Journal of Advanced Engineering Research
ISSN: 2393-8447
Volume 10, Issue 1, 2023, pp.65-69

Symmetric-based Cryptography Key Algorithm for Data Encryption and Decryption in Cloud Computing

Khushabu Agrawal[1,*], Puneet Sharma[2]

[1,2]Department of Computer Engineering, & Applications, GLA University, Mathura-281406, India

*Corresponding author email: agkhushboo1996@gmail.com, Tel. :8433434046

ABSTRACT

In these days, cloud computing is used in many regions such as information sharing in organizations, colleges, and the military to store a large amount of information. Cloud computing is very useful to access data from anywhere and anytime at the request of the user. Cloud computing raised security concerns while accessing a huge amount of data. This paper proposed a cryptography algorithm based on a symmetric algorithm where the user has the information related to the secret key to encrypt and decrypt the data. The proposed algorithm used the encrypt and decryption of data on the user side and cloud storage in order to protect information from various sorts of attackers. The proposed cryptography method increases the transparency between the user and cloud service provider as well as reduces the security risk.

Keywords - Cloud Computing, Cryptography, Symmetric Key, Asymmetric Key, Data Security.

1. INTRODUCTION

In cloud computing, security is one of the major issues. Many organizations used the cloud to store data rather than traditional ways to store the data [1], [2], [4], [11], [12]. Cloud storage provides the efficiency to access data from anywhere. However, the main issue in cloud computing raises concerns about data security. In this paper, we propose a cryptography algorithm to increase the security for cloud computing. The proposed method used the symmetric key algorithm for the encryption and decryption of the data in cloud computing environments. The proposed cryptography method increases the transparency between the user and cloud service provider as well as reduces the security risk.

The development of technology has raised the cost of hardware and software as well as increased internet use. therefore, Cloud computing gained popularity, as it provides the resources and services per the user, needs that optimize the user time and cost [3]–[5]. the main benefit of cloud computing is that the user does not need to have expertise in the infrastructure details of the cloud because it provides data abstraction. Virtualization, Load Balancing Computer Systems, Data Storage, and Data Accessibility are some of the technologies that have contributed to the success of Cloud Computing [2]. Even though cloud computing has many benefits, there are still some barriers preventing its wide acceptance. Since consumer's and corporate organizations' data is stored together on a platform that can be viewed by anybody, they give a third-party power over their data which can raise the security concern. Thus, leading to the data breach. The main objective of this study is proposed a symmetric-based cryptography algorithm for encrypting and decrypting the data. The information is stored in the cloud storage by using the security key to increase the data protection from attackers.

A. Cryptography in cloud computing

Cryptography technique used the secure the data. Each cloud provider's hosted data is secure, enabling users to access public cloud services quickly and securely [2], [13], [14]. Cloud cryptography secures sensitive data without affecting data flow. You may encrypt critical data using the strength of your organization's IT infrastructure using cloud encryption. We can only ensure that the information is encrypted, and authenticated [15], [16]. The cryptography key is kept in place without the privilege of actual, physical control of data storage in the cloud.

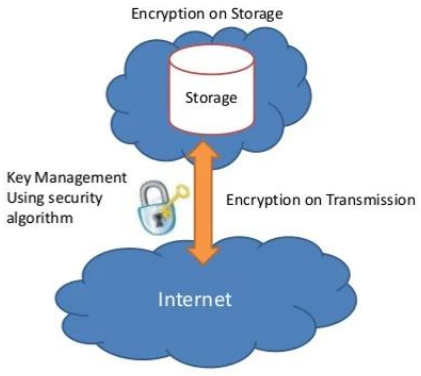

Fig. 1. sample image of a cryptography key management for security purpose.

Fig. 1 shows the sample image of a cryptography key management for security purposes. Data cryptography uses crypto techniques to encrypt the data. cloud computing provides data safety and resource accessibility with the help of cloud-provider. Fig.2 shows the classification of a cryptography key algorithm. cloud comput- ing increases security without slowing down the accessibility of information. Encryption provides the security of sensitive data. There are two types of key cryptography algorithms:

1 SYMMETRIC ALGORITHMS: The symmetric-based key encryption algorithm provides to encrypt the information of data and generates a key. The generated key is used to decrypt the information. The symmetric-based algorithm is easy for the encryption and decryption of the data information.

2 ASYMMETRIC ALGORITHMS: The asymmetric-based key encryption algorithm uses two different keys to encrypt and decrypt the data respectively. It is used for less amount of information and quite slower in comparison to the symmetric algorithms.

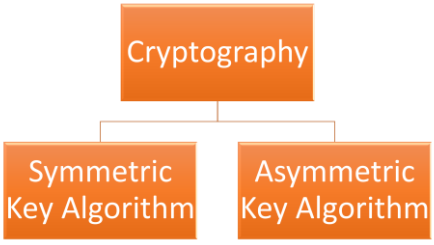

Fig. 2. The classification of cryptography.

2. RELATED WORK

Many studies have focused on cloud computing safety concerns. Since safety is the top priority, various authors have proposed various methods to ensure it. Users who are using the service. Using counter propagation neural (CPN) networks, Anshika Negi et al. [1] proposed a model where encryption and decryption are carried out. It is a modern approach named a tried-and-true security system. Three different types of authentications are discussed in order to boost data safety.

In order to strengthen cloud security, Shakeeba et al. pro- posed a multilevel encryption and decryption algorithm [2]. Decrypting data at multiple levels with this method is more time-consuming and complex than decrypting it at a single level, making it more secure. For each of these levels, a different algorithm is used: Rivest-Shamir-Adleman (RSA), and Advanced Encryption Standard (AES).

The authors Chunlin et al. [3] tackle the privacy and security concerns of cloud computing. Ubuntu Enterprise Cloud (UEC) was suggested as a means to address cloud computing security and privacy concerns. Specifically, this algorithm encrypts and decrypts data to accomplish its goal. To protect their client's privacy, UEC prevents administrators from gaining unfettered access to data even when doing their jobs.

Maintaining confidentiality is ensured by the cloud design, which prevents unauthorized access to user information. A model is put forth by Venter et al. [4] to lessen cyberattacks in the cloud. To do so, they protect for key management and encryption to be handled on the client side. They develop a novel cryptography system by combining neural cryptography and chaos. Because the strength of the encryption key is not determined by the length of the key but rather by the randomness of the input noise, this method can be used to increase the strength of encryption keys using chaotic random noise.

Raja et al. [5] propose a symmetric-based encryption algorithm for cloud data security. To generate keys, an alphanumeric encryption table is used. These keys are primarily used to authenticate users. The use of this algorithm ensures that data is safe from hackers.

The issues of accessibility, consistency, and security of data are tackled by Suryawanshi et al. in [6] by presenting two different schemes. The initial stage of their plan includes con- ducting assessments in public. In this scheme, the Third Party Authenticator (TPA) is a homomorphic linear authenticator. In contrast, their second plan uses threshold cryptography. The first scheme ensures that the TPA does not learn anything about the important data during the auditing process, and the second scheme ensures that the stored data cannot be used inappropriately by any unauthorized users. Both schemes work together to ensure that the data are secure.

A hybrid algorithm based on Blowfish, RSA, and SHA- 2 was proposed by Timothy et al. in [7]. It is an algorithm that combines symmetric and asymmetric techniques. Confidentiality of data is handled by Blowfish, and authentication is handled by RSA. The RSA algorithm and the SHA2 hashing algorithm both work together to keep information secure.

There is a lot of trust in this model because it ensures safe Internet data transmission. There was a presentation of a Hybrid Encryption Scheme by Manju Khari et al. in [8]. They employ biometric technology for user authentication. The Data Encryption Standard (DES), Secure Hash Algorithm (SHA), and Rivest-Shamir-Adleman (RSA) are all used in this piece. SHA and RSA algorithms are used for uploading information securely, while the 3 DES cryptography algorithm is used for transmitting information securely. The architecture we propose

here will result in an environment that is both secure and impenetrable to outsiders.

Singh et al. [9], detailed the use of the cryptographic method known as elliptic curve cryptography. As a result of the encryption that occurs on the client's side, the data in this location is inaccessible until it has been made available.

During the login process, the user authenticates themselves by providing a number of different input parameters. To increase security, the Elliptic Curve Cryptosystem (ECC) and Elliptic Curve Diffie-Hellman (ECDH) algorithms are used. They are efficient due to their smaller key size and high level of security.

Visual cryptography was suggested as a solution by Brindha et al. [10] for problems with data storage security. Data serversstore the data in encrypted form. Only after the user has been authenticated by the service provider are the keys to the sharedimage made available. Now, in order to obtain the secret key, user must have the knowledge about the encryption key.

3. PROPOSED METHOD

In this paper, the algorithm is proposed to encrypt and decrypt the data based on a symmetric key algorithm. The proposed algorithm encrypts the data using the binary data encryption method. In this method, we convert the data into the ASCII value and after that add the 100 value into the ASCII value. The ASCII value is then converted into a binary number and split the binary number into two parts. After that, calculates the 1's complement of both parts and combine them. Then, calculates the 2's complement and finds the hexadecimal value of 2's complement. Fig.3 shows the proposed algorithm based on a symmetric key algorithm.

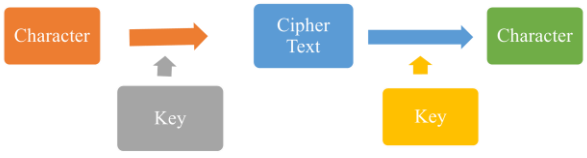

Fig. 3. shows the proposed algorithm based on a symmetric key algorithm.

For example, we have taken a character C and encrypt the character

covert in ASCII value C = 67
add 100 as a key = C + 100
= 67 + 100 = 167
Convert into the binary number = 10100111
Now, Reverse the number = 11100101
Split into two parts and Calculate the 1's complement = 00011010
Calculate the 2's complement = 00011011
Find the hexadecimal of this number
Cipher text = 2B03

Now, decrypt the number using the decryption algorithm

Firstly take the cipher text = 2B03
Convert into the binary number = 00011011
Now, calculate the 1's complement = 11100100
Calculate the 2's complement = 11100101
Now, Reverse the number = 10100111
Convert into the decimal number = 167
Subtract 100 key from the decimal number = 67
Convert into ASCII value for getting the character = C

Algorithm 3 Encryption

Step 1: Convert Character to ASCII value.
Step 2: Add 100 as a key into the ASCII value.
Step 3: Convert the value into the Binary value that is computed in step 2.
Step 4: Add the 0's on the left side of the digit to make the digit in 8-digit form.
Step 5: Now, reverse the number.
Step 6: Split into two part as number-1 and number-2.
Step 7: Now, calculate the 1's Complement of both the parts number-1 and number-2.
Step 8: Concatenate complement number-2 with complement number-1.
Step 9: Calculate the 2's complement of the number that is got from step 8.
Step 10: Now, find the hexadecimal value of the generated number from step 9.
Step 11: Format the hexadecimal value as eight digits and return it as a CipherText.

Example 1 and 2 show the overall process of the proposed algorithm for encryption and decryption. Algorithm 1 and 2 show the proposed cryptography key algorithm based on binary data encryption.

4. RESULT

The accuracy of the proposed cryptography algorithm is higher in comparison to the existing crypto algorithm. The proposed algorithm works well with efficiency. In the proposed section, we describe the working of the proposed cryptography algorithm.

Algorithm 2 Decryption

Step 1: Firstly convert the cipher text into the binary form.
Step 2: Make the binary digit into the 8-digit form by adding the 0's on the left side.
Step 3: Calculate the 2's Compliment of binary digit.
Step 4: After that split the binary number into two numbers as number-1 and number-2.
Step 5: Now, calculate the 1's Complement of both parts.
Step 6: Concatenate complement number-2 with complement number-1.
Step 7: Now, reverse the binary number.
Step 8: Find the ASCII value of the binary number.
Step 9: Subtract the key value 100 from the ASCII.
Step 10: Now, return the ASCII value as a Single character value.

5. CONCLUSION

In cloud computing, information sharing is one of the most important tasks. Recent research shows the advanced development in cloud computing security while sharing data in encrypted form. However, there is a lack of security-based algorithms to encrypt and decrypt the data in a cloud computing environment. In this paper, we proposed an approach to encrypt and decrypt the data based on symmetric key cryptography. In the proposed algorithm, we have used binarybased data conversion and utilized the 1's and 2's complement function to encrypt and decrypt the data. It enhances data security in a cloud computing environment as compared to traditional cloud cryptography algorithms. Our proposed method increases the security level up to the maximum level and takes less time in downloading and uploading the files as compared to traditional methods. In the future, Artificial Intelligence (AI) techniques can be used that enhance the security of cloud services.

REFERENCE

[1] Anshika Negi, Mayank Singh and Sanjeev Kumar, "An Efficient Security Framework Design for Cloud Computing using Artificial Neural Networks", International Journal of Computer Applications (0975 - 8887), vol. 129, no. 4, 2015. .

[2] Shakeeba S. Khan and R. R. Tuteja, "Security in Cloud Computing using Cryptographic Algorithms", International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization), vol. 3, no. 1, 2015.

[3] AL-Museelem Waleed and Li Chunlin, "User Privacy and Security in Cloud Computing", International Journal of Security and Its Applications, vol. 10, no. 2, pp. 341-352, 2016.

[4] N N Mosola, M T Dlamini, J M Blackledge, J. H. P Eloff and H S Venter, "Chaos-based Encryption Keys and Neural Key-store for Cloud-hosted Data Confidentiality", Southern Africa Telecommunication Networks and Applications Conference (SATNAC), 2017.

[5] Ramalingam Sugumar and K. Raja, "EDSMCCE: Enhanced Data Security Methodology for Cloud Computing Environment", International Journal of Scientific Research in Computer Science Engineering and Information Technology, vol. 3, no. 3, 2018, ISSN 2456-3307.

[6] Reshma Suryawanshi and Santosh Shelke, "Improving Data Storage Security in Cloud Environment Using Public Auditing and Threshold Cryptography Scheme", International Conference on Computing Communication Control and Automation (ICCUBEA), 2016.

[7] Divya Prathana Timothy and Ajit Kumar Santra, "A hybrid cryptography algorithm for cloud computing security", 2017 International conference on Microelectronic Devices Circuits and Systems (ICMDCS), pp. 1-5, 2017.

[8] Manju Khari, Manoj Kumar and Vaishali, "Secure data transference architecture for cloud computing using cryptography algorithms", 3rd International Conference on Computing for Sustainable Global Development (INDIACom), pp. 2141-2146, 2016.

[9] S. Singh and V. Kumar, "Secured user's authentication and private data storage-access scheme in cloud computing using Elliptic curve cryptography", 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom), pp. 791-795, 2015.

[10] K. Brindha and N. Jeyanthi, "Securing cloud data using visual cryptography", International Confernce on Innovation Information in Computing Technologies, pp. 1-5, 2015.

[11] Dharitri Talukdar, "Study on symmetric key encryption: An Overview", International Journal

of Applied Research, vol. 1, no. 10, pp. 543-546, 2015.

[12] David G. Rosado, Eduardo Fernandez-Medina and Eduardo B Fernandez, ”An analysis of security issues for cloud computing”, Journal of Internet Services and Applications, 2013.

[13] G. Devi and M. Pramod Kumar, ”Cloud Computing: A CRM Service Based on a Separate Encryption and Decryption using Blowfish algorithm”, International Journal of Computer Trends and Technology, vol. 3, no. 4, pp. 592-596, 2012, ISSN 2231-2803.

[14] Deepanshi Nanda and Sonia Sharma, ”Security in Cloud Computing using Cryptographic Techniques”, International Journal of Computer Science and Technology, vol. 8, no. 2, 2017.

[15] Adnaan Arbaaz Ahmed and M. I. Thariq Hussan, ”Cloud Computing: Study of Security Issues and Research Challenges”, International Journal of Advanced Research in Computer Engineering Technology (IJARCET), vol. 7, no. 4, 2018, ISSN 2278 - 1323.

[16] Moulika Bollinadi and Vijay Kumar Damera, ”Cloud Computing: Security Issues and Research Challenges”, Journal of Network Communiations and Emerging Technologies (JNCET), vol. 7, no. 11, 2017