International Journal of Grid Distribution Computing
Vol.7, No.4 (2014), pp.11-20
http://dx.doi.org/10.14257/ijgdc.2014.7.4.02

Encryption Techniques for Cloud Data Confidentiality

Aized Amin Soofi[1], M.Irfan Khan[1] and Fazal-e-Amin[2]

[1]*College of Computer Science and Information Studies, Government College University, Faisalabad, Pakistan*
[2]*College of Computer and Information Sciences, King Saud University, Riyadh, KSA*
aizedamin@yahoo.com, softchannel2000@hotmail.com , fazal.e.amin@gmail.com

Abstract

Cloud computing is one of the fastest growing internet based technology that facilitates users to utilize services by making use of large poll of resources without installation of any software. Adoption of this technology is increasing rapidly because of many advantages including reduction of cost and IT load. Despite the popularity of cloud computing, it faces many difficulties such as security that is one of the major inhibitors in the growth of cloud computing. Data confidentiality is at the top of the list of security concern for this technology. Many methods have been introduced to overcome this issue; encryption is one of them and widely used method to ensure the data confidentiality in cloud environment. In this study, an attempt is made to review the encryption techniques used for the data confidentiality. The results of review are classified on the basis of type of approach and the type of validation used to validate the approach.

Keywords: *Cloud data security, Data concealment, Data Encryption, Encryption algorithm*

1. Introduction

Cloud computing is the use of computing resources (hardware and software) that are shared as services over the internet. It is called "Cloud" computing because a cloud shaped symbol is often used to represent bulky networks especially the internet. Cloud Computing is defined by a major distributed computing pattern that is obsessed by economies of scale, in which a pool of virtualized, abstracted, managed computing power, storage, platforms, and services are delivered on demand to users over the Internet [1]. According to the NIST definition, cloud computing can be defined as a model for enabling useful, on-demand network access to a shared pool of configurable computing possessions [2].

According to Gartner [3] cloud computing can be defined as a technique of computing that delivered IT facilities 'as a service' to end users through internet. Foreign large companies such as Google, IBM, Amazon, Microsoft and Yahoo are leading the way in cloud computing. Many other companies like Myspace, Facebook, Salesforce and YouTube, also make an achievement in cloud computing [4].

The service models of cloud computing are divided into three categories: (1) IaaS (infrastructure as a service), it completely distracted the hardware working behind it and allowed users to consume infrastructure as a service without any inconvenience about the underlying complexities. (2) PaaS (plat form as a service), it builds upon IaaS and provides clients with access to the basic operating software and optional services to develop and use software applications without software installation. (3) SaaS (software as a service) enables the user to access online applications and software that are hosted by the service providers.

ISSN: 2005-4262 IJGDC

The deployment model of cloud computing include (1) Public cloud, which is owned by service provider and its resources are rented or sold to the public. (2) Private cloud, owned or rented by an organization. (3) Community cloud, similar to private cloud but cloud resources is shared among number of closed community. (4) Hybrid cloud, exhibits the property of two or more deployment models [5].

According to survey conducted by International Data Group (IDG) enterprise, the top three challenges to implementing a successful cloud strategy in enterprise vary significantly between IT and line-of-business (LOB). For IT, concerns regarding security is 66% and 42% of cloud-based projects are eventually brought back in-house, with security concerns 65% [6]. Many vendors declared that adoption of this technology can bring many benefits to the users such as cost reduction, convenience and continuous availability, scalability and performance, quick deployment and ease of integration, yet some organization are still not feeling comfortable in adoption of this technology due to concerns of trust and security *e.g.*, data security is one of them [7, 8].

In our previous work [9] the importance of data security issues and some of its solutions in cloud environment was discussed and it was also highlighted that encryption is the most widely used method to ensure the security of data in cloud. One of the best ways to ensure confidentiality of secret data in the cloud is to utilize encryption for data. Almost all cloud service providers support encryption for data storage [10]. Encryption plays a big role in fulfillment as many policies need specific data components to be encrypted. To protect a user‘s secret data in the cloud, encryption is considered as influential tool that can be used efficiently. User can confidently utilize cloud services by knowing that their confidential data is protected by encryption.

Security goals of data include three points which are Confidentiality, Availability and Integrity. Confidentiality of data in the cloud can be achieved by cryptography. Data cryptography is the shuffling of the content of the data, such as text, image, audio, video to make the data meaningless, unreadable or invisible during transmission or storage is termed Encryption. The main role of encryption is to take care of data secure from attackers. The process of getting back the original data from encrypted data is Decryption, which refurbish the original data. Both symmetric-key and asymmetric-key algorithms can be used to encrypt data in cloud storage.

2. Methodology

A systematic review is a means of evaluating and understanding all available research relevant to a particular research question or phenomenon of interest. A systematic literature review presented in [11] is followed in this research work to conduct the review about encryption methods used in cloud computing for data confidentiality. Some researchers provide a review on security issues in cloud computing but this review aims to focus on the encryption methods used to resolve the security issue of the data confidentiality in cloud environment.

Many researchers contribute their efforts in the field of software engineering/computer science by adopting [11] systematic literature review process such as in [12, 13] systematic literature review process was adopted for the review of aspect oriented implementation of software product lines components and software component reusability assessment approaches. In [14] systematic review process was followed for the analysis of security issues in cloud computing. In [9] systematic review process was adopted to conduct a review on data security in cloud computing.

2.1. Question Formalization

The posed questions relate with the aim of this work; that is to identify the encryption approaches and validation of these approaches. Therefore, the research questions addressed by our research are following:

Question 1: What encryption approaches have been used to ensure data confidentiality in cloud computing?
Question 2: How the approaches have been validated?

The keywords and related concepts that make up these questions and that were used during the review execution are cloud computing, cloud data security, data confidentiality, encryption and data encryption in cloud.

2.2. Selection of Sources

The selection criteria through which we evaluated study sources was based on the research experience of the authors of this work, and in order to select these sources we have considered certain limitation: studies included in the selected sources must be related to our research questions and these sources must be web-available. The review protocol is developed by using the above mentioned keywords and the following list of sources has been considered to conduct the systematic review: ACM digital library, IEEE Xplore, Science Direct Scopus and Google Scholar. This protocol is reviewed and validated after making some changes by researchers.

Another step in the search procedure is performed by searching the related work area of the selected papers to boost the review strength by confirming that no valuable reference is missed during the search process. Once the sources had been defined, it was necessary to describe the process and the criteria for study selection and evaluation. The inclusion and exclusion criteria for this study based on the research question. We therefore established that the studies must contain data related to our research questions i.e. encryption technique for data confidentiality in cloud environment. The research focuses on the year's 2007 to 2014. The final review protocol is shown in Table 1.

Table 1. Review Protocol

Year	Sources	Keywords
2007-2014	IEEE Xplore, Science direct, Scopus, Google scholar, ACM portal digital library	Cloud computing, Cloud data security, Data confidentiality, Encryption, Data encryption in cloud.

2.3. Review Execution

During this phase, the search in the defined sources must be proceed and the obtained studies must be evaluated according to the defined criteria for the review. After executing the search chain on the selected sources we obtained a set of about 53 results which were filtered with the inclusion criteria to give a set of about 22 relevant studies. This set of relevant studies was again filtered with defined exclusion criteria to give a set of studies which corresponds with 15 primary proposals. [15-29].

3. Results

The results of the review are presented in this section. A year wise result representation is presented in Table 2. The results are characterized with respect to the questions posed earlier.

Table 2. Year Wise Search Results

Year	No. of papers
2007	0
2008	1
2009	0
2010	2
2011	2
2012	4
2013	5
2014	1
Total	15

Question 1: What encryption approaches have been used to ensure data confidentiality in cloud computing?

The result of review defined in figure 1 shows the proposed encryption based approaches for the data security in cloud computing. The result is categorized into: (1) RSA, a cryptographic algorithm whose encryption key is public and differs from the decryption key which is kept secret. (2) Data Encryption Standard (DES) and Simplifies Data Encryption Standard (S-DES), where DES used symmetric key for encryption and decryption. (3) Secure Socket Layer (SSL) 128 bit encryption, it is commonly-used protocol for managing the security of a message transmission on the Internet and it uses public and private key encryption system. (4) Mixed encryption algorithms. (5) RC5 which is a symmetric key block cipher and it consists of a number of modular additions and Exclusive OR (EXOR). (6) Role Base Encryption (RBE), it enhances the protection of application data from unauthorized access. (7) Geo encryption, location based encryption and decryption of data. (8) Proxy re-encryption (PRE) and Hierarchical attribute-based encryption (HABE). The categories wise results are summarized in Table 3.

Table 3. Category Wise Result of Question 1

Question	Category	No. of papers
What encryption approaches have been used to ensure data confidentiality in cloud computing?	RSA	5
	DES and SDES	1
	SSL 128 bit encryption	2
	Mixed encryptions algorithms	1
	RC5	1
	RBE	1
	AES	2
	GEO encryption	1
	PRE and HABE	1
	Total	15

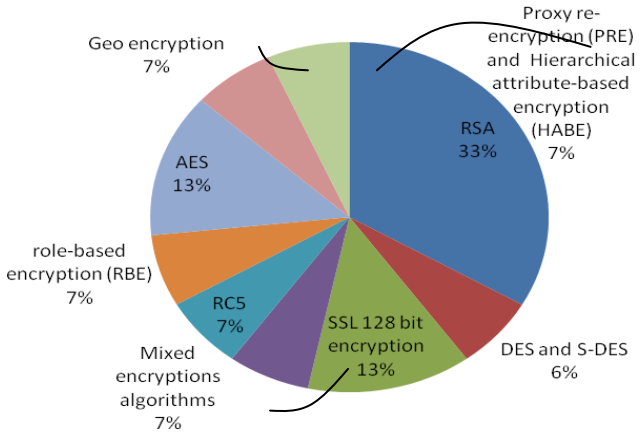

Figure 1. Proposed Approaches to Ensure Data Security using Encryption Techniques

In [16] a digital signature with RSA algorithm scheme is proposed to ensure the data security in cloud. In which software used to crunch down the data documents into few lines by using "hashing algorithm". These lines are called message digest then software encrypts the message digest with its private key to produce the digital signature. Digital signature will be decrypted into message digest by the software with own private key and public key of sender.

In [18] the cloud data security is assured by utilizing the RSA algorithm in which data and Bilinear Diffie-Hellman encrypted while keeping the keys exchanged. The technique which used is the addition of message header in the front of every data packet. When a cloud server receives a request for data storage from a user then it uniquely generates the user public and private key with user identification in certain server (SID) for user. After that it sends the user secret key and unique identification to user for the server. Before a user sends the file to cloud two tasks are performed at user end. Firstly, a message header is added to the data and secondly, data is encrypted including message header by using secret key. When a user will make a request for data to cloud server then it will pick the SID information and also will check the message header of received data.

In [19] two important encryption techniques playfair and vigenere incorporated with the structural elements of SDES and DES. In which a fixed block sized 64 bit plain text is considered and divided into two parts by the means of black box. The right part contains 2 bits while left part contains 6 bits, then for the further divisions of these 6 bits they are injected into "superior function" block where they divided in two parts in which first two bits express the rows and last four bits express the column. The corresponding value can be selected by recognizing the rows and columns. Then this function is implemented to all 8 octets vigenere block output and the resultant of black box is again of 64 bits. Four new octants are created by the further division of these bits and similarly right 4 bits are combined for the formulation of right parts. Lastly, left and right parts are XOR-ed to get the left half of this arrangement. Three times this process is repeated.

In [20] a technique for ensuring the confidentiality, availability and integrity of data cloud data is introduced in which SSL 128 bit encryption is used which can be then increased to 256 bit encryption. To access the encrypted data a user is required to provide valid user identity and password. A three layered based data security model is proposed in [21] where every single layer perform different task to secure data in cloud. First layer performs the task of authentication, second layer is responsible for data encryption and third layer perform the task

of data recovery. Additionally, at cloud end a software is implemented with two aspect authentication. One characteristic of this software is that it compares the eight recent encryption algorithms and to get the fastest and highest security algorithm which is based on cloud infrastructure.

In [22] RC5 an algorithm is implemented for the sake of cloud data security in which encrypted data is transmitted even if the data is stolen because there will be no relevant key to decrypt this data. In [23] Role Base Encryption (RBE) technique is suggested for cloud data security and role base access control (RBAC) cloud architecture for organizations in which they can store data securely in public cloud, whereas information about the organization's structure is maintained in private cloud. In [24] four authorities (data owner, data consumer, cloud server and N attribute authorities) are explained and attribute authorities sets were divided into N disjoint sets according to their category. The data owner will get the public key from any one of the authority and will encrypt the data before sending it to the cloud server. When data will be requested then the private key will be created by authorities and delivered to data consumer after that the consumer will be able to download the file if and only if he or she satisfies the related authority tree and approved by cloud server.

In [25] two secured cloud computing types are suggested in which one type needed a trusted third party but the other does not. These types use Elliptic Curve Diffie-Hellman (ECDH) and symmetric bivariate polynomial based secret sharing to ensure the data security in cloud environment. For the protection of cloud data confidentiality, a technique proposed in [26] in which digital signature and Diffie Hellman key exchange are used with Advanced Encryption Standard encryption algorithm. This scheme provides data security, verification and authentication simultaneously therefore known as three way approach. In [27] a method that was based on location encryption proposed for cloud data security in which geographical position and user location were used. In that method a geo encryption algorithm was applied on the cloud and user computer and then a label which identify the person or company was used on data. So, when the data will be required then the same label will be searched and retrieved and the information related to label will be retrieved from the cloud. After that data will encrypt by using Geo-Encryption algorithm along with information that was retrieved from cloud and then data will be delivered to user.

Question 2: How the approaches have been validated?

Figure 2 shows the result of review as regards to the procedure adopted for validation. The categories are: (1) Experiment where an experiment is carried out to validate the results. (2) Comparative analysis where the results of proposed scheme is compared to other schemes to validate the results. (3) Statistical analysis where the results are analyzed by using some statistical technique. (4) Some of the proposed approaches have not performed any validation. The category wise detail is presented in table 4 and fig 3 shows the type of validation in percentage. Let us explain the term validation. It refers to any kind of empirical method used as a proof apart from the manifestation of the proposed approach.

Table 4. Categories Wise Results of Question 2

Question	Category	No. of papers
How the approaches have been validated?	Comparative analysis	3
	Experiment	6
	No validation	5
	Statistical analysis	1
	Total	15

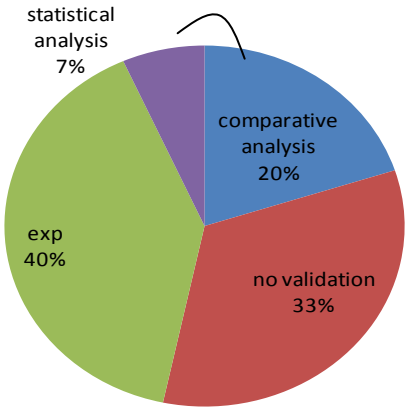

Figure 2. Types of Validation

The results of the question regarding validation of proposed encryption approaches show that 40% of the selected papers used experimentation to validate their proposed approach while 33% of the proposed techniques provide no validation.

In [20] cloud simulator named Hadoop was used to perform an experiment in order to test the validity of proposed model. It illustrated the security status after implementing three security parameters which are; Message Authentication Code, classification of data, index and encryption technique. In [22] Aneka 2.0 software was used in cloud environment for the validation of obtained results by the implementation of RC5 algorithm and then compared these results with Amazon S3 service. Aneka allows to buld and manage an interconnected network by using Microsoft .NET frameworks on these networks. In [23] proposed architecture was implemented in Java and results show that cipher text size is linearly proportional to the size of the plaintext with very good encryption and decryption efficiency. Results also show that the size of the decryption key is 48 bytes which is convenient for the users.

In [15] comparative analysis was made to validate the results by considering variables *i.e.* granularity, key management, degree of distribution, metadata management, level of implementation and level of concealment. In [25] comparative analysis was made between data Privacy by Authentication and Secret Sharing (PASS) and proposed technique that used trusted third party and non trusted third party. In [19] proposed encryption technique was compared with DES, SDES, Vigenere and Playfair encryption techniques for the validation of proposed approach results. In [21] sixteen NIST statistical tests were performed to validate the results by selecting eight modern encryption algorithms.

4. Conclusion

Cloud computing is latest development that provides easy access to high performance computing resources without installation of software. It provides many benefits for its users but it suffers with some security threats. Security of data is one of the top list impediments in the growth of this latest technology. In this study we provide an introduction of cloud computing with the importance of data confidentiality in this domain. A literature review of the works regarding to usage of encryption techniques in the area of cloud computing data security is conducted and the results of review are presented in this paper. The results show that the majority of approaches are based on RSA encryption is 33% out of which 60% RSA

encryption techniques results are validated by experiments. These results point towards the fact that most of researchers show their interest in RSA encryption technique for confidentiality of data in cloud computing environment. The results also reveal the fact of lack of validation in proposed approaches as 33% of the studies provide no validation of the results. This validation area needs the attention of the research community to gain the trust and confidence of cloud computing users.

References

[1] I. Foster, Z. Yong, I. Raicu and L. Shiyong, (2008, 12-16 Nov. 2008), Cloud Computing and Grid Computing 360-Degree Compared, Paper presented at the Grid Computing Environments Workshop, 2008, GCE '08.
[2] NIST SP 800-145, "A NIST definition of cloud computing", [online] 2012, http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf (Accessed: 23 December (**2013**).
[3] Gartner, "What you need to know about cloud computing security and compliance", (HeiserJ), [online] 2009, https://www.gartner.com/doc/1071415/need-know-cloud-computing- Security (Accessed 23 December 2013).
[4] Z. Yandong and Z. Yongsheng, "Cloud computing and cloud security challenges in Information Technology in Medicine and Education (ITME)", 2012 International Symposium on, (**2012**), pp. 1084-1088.
[5] IBM, "what is cloud computing" [online] http://www.ibm.com/cloud-computing/in/en/what-is-cloud-computing.html (Accessed: 14 December 2013).
IDG Cloud Computing Survey: "Security, Integration Challenge Growth", [online], http://www.forbes.com/sites/louiscolumbus/2013/08/13/idg-cloud-computing-survey-security-integration-challenge-growth.html/(Accessed: 28 December 2013).
[7] D. Catteddu and G. Hogben, "Cloud computing: Benefits, risks and recommendations for information security", European Network and Information Security Agency (ENISA), pp. 1–125.
[8] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications, vol. 34, no. 1, (**2011**), pp. 1-11.
[9] A. A. Soofi and M. I. K Fazal-e-Amin, "A Review on Data Security in Cloud Computing", International Journal of Computer Applications, vol. 94, no. 5, (**2014**), pp. 12-20.
[10] T. Dillon, C. Wu and E. Chang, "Cloud computing: issues and challenges", Paper presented at the Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on. (**2010**).
[11] P. Brereton, B. A. Kitchenham, D. Budgen, M. Turner and M. Khalil, "Lessons from applying the systematic literature review process within the software engineering domain", Journal of Systems and Software, vol. 80, no. 4, (**2007**), pp. 571-583.
[12] A. K. M. Fazal-e-Amin and A. Oxley, "A review on aspect oriented implementation of software product lines components", Information Technology Journal, vol. 9, no. 6, (**2010**), pp. 1262-1269.
[13] A. K. M. Fazal-e-Amin and A. Oxley, "A Review of Software Component Reusability Assessment Approaches", Research Journal of Information Technology, vol. 3, no. 1, (**2011**), pp. 1-11.
[14] K. Hashizume, D. Rosado, E. Fernández-Medina and E. Fernandez, "An analysis of security issues for cloud computing", Journal of Internet Services and Applications, vol. 4, no. 1, (**2013**), pp.1-13.
[15] R. Anane, S. Dhillon and B. Bordbar, "Stateless data concealment for distributed systems", Journal of Computer and System Sciences, vol. 74, no. 2, (**2008**), pp. 243-254.
[16] U. Somani, K. Lakhani and M. Mundra, "Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing", Paper presented at the Parallel Distributed and Grid Computing (PDGC), 2010 1st International Conference on. (2010, 28-30 Oct. 2010).
[17] W. Cong, C. Ning, L. Jin, R. Kui and L. Wenjing, "Secure Ranked Keyword Search over Encrypted Cloud Data", Paper presented at the Distributed Computing Systems (ICDCS), 2010 IEEE 30th International Conference on. (2010, 21-25 June 2010).
[18] H. Shuai and X. Jianchuan, "Ensuring data storage security through a novel third party auditor scheme in cloud computing", Paper presented at the Cloud Computing and Intelligence Systems (CCIS), 2011 IEEE International Conference on. (2011, 15-17 Sept. 2011).
[19] Vamsee and Sriram, "Data Security in Cloud Computing," in Journal of Mathematics and computer sciences, vol. 2, no. 1, (**2011**), pp. 15- 23.
[20] S. K. Sood, "A combined approach to ensure data security in cloud computing", Journal of Network and Computer Applications, vol. 35, no. 6, (**2012**), pp. 1831-1838.

[21] E. M. Mohamed, H. S. Abdelkader and S. El-Etriby, "Enhanced data security model for cloud computing", Paper presented at the Informatics and Systems (INFOS), 2012 8th International Conference on. (2012, 14-16 May 2012).
[22] J. Singh, B. Kumar and A. Khatri, "Improving stored data security in Cloud using Rc5 algorithm", Paper presented at the Engineering (NUiCONE), 2012 Nirma University International Conference on. (2012, 6-8 Dec. 2012).
[23] Z. Lan, V. Varadharajan and M. Hitchens, "Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage", Information Forensics and Security, IEEE Transactions on, vol. 8, no. 12, (**2013**), pp. 1947-1960.
[24] J. Taeho, L. Xiang-Yang, W. Zhiguo and W. Meng, "Privacy preserving cloud data access with multi-authorities", Paper presented at the INFOCOM, 2013 Proceedings IEEE, (2013, 14-19 April 2013).
[25] Y. Ching-Nung and L. Jia-Bin, "Protecting Data Privacy and Security for Cloud Computing Based on Secret Sharing", Paper presented at the Biometrics and Security Technologies (ISBAST), 2013 Internationa Symposium on. (2013, 2-5 July 2013).
[26] P. Rewagad and Y. Pawar, "Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing. Paper presented at the Communication Systems and Network Technologies (CSNT), 2013 International Conference on. (2013, 6-8 April 2013).
[27] M. S. Abolghasemi, M. M. Sefidab and R. E. Atani, "Using location based encryption to improve the security of data access in cloud computing", Paper presented at the Advances in Computing, Communications and Informatics (ICACCI), 2013 International Conference on. (2013, 22-25 Aug. 2013).
[28] Kalpana and singaraju, "Data Security in Cloud Computing using RSA Algorithm," in International Journal of Research in Computer and Communication technology (IJRCCT), vol. 1, no. 4, (**2012**).
[29] Q. Liu, G. Wang and J. Wu, "Time-based proxy re-encryption scheme for secure data sharing in a cloud environment", Information Sciences, vol. 258, (**2014**), pp. 355-370.

Authors

Aized Amin Soofi, he is currently a student of MS (computer science) in Government College University Faisalabad, Pakistan. His research interests include network security and cloud computing.

Irfan Khan, he is is currently serving as a lecturer in Government College University Faisalabad, Pakistan. His areas of interest include programming languages, compiler construction, web development and cloud computing.

Fazal-e-Amin, he received the BS degree in computer science from Hamdard University in 2003. He received Master's degree in information technology from Quid-i-Azam University in 2005 and Master's degree in software engineering from International Islamic University in 2008. He received PhD degree from Department of Computer and Information Sciences, Universiti Teknologi PETRONAS in 2012. His research interests include open source software, data security, cloud computing, and C4I systems.

