International Journal of Engineering Research and Advanced Technology (IJERAT)

DOI: 10.31695/IJERAT.2021.3731

E-ISSN : 2454-6135

Volume.7, No. 7
July -2021

Subject Review: Cloud Computing using RSA Algorithm

Haitham Salman Chyad, Raniah Ali Mustafa & Kawther Thabt Saleh

Mustansiriyah University

College of Education

Department of Computer Science, Iraq

ABSTRACT

Because of the advantages of resource sharing in an efficient and effective way, practical data storage mechanisms, and resources delivered on demand whenever they are needed in an adequate suitable environment, cloud computing plays an indisputable role in today's software. The data available in the cloud is going to be frequently shared via various customers under different cloud categorizations like public cloud, private cloud, hybrid cloud, and so on, as stated via the National Institute of Standards and Technology (NIST). Generally, access control can be defined as a method of confirming authorized users for access to cloud data and resource sharing. Cloud computing, in the opinion of researchers concerned with cloud data security, offers a high level of data mobility, storage, availability, data integrity, backup and recovery, confidentiality and privacy. Researchers studying cloud storage are focusing on data security, whereas also examining the influence of suggested algorithms on the performance of cloud. This work attempts to discuss and review a number of approaches for using RSA in cloud computing, as well as to compare such approaches.

Key Words: Cloud Computing, RSA algorithm, Data Security, Encryption, Decryption, Confidentiality, Integrity, Authentication.

1. INTRODUCTION

Cloud computing is of high importance in various big, medium and small businesses, and as more people turn to the cloud for services, their data security is becoming a main worry. Often, data security is critical, but due to the cloud computing critical nature as well as the huge volumes of complex data it transports, the requirement is considerably greater. Concerns about data security and privacy have thus proven to be a stumbling block to the widespread adoption of cloud computing services [1]. In addition, cloud computing entails the establishment of a network of remote servers and software that allows for centralized data storage and online access to computer resources and services [2]. There are three types of clouds: hybrid, private and public. Cloud computing, or simply "the cloud," is likewise concerned with increasing the efficiency of shared resources. Typically, cloud resources are shared by several users and dynamically reassigned according to demands [2].

The most significant problem concerning cloud computing is when third-party providers handle data and infrastructure management in cloud, there is often the risk of entrusting sensitive data to them. Despite the fact that the vendors of cloud computing guarantee more secure password-protected accounts, any evidence regarding a security breach could lead to the loss of enterprises and clients [3]. This study examines the RSA algorithm, which is applied for securing the information in cloud computing. The rest of this study is organized as follows: A literature review regarding a few solutions suggested in the last 10 years is presented in Section 2. Comparisons of the schemes presented in Section 2 are made in Section 3. Finally, in Section 4, the conclusions are presented.

2. LITERATURE SURVEY

Various approaches relating to the security of cloud computing have been investigated recently. A few of such studies are discussed in this section.

Nitin Ashokrao Vairagade and Rupali Sachin Vairagade [4] present their findings in this work. The cloud data models and cloud data storage architecture are presented initially. After that, utilizing RSA, the researchers propose a cloud security algorithm. The system of Cloud Computing provides several crucial security functions such as key generation, decryption and encryption. The

primary purpose is to safely handle and store data that isn't under the control of the data's owner. Furthermore, the data is stored in a cloud environment, and the security is provided using an RSA algorithm.

Challa Narasimham, Pachipala Yellamma, and Velagapudi Sreenivas [5], suggested an approach for storing and protecting data in the cloud by means of RSA public key cryptosystem. In addition, the security services described in virtual environment include encryption, key generation, and decryption.
Zaiton Muda, Balkees Mohamed Shereek, and Sharifah Yasin [6] present a novel technique for the security of Cloud Computing that combines Fermat's theorem and RSA algorithm. Its aids in building a novel secure cloud computing environment. Furthermore, the RSA Encryption could be sped faster by employing Fermat's theorem.

Biswaranjan Nayak and Sudhansu Ranjan Lenka [7] offer a novel security paradigm. The design offers a technique for securing communication while also concealing information from unauthorized users. In such concept, the researchers combined RSA encryption with a digital signature method that works with all sorts of cloud computing services, including SaaS, PaaS, and IaaS. Data security, verification and authentication are all provided by such technique. The researchers in this work offer the MD5 algorithm for authentication and RSA encryption method for data secrecy.

Prabha.R and Soumya.N.S [8]. presents the analysis of data security by means of RSA, which is a public key-based asymmetric cryptosystem. RSA is a high-potential and high-security data encryption algorithm. It is far more secure compared to any other encryption method.

Pooja Bharadwaj and Shivani Mankotia [9], the scope of this article encompasses significant topics like privacy, confidentiality, identity management, data Integrity, and other typical features related to cloud security. Also, one of the available options to increase security, namely decryption and encryption by means of RSA, is the topic of this disquisition. Following quick and simple descriptions of numerous security issues and concerns in the earlier section, the challenges posed by the network concept are discussed in the following section. In addition, the review covers recent work and advances or adjustments to RSA, or its progress in recent years. Furthermore, RSA is an encryption and decryption method that includes 3 main phases: key generation, encryption, and decryption.

P.K. Manjhi, Santosh Kumar Singh, and Dr. R.K. Tiwari [10] suggested an approach based on the RSA. The researchers assessed the performance related to algorithm on the basis of 3 parameters: Space Complexity, Time Complexity, and Throughput, following carrying out the RSA Algorithm. The proposed study attempts to encrypt the data by means of RSA to ensure that only the intended user has access to it. Unauthorized access to data is prevented by safeguarding. User data is encrypted before being uploaded to cloud. In the case when a user requests data from cloud provider, the cloud provider authenticates the user and delivers the requested data.

Debabrata Sarddar, Rajat Pandit, Priyajit Sen, Mousumi Biswas, and Debabrata Sarddar [11], discussed a method for solving the authentication challenge. The work utilized a person's unique identifying number, which was issued by a reputable agency. The authentication procedure is after that enhanced by using RSA method on that distinctive ID.

Boukari Souley and Adamu Ismail Abdulkarim [12], suggested an improved security system that uses RSA as an image steganography and digital signature for enhancing the security related to data stored on the cloud for preventing unauthorized users from accessing that data in the case when downloading or uploading it from the cloud, as well as evaluating the system's efficiency through measuring computing resources like CPU processing, memory storage, power, and net power.

Ghassan Sabeeh Mahmood [13], presented a data-protection model for cloud computing. RSA is used to encrypt the private data in such approach. In addition, the Challenge-Handshake-Authentication-Protocol (CHAP) protocol is utilized to strengthen the authentication security. The findings suggest that the model is both practical and secure.

Haw Wai Yee, Rajamohan Parthasarathy, and Seow Soon Loong [14], suggested an approach to provide data storage and security in cloud by means of public key cryptosystem through carrying out RSA algorithm, the study describes the security services such as encryption, key generation, decryption in virtual environment.

R. Mahammad Shafi and Y. Kiran Kumar [15], proposed a method to give data stored in cloud computing with authentication, integrity, and confidentiality. Only registered clients can upload and retrieve files from the cloud, ensuring authentication. RSA was utilized for securing the data in such a way that there was no risk of data leaking on the cloud. The file is

DOI : 10.31695/IJERAT.2021.3731

often encrypted and stored on cloud. As a result, just the authorized users can access the data by means of the generated private key in the proposed study. Even in the case when an intruder (unauthorized user) accidently or purposely obtains the data, he/she will be unable to decode it and recover the original data. Data security will now be ensured by using the RSA.

R. Mahammad Shafi and Y. Kiran Kumar [16], provided a useful mechanism with the characteristics of data integrity and privacy. This study focuses on issues related to virtual environment security and cloud data storage strategies. The research suggested a public key cryptosystem for offering data storage and security in cloud, which employs the concept of modified RSA to give improved security for data stored in cloud.

3. COMPARISON OF SCHEMES

Table 1: explains the comparison between previous systems.

Ref.	year	Privacy and security Mechanism	Confidentiality	Integrity	Authentication
[4]	2012	RSA algorithm	✓		
[5]	2013	RSA algorithm	✓	✓	
[6]	2014	RSA algorithm and Fermat's theorem	✓		
[7]	2014	RSA and MD 5 algorithm	✓		✓
[8]	2015	RSA algorithm	✓	✓	✓
[9]	2016	RSA algorithm	✓	✓	
[10]	2016	RSA algorithm	✓		✓
[11]	2017	RSA algorithm	✓		✓
[12]	2017	RSA, Digital Signature Algorithm (DSA) and image steganography	✓		✓
[13]	2018	RSA algorithm and Challenge-Handshake - Authentication-Protocol (CHAP)	✓		✓
[14]	2019	RSA algorithm	✓		
[15]	2019	RSA algorithm	✓	✓	
[16]	2020	modified RSA algorithm	✓	✓	

4. CONCLUSION

The presented work utilized a timeline to analyze several cloud computing solution on the basis of RSA throughout time (2012-2020). Cloud computing security has often been a significant part of cloud service providers' quality of service. Cloud computing, on the other hand, introduces various new security issues that have yet to be well examined. This study uses RSA for focusing on cloud computing. Those schemes of encryption are thoroughly investigated and analyzed in order to improve the encryption efficiency through employing RSA and to ensure security performance. According to the findings of this work, all of these approaches are useful for data encryption. Every plan is unique in its approach, which might be suitable for a variety of purposes. Today, new technology of encryption is being developed on a daily basis, and recently, suggested cloud computing technologies have also increased security. Every technology has a set of advantages and disadvantages; thus, new technologies have become more advanced.

DOI : 10.31695/IJERAT.2021.3731

ACKNOWLEDGMENT

The authors would like to thank Mustansiriyah University (https://uomustansiriyah.edu.iq, Baghdad- Iraq) for its support in this work.

REFERENCES

1. Parsi Kalpana and Sudha Singaraju, "Data Security in Cloud Computing using RSA Algorithm", *International Journal of Research in Computer and Communication technology, IJRCCT*, ISSN 2278-5841, Vol 1, Issue 4, September 2012.
2. K.R.MONISHA,"SECURE CLOUD COMPUTING USING AES AND RSA ALGORITHMS", *International Journal of Advances In Computer Science and Cloud Computing*, ISSN: 2321-4058 Volume- 3, Issue- 1, May-2015.
3. Amal Abdulbaqi Maryoosh, Rana Saad Mohammed and Raniah Ali Mustafa, "Subject Review: Cloud Computing Security Based on Cryptography", *International Journal of Engineering Research and Advanced Technology (IJERAT)*, E-ISSN: 2454-6135, DOI: 10.31695/IJERAT.2019.3569, Volume.5, Issue 9, September -2019.
4. Rupali Sachin Vairagade and Nitin Ashokrao Vairagade, "Cloud Computing Data Storage and Security Enhancement", *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, ISSN: 2278 – 1323, Volume 1, Issue 6, August 2012.
5. Pachipala Yellamma, Challa Narasimham and Velagapudi sreenivas,"DATA SECURITY IN CLOUD USING RSA", IEEE – 31661, 4th ICCCNT – 13, DOI: 10.1109/ICCCNT.2013.6726471,Tiruchengode, India, July 4 - 6, 2013.
6. Balkees Mohamed Shereek, ZaitonMuda and SharifahYasin," Improve Cloud Computing Security Using RSA Encryption WithFermat's Little Theorem", *IOSR Journal of Engineering (IOSRJEN)*, ISSN (e): 2250-3021, ISSN (p): 2278-8719, Vol. 04, Issue 02,February, 2014.
7. Sudhansu Ranjan Lenka and Biswaranjan Nayak," Enhancing Data Security in Cloud Computing Using RSA Encryption andMD5 Algorithm", International Journal of Computer Science Trends and Technology (IJCST),Volume 2 Issue 3, June-2014.
8. Ms. Soumya.N.S and Mrs. Prabha.R," Cloud Computing: Data Security Using RSA", *IJLTEMAS*, ISSN 2278 – 2540, Volume IV, Issue X, October 2015.
9. Pooja Bharadwaj and Shivani Mankotia," Up in the Air: Cloud Computing Security and RSA Algorithm", *International Journal of Science and Research (IJSR)*, ISSN (Online): 2319-7064, Volume 5 Issue 8, August 2016.
10. Santosh Kumar Singh, Dr. P.K. Manjhi and Dr. R.K. Tiwari," Data Security using RSA Algorithm in Cloud Computing", *International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE)*, ISSN (Online) 2278-1021, ISSN (Print) 2319 5940, Vol. 5, Issue 8, August 2016.
11. Debabrata Sarddar, Mousumi Biswas, Priyajit Sen3 and Rajat Pandit," Authentication using Unique Identification Number in Cloud Network using RSA Algorithm", International Journal of Grid and Distributed Computing, Vol. 10, No. 4 (2017), pp.1-8, http://dx.doi.org/10.14257/ijgdc.2017.10.4.01
12. Adamu Ismail Abdulkarim and Boukari Souley, " An Enhanced Cloud Based Security System Using RSA as Digital Signature and Image Steganography", *International Journal of Scientific & Engineering Research*, ISSN 2229-5518, Volume 8, Issue 7, July-2017.
13. Ghassan Sabeeh Mahmood,"Data Security Protection in Cloud Computing by using Encryption", *Kirkuk University Journal /Scientific Studies (KUJSS)*, ISSN 1992 – 0849, Volume 12, Issue 4, 2018.
14. Dr. Rajamohan Parthasarathy, Ms. Haw Wai Yee and Mr. Seow Soon Loong," Implementation of RSA Algorithm to Secure Data in Cloud Computing", *IJISET - International Journal of Innovative Science, Engineering & Technology*, ISSN (Online) 2348 – 7968, Vol. 6 Issue 4, April 2019.

DOI : 10.31695/IJERAT.2021.3731

15. Y. Kiran Kumar and Dr. R. Mahammad Shafi," Secure Data Storage in Cloud Computing using RSA Algorithm", *International Journal of Scientific & Engineering Research*, ISSN 2229-5518, Volume 10, Issue 4, April 2019.
16. Y. Kiran Kumar and R. Mahammad Shafi," An efficient and secure data storage in cloud computing using modified RSA public key cryptosystem", *International Journal of Electrical and Computer Engineering (IJECE)*, ISSN: 2088-8708, DOI: 10.11591/ijece.v10i1.pp530-537, Vol.10, No.1, February 2020, pp. 530~537.

DOI : 10.31695/IJERAT.2021.3731