud computing has been transformed, from a potential business concept, into one of the fastest growing areas in IT industry. However, by increasing the companies' data in the cloud, concerns have increased in the context that what' cloud environment status with respect to security. Regardless of all the capabilities in the cloud, customers are still reluctant to put their business in the cloud. Security is one of the issues that reduces the growth of cloud computing. And complexities related to data privacy and data protection are still incomprehensible issues for cloud computing technology. Security is a very complex area for users of cloud services and cloud service providers and the most fundamental concerns of consumers of cloud services. Most organizations and firms have a combined environment including public and private cloud, in which the systems within the organization get connected to the cloud environments, causing a security risk and security complication. Having a strong strategy, to deal with potential threats when using cloud services, is essential for an organization. Data integration and security strategy from CSP is the basic principle for organizational strategies which should use identity management, encryption, and data discovery for data of DS. In Table (2), security solutions for DS are shown.

Table 2. Security Solutions for DS

1.	Set access permissions so that users only have access to the programs and data that they have been given access to.
2.	Validation of all the people who have access to the Cloud network.
3.	Validation of all applications that run on the DS.
4.	Taking advantage of the tools and the logical access control systems to the data
5.	Registration and alarm systems in case of possible cyber-attacks on DS
6.	Providing backup servers from DS databases
7.	Performing security assessments and penetration tests on an ongoing basis and at regular intervals
8.	Use of cryptographic algorithms for data storing in DS
9.	Using security protocols such as SSL for Cloud communications and outside of the DS
10.	Prevention and repair of software and hardware errors and denial of malicious accesses to the data
11.	Privacy or usability of the data determined only by authorized user and within certain framework
12.	The limitations of the database including database type, authentication of the database, database security
13.	Operating system security including the type of operating system and operating system services.

The most important issue facing the cloud formation in its construction and architecture is the security issue. Many techniques and technologies are used and developed to provide high levels of security. Many secret methods are used to detect security that lead to the complexity of the task, and it seems that it disrupts the performance of the cloud environment. Currently, only some of these methods are applicable; not only are they registered and classified, but also track and monitor users' action. To create the comprehensive security

mechanism for data and programs in the cloud environment, at the first step, we should avoid un-trusted activities which are applicable using reliable and robust mechanisms. And overall, principles and practices that limit the access to the system or prohibit login to it or permit it must be identifiable for access control. In addition, it is possible that all documents and evidences and all the actions that have been logged in become identified by an invalid user and strive to attain the system.

Governmental organizations and private firms' intelligence infrastructures host highly valuable data. Various types of attacks and threats such as virus attacks and network intrusion always threat cloud intelligence infrastructures. These threats can impose irreparable damages to data and services. This damage can include loss of valuable customer data and credit of organizations. With the growing of security threats, the importance of addressing cloud security infrastructures becomes more visible. That is why in recent years, many security solutions have attracted the attention of developers, manufacturers, network operators, and managers of organizations for security of cloud computing environments and DS. Although the use of protective strategies is effective in preventing some attacks and security threats, but alone will not supply security. Discovered attacks and threats must be registered as a non-real-time quote. The announcement can be done through various mediums such as notification via the console data center, sending an e-mail, and texting. With these methods, experts of operations center can act and show the best reaction to penetration in the shortest time possible. The reactions can include preventing the spread of penetration and, if necessary, return of the systems to the previous status. Security in the cloud environment in each of the areas of operating systems, databases, hardware, and software should be examined separately. Security Tips should also be considered in software s' production of DS environment, in which software act independently, and vulnerability of the DS context does not damage data of organizations. For software independence, all protocols and interactions of the software with DS substrate should be run as standard.

4. Conclusion and Future Works

Using of cloud computing as a technology with great potential is increasing dramatically. In the case that the highest contribution to the world of technology and future communications technologies will be cloud computing. From the most important obtained results of cloud computing can be mentioned to the increase of customer access to various services, improve of productivity and efficiency, resource management and reduction of costs. In addition, improving the ability to meet the needs of its customers and accelerating the benefits of cloud computing is the other operation of the loud computing. DS is the main source of the data saving in the cloud environment that its data must be encrypted for more security. So in this article, we considered security and user access control in a cloud environment and concluded that we can present more efficient model for DS security using a combination of encryption algorithms in the future.

REFERENCES

[1] S.L Lee, G., Sung Jong, L., Im-Yeong, Secure Method for Data Storage and Sharing During Data Outsourcing, Information Technology Convergence, Vol. 253, pp. 485-493, 2013.

[2] M. Sookhak, A. Gani, M.K. Khan, R. Buyya, Dynamic Remote Data Auditing for Securing Big Data Storage in Cloud Computing, Information Sciences, 2015.

[3] C.Wang, Q.Wang, K. Ren, and W. Lou, Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing, IEEE 29th International Conference. Computer Comm. (INFOCOM), pp. 525-533, 2010.

[4] F.S. Gharehchopogh, R. Rezaei, I. Maleki, Mobile Cloud Computing: Security Challenges for Threats Reduction, International Journal of Scientific and Engineering Research (IJSER), Vol. 4, No. 3, pp. 8-14, March 2013.

[5] Q. Wang, C. Wang, K. Ren, W. Lou, J. Li, Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing, IEEE Transactions on Parallel and Distributed Systems, Vol. 22, No. 5, pp.1-13, May 2011.

[6] Z.A. Khalifehlou, F.S. Gharehchopogh, Security Directions in Cloud Computing Environments, 5th International Conference on Information Security and Cryptology (ISCTURKEY2012), Ankara, Turkey, pp. 327-330, 17-19 May 2012.

[7] H. Takabi, J.B.D. Joshi, G.Ahn, Security and Privacy Challenges in Cloud Computing Environments, IEEE Security Privacy Magazine, Vol. 8, IEEE Computer Society, pp.24-31, 2010.

[8] N. Kolsi, A. Abdellatif, K. Ghedira, Agent Based Dynamic Data Storage and Distribution in Data Warehouses, Agent and Multi-Agent Systems:

Technologies and Applications, Vol. 4469, pp. 375-384, 2007.

[9] G. Xu, C. Chen, H. Wang, Z. Zang, M. Pang, P. Jiang, Two-Level Verification of Data Integrity for Data Storage in Cloud Computing, Advanced Research on Electronic Commerce, Web Application, and Communication, Vol. 143, pp. 439-445, 2011.

[10] L. Zhou, V. Varadharajan, M. Hitchens, Secure Administration of Cryptographic Role-Based Access Control for Large-Scale Cloud Storage Systems, Journal of Computer and System Sciences, Vol. 80, No. 8, pp.1518-1533, 2014.

[11] M.K. Sarkar, T. Chatterjee, Enhancing Data Storage Security in Cloud Computing Through Steganography, International Journal on Network Security, Vol. 5, No. 1, pp. 13-19, 2014

[12] M.I. Husain, S. Y.Ko, S. Uurtamo, A. Rudra, R. Sridhar, Bidirectional Data Verification for Cloud Storage, Journal of Network and Computer Applications, Vol.45, pp.96–107, 2014.

[13] K. HariPriya, P. Krishnamoorthy, An Efficient Cloud Storage with Secure Dynamic Data Modification, International Journal of Computer Trends and Technology (IJCTT), Vol. 4, Issue5, pp. 1075-1079, 2013.

[14] L. Ran, H. Jin, SDSPF: A Secure Data Storage and Processing Framework for Cloud Computing Systems, ITCS & STA 2012, LNEE 180, pp. 127–133, 2012.

[15] C. Selvakumar, G. Jeeva Rathanam, M. R. Sumalatha, PDDS - Improving Cloud Data Storage Security Using Data Partitioning Technique, IEEE, pp. 7-12, 2012.

[16] T.K. Chakraborty, A. Dhami, P. Bansal, T. Singh, Enhanced Public Auditability & Secure Data Storage in Cloud Computing, IEEE, pp. 101-106, 2012.

[17] H.B. Patel, D.R. Patel, B. Borisaniya, and A. Pate, Data Storage Security Model for Cloud Computing, Social Informatics and Telecommunications Engineering, CNC 2012, LNICST 108, pp. 37-45, 2012.

[18] P.M. Pardeshi and B. Tidke, Improvement of Data Integrity and Data Dynamics for Data Storage Security in Cloud Computing, Information Systems Design and Intelligent Applications, Advances in Intelligent Systems and Computing, Vol. 339, pp. 279-289, 2015.

[19] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing, ESORICS 2009, LNCS 5789, pp. 355-370, 2009.

[20] F.S. Gharehchopogh, M.Bahari, Evaluation of the Data Security Methods in Cloud Computing Environments, International Journal in Foundations of Computer Science & Technology (IJFCST), Vol: 3, No: 2, pp. 41-51, 2013.