International Journal of Engineering Research and Advanced Technology (IJERAT)

DOI: 10.31695/IJERAT.2019.3569

E-ISSN : 2454-6135

Volume.5, Issue 9
September -2019

Subject Review: Cloud Computing Security Based on Cryptography

Amal Abdulbaqi Maryoosh[1], Rana Saad Mohammed[2] & Raniah Ali Mustafa[3]

[1-3]Department of Computer science

Collage of education, Mustansiriyah University

Baghdad- Iraq

ABSTRACT

The cloud computing providing to users and companies many services and facilities such as less cost, availability and risk management. The services of cloud computing are delivered in pay per usage way and on-demand and it can store huge amount of data. But the security concern is the main reason that makes companies afraid of using cloud computing and store their data on cloud servers. In this paper, we try to review and describe many encryption methods that used to protect data which stored in cloud computing and make a comparison among these methods.

Key Words: *Cloud Computing, Chaotic Schemes, Deoxyribonucleic acid series, Cryptography.*

1. INTRODUCTION

Cloud computing has become one of the hottest topics in the technology world, that used virtualization to provide scalable services over the internet. users move their data and applications to the remote "Cloud" via various devices such as mobile phone, laptops, PC, etc...and can access to them in a simple way over the internet. In the last years, many web applications become available on cloud computing platform such as Hotmail, Gmail, etc... [1].

In cloud computing users can used the services everywhere, anywhere. There are two types of models in cloud computing, services models and deployment models. in service model there are three type of service (SaaS, PaaS, and IaaS), and in deployment models there are four type of models (Public, Private, Community, and Hybrid cloud). Also there are five essential characteristics in the cloud computing (On-Demand, BroadNetwork Access, Rapid Elasticity, Measured Service, and Resource pooling) [2].

The biggest concern about cloud computing when data management and infrastructure management in cloud is provided by third-party, it is always a risk to deliver the sensitive information to these providers. Although the cloud computing vendors ensure more secure password protected accounts, any sign of security breach would result in loss of clients and businesses [3].

In this paper, we conduct a deep analysis of cryptographic techniques that used for securing information in cloud computing. The remaining of this paper arranged as follow: In Section 2 the literature survey of some schemes that proposed in the latest decade. In Section 3 comparison among the schemes that discussed in section 2. Finally, the conclusions are shown in Section 4.

2. LITERATURE SURVEY

In the last decade, there are many methods that related to cloud computing security has been studied. In this section we discuss some of these research.

Syam Kumar and Subramanian [4] proposed an effective and safe method by using ECC and Sobol sequence. In this method, they were achieving a confidentiality and they could verify the data integrity without retrieving original data.

Arjun Kumar et al. [5] proposed a new method that used ECC to allows the user to store their data and retrieval it from cloud storage securely. This proposal divided the storage to two section the first section to store user private data, and the second to store shared data and use pin number with secret key to encryption data.

Sameeh A. [6] proposed a new scheme for Identity and Access Management (IAM) which depends on mixing of the Trusted Cloud (TC) with Identity-Based Cryptography (IBC) to facilitate the management and present more security for cloud computing, and used AES algorithm for secure file encryption.

A new framework suggested by Nagendra Kumar et al [7] that provided double authentication techniques and particularise proceedings that can protect data efficaciously through the period of transmission it to the cloud computing storage. In thismethod they were utilizes DS (Digital Signature) based on RSA algorithm for identity, access and data security when it stores in private cloud.

Sudhansu Ranjan Lenka and Biswaranjan Nayak [8] Suggested a new security model that provides a mechanism for create a secure connection and data hiding from unauthorized parties. In this scheme, they were applied a blending of digital signature technology and RSA encryption that could be simply combined with all kinds of cloud computing models such as: SaaS, PaaS and IaaS. This collection technique provides triple security, such as verification, authentication and data security. Also, the RSA algorithm was used to provide data confidentiality and the MD 5 algorithm was applied for authentication.

Nikhil Gajra et al. [9] provided the security for files and data authentication by used hybrid of AES and Blowfish for encryption, and used Elliptic Curve Cryptography (ECC) for key generation and used Diffie-Hellman (DH) for key exchange. These combination of algorithms provide authentication and confidentiality for outsourced data with low cost and minimal performance.

In this article, Sana Belguith et al. [10] proposed a new encryption algorithm which composed of merging secret key algorithm (AES) for data encryption and public key algorithm (RSA) for keys distributing. This collection aids to get advantage of secret key efficiency and speed performance of public key encryption, while keeping the rights of users to access data by a secured and authorized way.

A new method for data protection in cloud computing proposed by Salim A. Abbas and Amal A. Maryoosh [11] to reduce the complication of management based on Identity Based Cryptography (IBC), and providedata security based on Elliptic Curve Cryptography (ECC) and data integrity by using Elliptic curve digital signature algorithm (ECDS). In this approach they combined the security of IBC and ECC with Trusted Cloud (TC). The use of IBC was greatly reduced key management complication and the certificate issued was not required. furthermore, the denial of service attack (DOS) on CSPs was reduced via the use of TC, this important attraction because TC used for save users' data.

Noha MM. Abdelnabi et al. [12] used a hybrid of cryptographic algorithms. This combination contains (RSA and AES) algorithm to provide confidentiality and authentication, and used SHA256 to generate a signature. The proposed scheme provided the three security primitives – authentication, confidentiality and integrity.

A new scheme to provide data confidentiality and integrity suggested by Salim A. Abbas and Amal A. Maryoosh [13] via using Elliptic Curve Integrated Encryption Scheme (ECIES), and the key generated by used modified Identity Based Cryptography (MIBC). In this method they were combined the security of ECIES and MIBC with Trusted Cloud (TC). The key generation complication was decreased by utilized the MIBC and the certificate issued was not need to used.

Harpreet Kaur [14] used blowfish with MD5 method to ensure the security of data in cloud computing. a method is implemented for ensuring the data security of the files being uploaded to the cloud by different clients.

Divya Prathana Timothy and Ajit Kumar Santra [15] designed a new cryptographic scheme for data security in cloud based on a hybrid cryptosystem. this cryptosystem was comprised of secret key and public key cryptographic algorithms. in this method the Blowfish algorithm used for data security while RSA algorithm was used for user an authentication. Also the Secure Hash-2 function used in this scheme to provide data integrity.

hybrid approach that contain the combination of Blowfish and ECC encryption algorithms was implemented by Jobandeep Kaur et al [16] In this paper, where access policies will not leak any privacy data and improve security and performance standards such as decryption and encryption time and accuracy then compared with current performance parameters. Security is the main limitation while storing data via the cloud server. The approach presented is appropriately applied even if the tenant has access to the information, all that may appear is vulnerability. Hijacking sessions while accessing data, threats from within, data loss,malicious attacks from outside, disruption of service and loss of control. Enhancing the security of multimedia data storage in the cloud is critical.

combination of secret key and public key cryptography were used by Zinah Raad Saeed et al [17] in this paper. these algorithms were AES, RSA and ECC cryptographic method. This system provides high level of security for cloud computing in terms of encryption and authentication. The scheme in this study the data was encrypted using AES then, AES key have been encrypted using ECC only after that RSA will encrypt both the ciphertext and the encoding key again.

DOI : 10.31695/IJERAT.2019.3569

Shaheen Ayyub and Praveen Kaushik [18] proposed a new scheme for securing image that stored in cloud computing. this scheme contains the combination of chen and liu chaotic system. at first, they divided the mask image to 8 blocks, then they done the shuffling method based on logistic map on these blocks. Finally, the apply the hyper chaotic system on the resulting image to get the encrypted image. One of the benefits of this proposal, the key is also encrypted. Some values of generated encrypted key with the index is sent to the server & other value is sent to the user. before storing the image in the cloud, index was created for these images.

3. COMPARISON AMONG THE SCHEMES

Table 1 will explain the comparison among previous systems.

Table1.1. Comparison among cryptographic schemes

Ref.	Year	Privacy and security mechanism	Confidentiality	Integrity	Authentication
Syam and Subramanian [4]	2011	ECC and Sobol sequence	✓	✓	
Arjun et al. [5]	2012	ECC and ECDH key exchange algorithm	✓		
Sameeh [6]	2013	IBC with the Trusted Cloud (TC) and AES algorithm	✓		✓
Nagendra et al. [7]	2014	RSA and SHA1 algorithms	✓	✓	✓
Sudhansu et al. [8]	2014	RSA and MD5 algorithms	✓	✓	✓
Nikhil et al. [9]	2014	AES, Blowfish, ECC and DH	✓		✓
Sana et al. [10]	2015	Combination of AES and RSA algorithms	✓		
Salim and Amal [11]	2015	IBC, ECC, ECDS and TC	✓	✓	✓
Noha et al. [12]	2016	RSA, AES and SHA256	✓	✓	✓
Salim and Amal [13]	2016	MIBC, ECEIC and TC	✓		✓
Harpreet [14]	2017	Blowfish with MD5	✓		
Divya and Ajit [15]	2017	Blowfish, RSA and SHA2	✓	✓	✓
Jobandeep et al.[16]	2018	Blowfish and ECC	✓		✓
Zinah [17]	2018	AES, RSA and ECC	✓		
Shaheen and Praveen [18]	2019	Chen and Liu chaotic system	✓		

4. CONCLUSION

In this paper, we reviewed different techniques that used for ensuring data security in cloud computing within the period (2011-2019). Data security become very significant specially when the transmitting will have done thought open network and all cloud types are open network. These encryption schemes are studied and analyses fully to boost the efficiency of the encryption methods and to guarantee the security performance. the summary of this study, all these the techniques are beneficial for data encryption. every scheme is unrivaled in its own method, which may be appropriate for various applications. The new encryption technology is evolving every day, so the fast and secure traditional encryption technology will always achieve a high security rate. All technologies have some benefits and drawbacks and therefore new technologies have been developed.

REFERENCES

1. Jeffrey Voas and Jia Zhang, “Cloud Computing: New Wine or Just a New Bottle?”, *IEEE Computer Society*, 2009.
2. Sameeh A. Jassim, MSc thesis, “Mediated IBC-Based Management System of Identity and Access in Cloud Computing”, *College of Computer, University of Anbar*, 2013.

DOI : 10.31695/IJERAT.2019.3569

3. SameeraAbdulrahmanAlmulla and Chan YeobYeun, "Cloud Computing Security Management", *Engineering Systems Management and Its Applications (ICESMA), Presented at 2nd IEEE International Conference*, 30 march 2010.
4. Syam Kumar P and Subramanian R, "An Efficient and Secure Protocol for Ensuring Data Storage Security in Cloud Computing", *IJCSI International Journal of Computer Science Issues*, Vol. 8, Issue 6, No 1, November 2011.
5. Arjun Kumar et al, "Secure Storage and Access of Data in Cloud Computing", *ICT Convergence (ICTC), International Conference, Jeju Island*, pp. 336 - 339, 2012.
6. Sameeh A. Jassim, MSc thesis, "Mediated IBC-Based Management System of Identity and Access in Cloud Computing", College of Computer, University of Anbar, 2013.
7. Nagendra Kumar, Ashok Verma and Ajay Lala, "Access, Identity and Secure Data Storage in Private Cloud using Digital Signature", *International Journal of Innovative Research in Computer and Communication Engineering*, Vol. 2, Issue 3, March 2014.
8. Sudhansu Ranjan Lenka and Biswaranjan Nayak, "Enhancing data security in cloud computing using RSA encryption and MD5 algorithm", *International Journal of Computer Science Trends and Technology (IJCST)*, Volume 2 Issue 3, June-2014.
9. Nikhil Gajra, Shamsuddin S. Khan and Pradnya Rane, "PRIVATE CLOUD DATA SECURITY: SECURED USER AUTHENTICATION BY USING ENHANCED HYBRID ALGORITHMS", *International Journal of Computer Engineering and Technology (IJCET)*, Volume 5, Issue 8, August (2014).
10. Sana Belguith, Abderrazak Jemai and Rabah Attia, "Enhancing Data Security in Cloud Computing Using a Lightweight Cryptographic Algorithm", *The Eleventh International Conference on Autonomic and Autonomous Systems*, 2015.
11. Salim Ali Abbas and Amal AbdulBaqi Maryoosh, "Improving Data Storage Security in Cloud Computing Using Elliptic Curve Cryptography", *IOSR Journal of Computer Engineering (IOSR-JCE)*, Volume 17, Issue 4, Ver. I (July – Aug. 2015).
12. Noha MM. AbdElnapi, Fatma A. Omara and Nahla F.Omran, "A Hybrid Hashing Security Algorithm for Data Storage on Cloud Computing", *International Journal of Computer Science and Information Security (IJCSIS)*, Vol. 14, No. 4, April 2016.
13. Salim Ali Abbas and Amal AbdulBaqi Maryoosh, "Data Security for Cloud Computing based on Elliptic Curve Integrated Encryption Scheme (ECIES) and Modified Identity based Cryptography (MIBC)", *International Journal of Applied Information Systems (IJAIS)*, Volume 10 – No.6, March 2016.
14. Harpreet Kaur, "A Novel Technique of Data Security in Cloud Computing based on Blowfish with MD5 method", *International Journal of Advance Research, Ideas and Innovations in Technology*, Volume 3, Issue 6, 2017.
15. Divya Prathana Timothy and Ajit Kumar Santra, "A Hybrid Cryptography Algorithm for Cloud Computing Security", *IEEE*, 2017.
16. Jobandeep Kaur, Dr Vishal Bharti2 and Mr. Shamandeep Singh, "Enhanced Hybrid Blowfish and ECC Encryption to Secure Cloud Data Access and Storage Policies", *International Journal of Computer Science and Information Security (IJCSIS)*, Vol. 16, No. 5, May 2018.
17. Zinah Raad Saeed et al., "Improved Cloud Storage Security of Using Three Layers Cryptography Algorithms", *International Journal of Computer Science and Information Security (IJCSIS)*, Vol. 16, No. 10, October 2018.
18. Shaheen Ayyub and Praveen Kaushik, "Secure Searchable Image Encryption in Cloud Using Hyper Chaos", *The International Arab Journal of Information Technology*, Vol. 16, No. 2, March 2019.

DOI : 10.31695/IJERAT.2019.3569