Subject Review: Cloud Computing Security Based on Cryptography
Amal Abdulbaqi Maryoosh¹, Rana Saad Mohammed² & Raniah Ali Mustafa³

¹-³Department 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 this method 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. Abelnabi 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.
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.

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

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


