Advances in Computer Science and Information Technology (ACSIT)
Print ISSN: 2393-9907; Online ISSN: 2393-9915; Volume 2, Number 3; January-March, 2015 pp. 276-280

http://www.krishisanskriti.org/acsit.html

Encryption Techniques in Cloud Computing

Meena Kumari[1] and Rajender Nath[2]

[1]PhD Research Scholar, Department of Computer Science and Applications Kurukshetra University, Kurukshetra, Haryana, India
[2]Professor, Department of Computer Science and Application Kurukshetra University, Kurukshetra, Haryana, India
E-mail: [1]sanger.meena@gmail.com, [2]rnath2k3@gmail.com

Abstract—*Cloud computing is the apt technology for the decade. It allows user to store large amount of data in cloud storage and use as and when required, from any part of the world, via any terminal equipment. Since cloud computing is rest on internet, security issues like privacy, data security, confidentiality, and authentication is encountered. In order to get rid of the same, a variety of encryption algorithms and mechanisms are used. 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.*

Keywords: *Cloud Computing, Encryption, Confidentiality, Integrity, Authorization.*

1. INTRODUCTION

Cloud computing is under development, there are no widely accepted unified definition. In different stages of development or from a different perspective has a different understanding on the cloud. There are many definitions [2-4] of cloud computing given by various authors. U.S. National Institute of Standards and Technology (NIST) definition is one of the clearest and most comprehensive definitions of cloud computing and is widely referenced. The NIST definition summarizes cloud computing *as 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* [5]. Although there are still many internet forum and blog discussions on what cloud computing is and is not, the NIST definition seems to have captured the commonly agreed aspects of cloud computing that are mentioned in most of the academic papers published in this area.

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.

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 [1].

Cloud computing is envisioned as the next-generation architecture of IT Enterprise, which aims to consolidate the economic utility model with the evolutionary development of many existing approaches and computing technologies, including distributed applications, services, and information infrastructures consisting of pools of computers, networks, and storage resources. Via cloud computing, users can uniformly access distributed resources on the internet on demand. It generates great interest in IT industry. Many big companies such as IBM, Google, Amazon, Microsoft, Yahoo and others accelerate their pace to develop cloud computing platforms, and business enterprises strive to utilize cloud computing to create new business models to improve service efficiency. However, cloud computing is filled with security risks. In cloud computing, data is processed and stored in cloud, not in the owner's local computer any more, which introduces potential security issues.

In this paper, an attempt is made to review the encryption techniques used for the data confidentiality. A systematic literature review presented in [6] 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.

The rest of the paper is organized as follows: Section II gives the review method and Section III summarizes the result and Section IV presents concluding remarks.

2. REVIEW METHOD

A systematic literature review endeavor to provide a comprehensive review of current literature relevant to a specified research questions. A systematic literature review presented in [6] is followed in this research work to conduct the review about encryption methods used in cloud computing for data confidentiality.

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 this paper 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.

a. Selection of Sources

In order to select sources this paper has considered certain limitation such as studies included in the selected sources must be related to above mentioned research questions and these sources must be available online. The review protocol is developed by using the above mentioned keywords and the following databases have been considered to conduct the systematic review: ACM digital library, IEEE Xplore, Science Direct and Google Scholar.

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 are based on the research question. This study therefore established that the studies must contain data related to our research questions. i.e. encryption technique for data confidentiality in cloud environment.

b. Review Execution

During this phase, the search in the defined Databases 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 50 results which were filtered with the inclusion criteria to give a set of about XXX relevant studies.

3. RESULTS

The results of the review are presented in this section. The results are characterized with respect to the questions posed earlier. A year wise result representation is presented in Table 1.

Table 1: Year wise result representation

Year	No. of Papers
2007	2
2008	1
2009	4
2010	0
2011	4
2012	7
2013	3
2014	3
Total	24

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

The result of review shows the proposed encryption based approaches for the data security in cloud computing. The result is categorized into: (1) RSA, which is a Public-Key algorithm. It consists of Public-Key and Private-Key.

Table 2: 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	2
	DES and SDES	2
	SSL	2
	RC5	2
	AES	1
	Blowfish	2
	Location based encryption	3
	Full homomorphic encryption	3
	Others	7
	Total	24

Public-Key is known to all, whereas Private-Key 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)RC5 which is a symmetric key block cipher and it consists of a number of modular additions and Exclusive OR (EXOR). (5) Role Base Encryption (RBE), it enhances the protection of application data from unauthorized access. (6) Location based encryption and decryption of data. (7) Fully Homomorphic Encryption, allow complex mathematical operations to be performed on encrypted data without compromising the encryption. (8) Blowfish a variable-length key, 64-bit block cipher (9) Others, combination of various encryption algorithms .The categories wise results are summarized in Table 2.

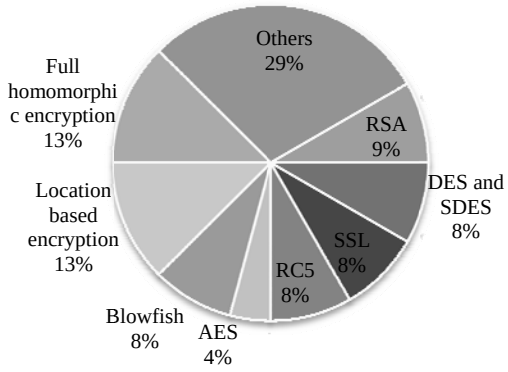

Fig. 1: Approaches to Ensure Data Security using Encryption Techniques

In [9] RSA encryption technique is proposed in which only the authorized user can access the data. Even if some intruder (unauthorized user) gets the data accidentally or intentionally if he captures the data also, he can't decrypt it and get back the original data from it. In [10],[21],[22] various encryption algorithms like DES, S-DES, Playfair, Vigenere, Caesar, Blowfish, RC-5 are compared in terms of Avalanche effect(Avalanche effect is the phenomenon that describes the effect in the output cipher text if a single or few bits are changed in the plain text), number of rounds, block size and the length of secret key respectively.

In [11] a new block based symmetric cryptography algorithm is proposed which uses a random number for generating the initial key, where this key is used for encrypting the given source file. The proposed key blocks contains all possible words comprising of number (n) of characters each generated from all characters whose ASCII code is from 0 to 255 in a random order.

In [12], Symmetric encryption algorithms such as Blowfish and Rejindael algorithms are compared and performance is Evaluated along with Experimental results to demonstrate the performance of these algorithms. [13] introduces a new method to enhance the performance of the Blowfish Algorithm. Cellular automata (CAs) is used to design a symmetric key cryptography system based on Blowfish algorithm, CAs are applied to generate a multiple pseudo-random numbers sequence (PNS) which were used during the encryption process.[7, 14] and [8] introduced the concept of Ceaser cipher and Vigenere cipher respectively.

[15] created a system for Ciphertext-Policy Attribute Based Encryption. That system allows for a new type of encrypted access control where user's private keys are specified by a set of attributes and a party encrypting data can specify a policy over these attributes specifying which users are able to decrypt. This system allows policies to be expressed as any monotonic tree access structure and is resistant to collusion attacks in which an attacker might obtain multiple private keys. They also provide an implementation of their proposed system, which included several optimization techniques.

[16-18] introduces a Fully homomorphism encryption scheme including 4 methods. They are the key generation algorithm, encryption algorithm, decryption algorithm and additional Evaluation algorithm.

Traditional encryption is used to provide assurance that only authorized users can use the secure content. However, it would still be useful to have an additional layer of security that provides assurance that the secure content can only be used at authorized location and time. The concept of location based encryption or geoencryption is being developed for such a purpose. Geoencryption is the use of position navigation and time (PNT) information as means to enhance the security of a traditional cryptographic system[20].[19] examines the benefits of using Loran for geoencryption and the implementation of geoencryption on Loran.

[20] introduced the concept of RC5 which is a parameterized symmetric encryption algorithm. RC5 algorithm uses three primitive operations and their inverses. These are Modulo Addition/subtraction, Bit-wise exclusive-OR and Rotation.[20] illustrated two hardware models to implement RC-5 and also compared their performance and efficiency.

[23] have proposed a framework for securing the communication between the client and the server in SSL. a *Linear Block Cipher(LBC)* has been proposed that switches from the domain of integers to the domain of bit stuffing to be applied to the first function of SSL that would give more secure communication. [24] characterizes the cryptographic strength of public servers running SSL/TLS. They also proposed a tool for this purpose, the Probing SSL Security Tool (PSST), and evaluate over 19,000 servers. This has exposed the great diversity in the levels of cryptographic strength that is supported on the Internet.

[25] has formulated a general secure database model SCONEDB (Secure Computation ON an Encrypted DataBase), which is defined independent of the query type.

The model incorporates the attacker capability as a distinct component and uses it to measure the security level of the encryption scheme. It also defines the notion of an encrypted database which can support secure computation such as secure kNN (k-nearest neighbor) queries on encrypted data.

[26] proposed a scheme for receiver-deniable public-key encryption. This scheme is based on mediated RSA PKI.By this scheme the receiver is able to lie about the decrypted message to a coercer and hence, escape a co-ercion.[27] has proposed to use federated identity management and hierarchical identity-based cryptography HIBC in the cloud which simplifies public key distribution and reduces SOAP header size.[28] have proposed to make use of digital signature and Diffie Hellman key exchange blended with (AES) Advanced Encryption Standard encryption algorithm to protect confidentiality of data stored in cloud.

Question 2: How the approaches have been validated?

This section shows the result of review as regards to the procedure adopted for validation. validation refers to any kind of empirical method used as a proof apart from the manifestation of the proposed approach. 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)No validation. The category wise detail is presented in table 3 and fig 2 shows the type of validation in percentage.

Table 3: Categories Wise Results of Question 2

Question	Category	No. of papers
How the approaches have been validated?	Comparative analysis	6
	Experiment	5
	Statistical analysis	4
	No validation	9
	Total	24

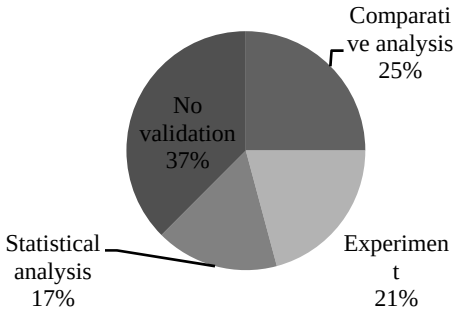

Fig. 2: Types of Validation

The results of the question regarding validation of proposed encryption approaches show that 21% of the selected papers used experimentation to validate their proposed approach while 37% of the proposed techniques provide no validation.

4. CONCLUSION

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. This can be concluded that most of the papers included for review are published in year 2012.Most of the papers were involved in comparison of different encryption algorithms. 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] IBM, “what is cloud computing”, [online] http://www.ibm.com/cloud-computing/in/en/what-is-cloud-computing.html, Accessed: 3 January 2015.

[2] Vaquero et al.,” A break in the clouds: towards a cloud definition”, SIGCOMM Comput. Commun. Rev. 39, 1, 50-55,2008.

[3] Mollah Muhammad Baqer et al.,” Next Generation of Computing through Cloud Computing Technology” In: Proc. Of 25th IEEE Canadian Conference on Electrical and Computer Engineering (CCECE),2012.

[4] Buyya et al.,”Cloud Computing and emerging IT platforms: vision, hype, and relatity for deliverling computing as the 5th utility”, Future Generation Computer System 25(6),pp. 599–616 ,2009.

[5] P. Mell and T. Grance, "The NIST Definition of Cloud Computing (ver. 15)", National Institute of Standards and Technology, Information Technology Laboratory, October 7, 2009.

[6] P. Brereton et al., “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.

[7] Savarese Chris et al.,” The Caesar Cipher”, [online] http://www.cs.trincoll.edu /~crypto/historical/ caesar.html, Accessed on: 16 January 2015.

[8] Morelli R.,” The Vigenere Cipher”, [online] http://www.cs.trincoll.edu/~crypto/historical/ vigenere.html,Accessed at: 16 January 2015.

[9] Parsi Kalpana et al.,” Data Security in Cloud Computing using RSA Algorithm”, International Journal of Research in Computer and Communication technology,IJRCCT, Vol 1, Issue 4, September 2012.

[10] Asif Ali Mir Arif Mir et al.,”A Review on Classical and Modern Encryption Techniques”, International Journal of Engineering Trends and Technology (IJETT) , Volume 12, Jun 2014.

[11] Gupta Vishwa et al.,” Advance cryptography algorithm for improving data security”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 1, January 2012.

[12] Kumar M. Anand et al.,” Investigating the Efficiency of Blowfish and Rejindael (AES) Algorithms”, I. J. Computer Network and Information Security, 2012,pp 2-28.

[13] Afaf M. Ali et al.," New Approach for Modifying Blowfish Algorithm by Using Multiple Keys", IJCSNS International Journal of Computer Science and Network Security, Vol.11 No.3, March 2011.

[14] RAO M.CHALAPATHI," Implementation of Strong Encryption Method Using Caesar Cipher Algorithm", International Journal of Engineering Research & Technology (IJERT),Vol. 2 Issue 11, November – 2013.

[15] Bethencourt John et al.," Ciphertext-Policy Attribute-Based Encryption",IEEE,2011.

[16] Gentry Craig,"Fully Homomorphic Encryption Using Ideal Lattices", In Proc. Of : 41st ACM Symposium on Theory of Computing (STOC), 2009.

[17] Tan Yubo et al.," Research of Cloud Computing Data Security Technology", IEEE,2012.

[18] Zhao Feng et al.," cloud computing security solution based on fully homomorphic encryption",In Proc. Of : ICACT,2014.

[19] Qiu Di et al.," Geoencryption Using Loran",IEEE,2011.

[20] Ambulgekar H P et al.," A Survey on Location Based Data Encryption Algorithms for Mobile Devices", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 5, May 2014.

[21] Verma Harsh Kumar et al.," Performance Analysis of RC5, Blowfish and DES Block Cipher Algorithms", International Journal of Computer Applications ,Vol 42– No.16, March 2012.

[22] Jasim Omer K. et al.," Efficiency of Modern Encryption Algorithms in Cloud Computing", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS),Volume 2, Issue 6, November – December 2013.

[23] Kuppuswamy Prakash et al.," Implementing Secure Socket Layer By Using LBC-Public Key Algorithm", International Journal of Latest Research in Science and Technology, Vol.1,Issue 3 :pp 225-228 ,September-October,2012.

[24] Lee Homin K. et al.," Cryptographic Strength of SSL/TLS Servers: Current and Recent Practices", ACM digital library,IMC'07, 2007.

[25] Cheung David W. et al.," Security on Cloud Computing, Query Computation and Data Mining on Encrypted Database",IEEE,2011.

[26] Ibrahim Maged H.," Receiver-deniable Public-Key Encryption", International Journal of Network Security, Vol.8, No.2, pp 159-165, Mar. 2009.

[27] Yan Liang et al.," Strengthen Cloud Computing Security with Federal Identity Management Using Hierarchical Identity-Based Cryptography", CloudCom, Springer,pp.167–177, 2009.

[28] Rewagad Prashant et al.," Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing", International Conference on Communication Systems and Network Technologies,2013.