Journal of Theoretical and Applied Information Technology
15th March 2023. Vol.101. No 5

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

MODEL OF PROTECTING DATA IN THE CLOUD

[1]OSAMA ALJUMAIAH, [2] MOUNIR FRIKHA

[1] King Faisal University, College of Computer Sciences & Information Technology, Saudi Arabian

[2] King Faisal University, College of Computer Sciences & Information Technology, Saudi Arabian

E-mail: [1]osaljumaiah@gmail.com, [2] mmfrikha@kfu.edu.sa

ABSTRACT

With the wide spread of cloud services, people use cloud technology to store their personal information. Technologies have a significant part in the operation of our lives. The most major issue is data breaches caused by hackers. Therefore, we must provide a cryptographic technique that cannot be broken to safeguard the data from hackers. Cryptography encrypts data so that only the authorized user may decode it. This project aims to propose a protection model for data in the cloud using RSA Algorithms.
Keywords: *Cloud, Security, Privacy, Encryption, Data*

1. INTRODUCTION

The demand for cloud computing has gained much attention in recent years. Organizations are moving to the cloud to increase their information technology capabilities by enhancing capacity and dynamically adding expertise without spending money on expensive infrastructure, software licensing or hiring new staff. Among its many advantages, cloud computing gives users a more flexible way to access storage and computing resources as needed. There are three service models for the cloud Platform as a Service (PAAS), Infrastructure as a Service (IAAS), and Software as a Service (SAAS) Control-based policies, compliance, and technologies have been developed to protect the applications, data, and infrastructure related to the cloud. As more businesses use the cloud to operate their data, it has become more critical to contract with providers who can provide adequate security and address potential vulnerabilities. When needs for shared resources, access control, privacy, and identity management arise, cloud computing security is the primary concern. Cloud computing provides users with a network-based environment, allowing them to share resources regardless of location.

With the huge increase in demand for cloud computing, there are several issues and concerns regarding the security and privacy of data in cloud services. More trust must be placed in cloud service providers, whether they have seen or breached this data. Also, cloud service providers maintain data centers in geographically distributed locations, with multiple security challenges and threats. Users need to be made aware of the exact location of their sensitive data. Due to the rapid spread of threats in virtualized environments, traditional security techniques such as firewalls, host-based antivirus software, and intrusion detection systems need to provide adequate security in virtualized systems.

According to the Cloud Security Alliance (CSA), data breaching is the most critical security issue that needs to be addressed.

The rest of this paper is organized as follows:
Section 2

briefly explains the project contributions. The related works and the security solutions used for data protection in the cloud are discussed in Section 3. Our proposed solutions follow this in Section 4. Finally, the paper's conclusions and future works are in Section 5.

2. CONTRIBUTIONS

In this paper. It will provide an overview of the cloud computing architecture model. Also, discuss cloud security challenges and issues. Based on existing research publications, we will conduct a survey study about security solutions to protect data from unauthorized access or breaches. To help the cloud service providers safeguard customer data. And proposed a model for protecting data in the cloud using RSA encryption algorithms. The goal of the model is to protect users' data in the cloud while also improving the cloud user experience in terms of data confidentiality and trust.

3. RELATED WORK

When we talk about cloud computing, the first thing to think about is data security. As with

many challenges in cloud computing, data security has been selected as the top trending topic to be discussed. R.Barona and E.A.Mary Anita [1] think that the leading cloud security concern is a data breach in the cloud. Researchers and the cloud community must focus on developing strategies to protect data in the cloud. The authors in [2] have proposed a risk model to measure the risk of cloud computing service providers. That can help the client \ user to decide which provider has less risk and to work with based on many permitters and security measures the service provider should apply. Many researchers have started to study that concern and come up with countermeasures to protect data in the cloud, as Bijayalaxmi Purohit and Pawan Prakash Singh [3] implemented My DLP technology to be used as data prevention to protect data from being leaked.

Cloud computing security is not always the end-user's responsibility. The authors [4] debated whether the cloud service provider's responsibility for service security should be considered a valuable consideration. Encryption has been used to protect data in the cloud by many researchers and references [5].In this paper, the authors implement the Digital Signature Algorithm, Data Encryption Standard, and Steganography to provide maximum security in cloud computing. In [6], the authors also suggest different encryption models ensure the availability and integrity of data by dividing the data into sections: Index builder,128-bit SSL encryption; message authenticates code, a double authentication of the user, one by the owner and the other by the cloud, and verification of the digital signature of the owner. Other authors discuss this in [7] Improving Cloud Computing Data Security by Using Digital Signatures and the RSA Encryption Algorithm. In [8], the authors proposed a third-party auditor for cloud computing to ensure the security of data access in cloud computing by proposing a scheme using RSA and bilinear Diffie-Hellman techniques.

Other researchers think of different ways to simplify the encryption model [9]. In this paper, a new lightweight cryptographic algorithm has been proposed. It is called a "New Lightweight Cryptographic Algorithm" (NLCA) for enhancing data security in the cloud computing environment. It encrypts data based on symmetric cryptography with a (128-bit) key to encrypt the data. In [10] author has proposed the classification of data in the cloud to minimize the encryption and decryption process and apply the encryption level based on data classification. In [11], the author suggests a technique for symmetric cryptography based on a symmetric model essential to cryptography. There will only be one private key used for each.

The process of encrypting and decrypting data. In [12], the authors proposed a cloud architecture scheme for the encryption box that includes different cryptographic algorithms using the quantum approach in search based on Grover's algorithm.

In [13], the authors' design architecture for the encryption system, the first user must upload a file using AES key creation and encrypt the file's contents using the generated key. After generating a key, the file is successfully uploaded to a cloud database. In the download phase, the user must request a file download, and its authenticity is confirmed against an admin-maintained cryptography server. Once validated, the file is decrypted using the user's private key, and the user can successfully download the content. In [14], the approaches consist of data encryption and password hashing. Encryption of data refers to the transformation of data into an encrypted form with an encryption key, after which it is decrypted using a password or decryption key. The author [15] proposed that the Deep Substitution Encryption Method (DSEM) is a bit-based encryption algorithm. They are using a method based on bit substitution. A single letter is encoded into six letters. DSEM performs five varying steps of a replacement process utilizing a key. In [16], the authors proposed cryptographic methods such as the AES algorithm Using S- box with the Feistel Algorithm to get high performance and security for cloud data compared to other techniques. In [17] they propose a mechanism for offering enhanced data security using cloud storage services; they use the double encryption techniques AES and RSA for file encryption.

Direction and analysis in Table:1 based on the related work; we find out there are multiple approaches that rely on encryption to enhance the protection of these data. For better security, encryption is a great choice, but we must choose the better encryption techniques that may protect the user data comparisons between different algorithms techniques

4. THE PROPOSED SOLUTIONS

The model proposed for protecting user data applies the RSA encryption algorithm before storing the data in the cloud. RSA (Rivest–Shamir–Adleman) is one of the first public-key cryptosystems widely used for secure communication. RSA is an asymmetric encryption

Journal of Theoretical and Applied Information Technology
15th March 2023. Vol.101. No 5

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

method used to encrypt internet-transmitted data. It requires a lot of time and effort for a potential hacker to penetrate the system since it generates a massive amount of gibberish that might discourage them. Therefore, it is a robust and trustworthy encryption technique that may be utilized to defend an organization's network security. RSA depends on the factorization of two huge prime integers into prime factors. Using these two random prime numbers, a new huge number is produced. Only the sender can decipher the message by knowing these two prime integers. This enormous, compounded number would make it difficult for the hacker to find the starting prime number. However, the technique may become slower when encrypting a huge amount of data. RSA is typically employed in various applications. The proposed model encrypts data using RSA encryption, sends it to the cloud to ensure data confidentiality, and decrypts it when needed. Figure 1 shows the proposed model.

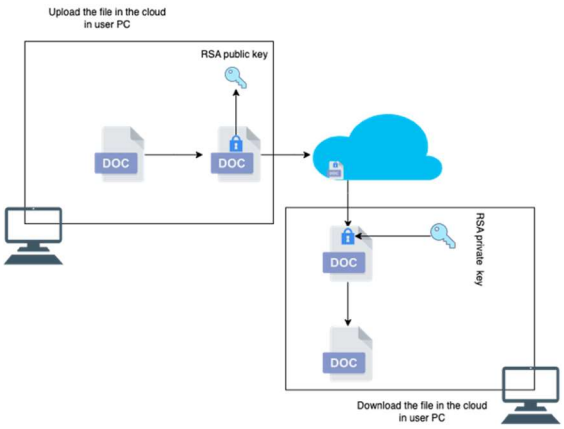

Figure 1: RSA encryptions model for cloud computing

We try to implement and simulate the RSA encryption mechanism to compare it with other encryption algorithms. The main objective is to implement an encryption algorithm to protect data in the cloud, and since the RSA provides strong security, it can be a great choice to use in cloud computing.

During the upload phase, the user will upload a file using RSA key generation and encrypt the file's contents using the generated key. After key creation, the file is successfully uploaded to the cloud. The user must request that a file be downloaded and decrypted using the user's private key and the file.

The proposed Architecture, as shown in figure 2

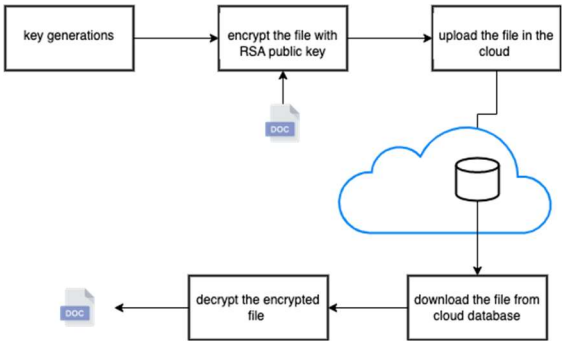

Figure 2: proposed model architecture

The key generation algorithm (the algorithm for generating public and private keys) in Step 1 is the most complicated aspect of RSA cryptography. Using the Rabin-Miller primality test procedure, two huge prime numbers, p, and q, are produced. The modulus n is determined by multiplying p and q. Both public and private keys utilize this number. The second step is to encrypt the file with the generated public key. The encrypted file is then uploaded to a cloud database, where it will be securely stored, and no one will be able to access or edit it because it is encrypted with a key. Whenever the user needs to access a file from the cloud, download the file from the cloud and decrypt it using the generated private key.

5. CONCLUSION AND FUTURE WORK

Security in the cloud is one of the significant challenges in cloud computing. And one of the top security concerns is a data breach in the cloud. In this project, we proposed an RSA encryption model to ensure data confidentiality in the cloud system. Our goal is to create a simple model that a home user with limited resources can use. To protect and enhance the user's data protection while using the cloud and provide powerful encryption with a sample implementation,

Limitations: In this model, RSA encryptions are not practical in handling a huge amount of data, such as enterprise data, because they will consume too much power and are much slower to process. It is powerful for home users and has a limited data size.

For future work, we will implement that model into the software with a graphical interface, which will be helpful for people and ensure a better user experience. and optimize the model for large data sets while minimizing resource use.

FUNDING: This work was funded by King Faisal University, Saudi Arabia [Project No. GRANT2,707].
ACKNOWLEDGMENTS: This work was supported through the Annual Funding track by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia [Project No. GRANT2,707].
CONFLICTS OF INTEREST: All authors declare no conflict of interest.

REFERENCES:

[1] Barona, R. and Anita, E.M., 2017, April. A survey on data breach challenges in cloud computing security: Issues and threats. In 2017 International conference on circuit, power and computing technologies (ICCPCT) (pp. 1-8). IEEE.

[2] Sharma, P.K., Kaushik, P.S., Agarwal, P., Jain, P., Agarwal, S. and Dixit, K., 2017, October. Issues and challenges of data security in a cloud computing environment. In 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON) (pp. 560-566). IEEE.

[3] Purohit, B. and Singh, P.P., 2013. Data leakage analysis on cloud computing. International Journal of Engineering Research and Applications, 3(3), pp.1311-1316

[4] Kolevski, D., Michael, K., Abbas, R. and Freeman, M., 2020, November. Stakeholders in the cloud computing value-chain: A socio-technical review of data breach literature. In 2020 IEEE International Symposium on Technology and Society (ISTAS) (pp. 290-293). IEEE.

[5] Saini, G. and Sharma, N., 2014. Triple security of data in cloud computing. International Journal of Computer Science and Information Technologies, 5(4), pp.5825-5827.

[6] Sood, S.K., 2012. A combined approach to ensure data security in cloud computing. Journal of Network and Computer Applications, 35(6), pp.1831-1838.

[7] Somani, U., Lakhani, K. and Mundra, M., 2010, October. Implementing digital signature with RSA encryption algorithm to enhance cloud data security in Cloud Computing. In 2010 First International Conference On Parallel, Distributed and Grid Computing (PDGC 2010) (pp. 211-216). IEEE.

[8] Han, S. and Xing, J., 2011, September. Ensuring data storage security through a novel third party auditor scheme in cloud computing. In 2011 IEEE International Conference on Cloud Computing and Intelligence Systems (pp. 264-268). IEEE.

[9] Thabit, F., Alhomdy, S., Al-Ahdal, A.H. and Jagtap, S., 2021. A new lightweight cryptographic algorithm for enhancing data security in cloud computing. Global Transitions Proceedings, 2(1), pp.91-99.

[10] Singh, K.P., Rishiwal, V. and Kumar, P., 2018, February. Classification of data to enhance data security in cloud computing. In 2018 3rd International conference on internet of things: Smart innovation and usages (IoT-SIU) (pp. 1-5). IEEE

[11] Nooh, S.A., 2020, September. Cloud Cryptography: User End Encryption. In 2020 International Conference on Computing and Information Technology (ICCIT-1441) (pp. 1-4). IEEE.

[12] Amellal, H., Meslouhi, A., El Allati, A. and El Haddadi, A., 2018, November. Protect privacy in the cloud via data encryption. In 2018 International Symposium on Advanced Electrical and Communication Technologies (ISAECT) (pp. 1-4). IEEE.

[13] Subasini, C.A., and Bushra, S.N., 2021, April. Securing of Cloud Data with Duplex Data Encryption Algorithm. In 2021 5th International Conference on Computing Methodologies and Communication (ICCMC) (pp. 252-256). IEEE.

[14] Ghosh, S., Singh, A.R., Pandey, G. and Lakhanpal, A., 2020, December. A Novel Solution to Cloud Data Security Issues. In 2020 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN) (pp. 857-860). IEEE.

[15] Lavanya, B. and ThamizhThendral, V., 2019, October. A novel data ciphering method for secure cloud storage. In 2019 International Carnahan Conference on Security Technology (ICCST) (pp. 1-6). IEEE.

[16] Tyagi, S.S., 2021, February. Secure Data Storage in Cloud using **an**Encryption Algorithm. In 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV) (pp. 136-141). IEEE.

[17] Jasmin , K., Selvan, S., Sahana, S. and Thanmai, G., 2021, March. Efficient and Secure File Transfer in Cloud Through Double Encryption Using AES and RSA Algorithm. In 2021 International Conference on Emerging Smart Computing and Informatics (ESCI) (pp. 791-796). IEEE.

RELATED WORK ANALYSIS

Table 2: Related work analysis

Author / references	The proposed solutions	Methodology	Analysis
[1]	have proposed a risk model to measure the risk of cloud computing service providers. That can help the client \ user to decide which provider has less risk and to work with based on many permitters and security measures the service provider should apply.	model to measure the risk of cloud	The proposed solution is great for choosing the best cloud service provider to be chosen
[3]	My DLP technology to be used as data prevention to protect data from being leaked.	DLP tool	The DLP tools can enhance the security of the Data in the Cloud, but it is difficult to be implemented in the case of a normal end user. And it will not protect the data in case if it's breach
[5]	the Authors implement the Digital Signature Algorithm, Data Encryption Standard, and Steganography to provide maximum security in cloud computing.	DES and Digital signature algorithm	The proposed solution did not provide enough security by using DES
[6]	Authors suggest different encryption models to ensure the availability and integrity of data by dividing the data into sections Index builder,128-bit SSL encryption, Message authenticates code, and a double authentication of the user, one by the owner and the other by cloud and verification of the digital signature of the owner.	128-bit SSL encryption	The proposed solution is a complicity issue for the use of end uses and needs to be integrated with the cloud service provider.
[7]	Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing	Digital signature and RSA	The RSA Algorithm can provide more security in the user data, but it bit slow compared to other Algorithm
[8]	the authors proposed a third-party auditor for cloud computing to ensure the security of data access in cloud computing by proposing a scheme using RSA and Bilinear Diffie-Hellman techniques	RSA and Bilinear Diffie-Hellman techniques	The RSA Algorithm can provide more security in the user data, but it bit slow compared to other Algorithm
[9]	New Lightweight Cryptographic Algorithm (NLCA) for enhancing data security in the cloud computing environment. It encrypts data based on symmetric cryptography with a (128-bit) key to encrypt the data.	128-bit SSL encryption	The suggested sublations is not cover the data in rest and cover the connection of clients and service provider

[10]	classification of data in the cloud to minimize the encryptions and decryption process and apply the encryption level based on the classification of data.	Classifications	Classification of data did not protect the data in case if it breach but it can help the cloud service provider to design security tools for each categories
[11]	symmetric model essential to cryptography There will only be one private key used for each. The process of encrypting and decrypting data	Symmetric key cryptography	The model did not include Audio and video and complex data
[12]	the authors proposed an cloud architecture scheme for the encryption box, which includes different cryptographic algorithms by using the quantum approach in search based on Grover's algorithm	the encryption box using quantum approach	Did not include the type of encryption. Will be used in this proposal.
[13]	The authors' design architecture of the encryption system connects to the cloud database. design to encrypted and decrypt the data before and after that data been save in cloud	AES and RSA algorithm	the purposed not capability to connect with other cloud service providers. But it is great companion for security strong and fast security
[14]	The approaches consist of Data Encryption and password hashing. Encryption of data refers to the transformation of data into an encrypted form with the use of an encryption key, after which it is decrypted using a password or decryption key.	asymmetric key encryption hashing functions SAH256	The purposed solutions is provide very strong encryption Algorithm and hashing function which will be difficult to be break meanwhile that implementation require resources to be implemented
[15]	The Deep Substitution Encryption Method (DSEM) is a bit-based encryption algorithm. A single letter at encodes into six letters. DSEM performing five varying steps of a replacement process utilizing a key.	using a method based on bit substitution.	Substitution is great and easy to be deployed but it has some limitation and
[16]	proposed cryptographic method such as AES algorithm Using S- box with the Feistel Algorithm to get high performance and security of cloud data in comparison to an other technique.	AES algorithm and Feistel algorithm	AES is providing an Excellent security and provide the fastest compare to other
[17]	Propose a mechanism for offering enhanced data security Using Cloud storage services, They make of the Double Encryption Technique AES and RSA for file encryptions	AES algorithm and RSA algorithm	Great companion mechanism for the best approach between the Excellent security and fast generations