2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) | 979-8-3503-9926-4/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICACITE57410.2023.10182499

A Novel Hybrid Encryption Technique for Cloud Data Security

Papri Das
Assistant Professor
School of IT,
AURO University
India
papri.ghosh@aurouniversity.edu.in

Sunil Kumar
Assistant Professor
School of IT,
AURO University
India
sunil.kumar@aurouniversity.edu.in

***Abstract*- In this digital world, as the internet has become an integral part of our daily life and we are heavily using it to exchange data of numerous types. Cloud computing is also a type of internet-based computing which has established itself as a potential business model of the most rapidly expanding sector of the information technology industry. Most IT-related businesses, organizations, and educational institutions migrating their operations to the cloud to save their IT infrastructure cost and maintenance. On the other hand, people are also worried about the safety and privacy of their data, which is kept on the servers of the service providers. To address this aspect, in this paper, we have studied existing available solutions given by many researchers and proposed a novel hybrid encryption scheme as a means of ensuring the confidentiality and safety of the data stored in our cloud-based dynamic environment.**

Keywords: Data Security; Hybrid Encryption; Cloud Computing; Cloud Security; Cryptography

I. INTRODUCTION

The term "cloud computing" refers to a network paradigm providing ubiquitous, on-demand access to a pool of configurability computing resources over the internet (e.g., servers, applications, services, and networks). Various businesses use the cloud in accordance with their convenience based on the three different service models (SaaS, PaaS, and IaaS) and four different deployment types (Public cloud, Hybrid cloud, Private cloud, and Community cloud) [1]. The software and data that a user or client accesses may be kept on various servers spread across various locations. Because of internet-based computing both service providers and users faced with various security challenges like how to maintain the confidentiality, integrity, and availability of the customer data [2]. As virtualization is the backbone of cloud computing model. To preserve and use data, many governments have created and implemented several laws and regulations. Since the credit card sector in the US has been safe, very strict security measures are becoming the norm. More nations are forming an alliance or conglomerate to establish strict security standards. As per the characteristics of cloud model is service-oriented and prioritizes lowering costs, using less equipment, and only paying for services that are really used. The cloud can be accessed from anywhere because it is managed remotely. The cloud provider makes use of computer services. Important data on the cloud may be accessed by unauthorised people, making it unsecure[3]. Therefore, there is a need of a strong encryption technique for this internet based cloud computing model. Cryptography provides a number of techniques to encrypt and decrypt the plain text s that we can achieve the confidentiality and our message will remain secret from the intruder. There are two main systems: symmetric and asymmetric cryptosystems that are very famous nowadays [4]. In symmetric cryptosystem, we will use the same key for the encryption and decryption. DES, 3DES, AES, Blowfish are common names of symmetric encryption, whereas there will be two different keys known as private and public keys: one for the encryption and another for the decryption. Asymmetric encryption technique is widely used in digital signature generation and hashing that is mostly used in blockchain technology. ECC and RSA algorithms are widely used asymmetric encryption techniques. Therefore, with the help of cryptography, we can easily achieve the CIA (Confidentiality, Integrity, and Availability) three pillars of information security [5].

II. RELATED WORK

There are many researchers, who has used the cryptography techniques to provide the security to the information available on the local information system, computer network or even on the cloud computing environment that's fully operated on the internet. Kumar et al [6] developed a new encryption technique for the private cloud environment and implemented by using the Java programming language. To provide security to cloud big data environment [7] proposed an agent- based security model for computing the big data on the cloud environment. In [8] authors have done a systematic analysis on open security challenges and opportunities in cloud computing and identified current data security challenges and their solutions that can be used to overcome the risk involved in cloud computing. They have also suggested encryption as a solution to secure the information in a better manner. In this paper, authors have also reviewed the services related to Sql and Nosql data. To better comply with government and organizational data security regulations, the authors of [9] demonstrated how an HFL system can be used to assess data and user access restriction based on data sensitivity. Prominent researchers have discussed data security and its efficacy [11, 12]. Even several scientists suggested security techniques using renowned mathematical techniques. [18,19,20].

In [10] author has made a deep analysis on security and also presented a new type based keyword search technique to enable users to search keywords from the encryption-protection data. Also, he suggested the method to manage the encrypted big data also on the cloud. Kumar et al [13] has focused on the vehicular ad hoc network that's equipped with sensor and communication and Vehicular Cloud Environment (VCE) that is a new emerging research field in cloud and

vehicular network, which gives four-wheels like cars networking and sensor capabilities for V2I or V2V communication with roadside infrastructure. They have proposed and prove a new security model based using the random oracle concept. Because of the complexity due to high image resolution in cloud authors of [14] proposed an Advanced Cipher-text Algorithm (ACTA) that provides extra security needed tools for the privacy sensitive medical images. In [15] authors provided the protection to healthcare data developed light weight framework. [16] proposed a semantic machine learning algorithm for cyber threat monitoring and detection systems. In [17] authors has deeply analyzed and suggested a list of threats, vulnerabilities as well as their countermeasures related to cloud computing environment. Authors of [21] proposed and simulated an encryption approach for securing image-based communication by using the particle swarm optimization to receive optimized encryption effect. In [22] authors suggested hybrid cryptographic algorithm to protects information or by using substitution and transposition encryption techniques. In [23-27] authors proposed homomorphic encryption technique for cloud environment. After reviewing these research articles, we find that we need a hybrid encryption technique to provide an effective security solution in the cloud computing environment.

III. Proposed Hybrid Encryption Technique

The technique which we have proposed is based on the fundamental methods of cryptography. It is a hybrid method which combines both the transposition and substitution method. In the traditional substitution method, the plain text converts to cipher by substituting some digits based on the type of the key. In the same manner the plain text converts to cipher in a transposition method by interchanging the columns. Classical transposition is a method where the matrix columns are interchanged based on the types of the keys. The proposed method applies substitution twice, where three different keys are used. The fourth key will be used for transposition. The fourth key is randomly generated which depends on the size of the matrix. For decryption the same process is followed in reverse way and plain text is obtained from the cipher text. The forte of the algorithm is the different keys, and the idea is to make the algorithm highly secured. The same keys will be used for encryption and decryption. In total four different keys will be generated to make the algorithm more secure. The encryption technique steps can be described below:

STEP I: Input the text from the user.

STEP II: Count the characters and white space of given plain text (N).

STEP III: Convert the given text to equivalent ASCII code.

STEP IV: Form a square matrix (M) with ASCII value of N (characters to be placed in the matrix row wise). Empty cell to be filled with ASCII value of ” *”.

STEP V: Divide the elements of the matrix as: diagonal, upper triangle and lower triangle.

STEP VI: Using keys k1, k2 and k3 add with elements of diagonal, upper triangle and lower triangle of the matrix respectively.

STEP VII: Read the element of the matrix into outer, middle and inner circle.

STEP VIII: Using keys k1, k2 and k3 add with elements of outer, middle and inner circle of the matrix respectively.

STEP IX: Rearrange the matrix column wise as per key k4. Read the matrix row wise.

STEP X: Convert ASCII to characters to obtain the cipher.

Also the encryption flow has been depicted in Fig.1.

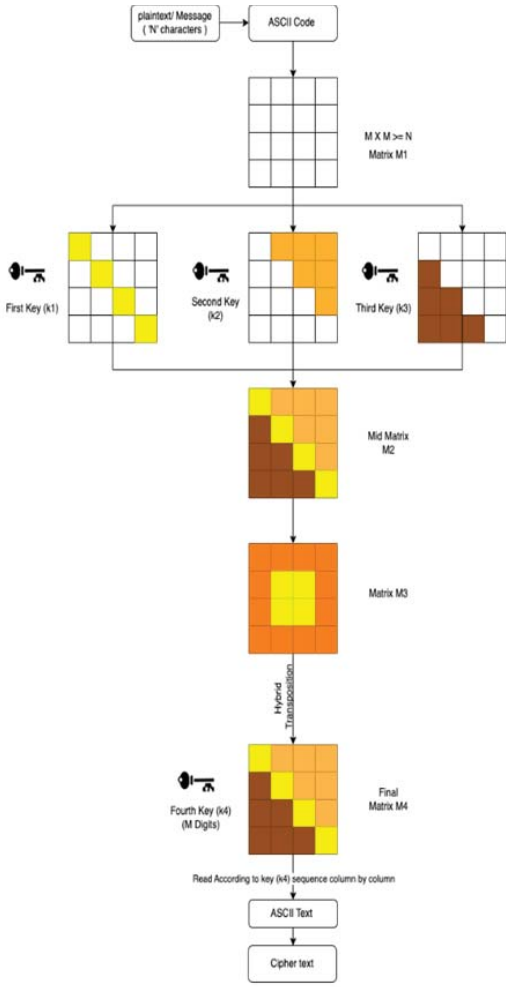

Fig. 1. Encryption Flow Diagram

IV. Illustrative Example

In this section, we have demonstrated the proposed encryption technique with the help of an example.

Step-1: First we will take the plain text as an input: Suppose our input value is ‘Auro University.’

Step-2: Count character of plain text with white space: 15(including space)

Step-3: Convert text to equivalent ASCII value:

Auro University: 65 117 114 111 32 85 110 105 118 101 114 115 105 116 121

Step-4: We will arrange in a square matrix form M1:

Size of matrix (M X M): 4 X 4, where M * M or (M2) ⩾ N (i.e., 16 > 15) as shown in Fig. 2.

Plain Text: Auro University

65	117	114	111
32	85	110	105
118	101	114	115
105	116	121	

65	117	114	111
32	85	110	105
118	101	114	115
105	116	121	88

Fig. 2. ASCII value of Plaintext

Fig. 3. Empty Cell filled with ASCII of 'X'

We will arrange the character row wise.

We must fill the empty cells of the matrix with ASCII value of maybe X (For convenience). As shown in Fig. 3.

Step-5: Divide and read the matrix as: diagonal, triangle above diagonal and triangle below diagonal (65, 85, 114, 88) (117, 114, 111, 110, 105, 115) (32, 118, 101, 105, 116, 121) as shown in Fig. 4.

65	117	114	111
32	85	110	105
118	101	114	115
105	116	121	88

Fig. 4. Matrix with Diagonal, Upper & Lower Triangle

Step-6: The size of the keys will be in two digits (0-99). Using key 1, key 2 and key 3 substitute triangle above diagonal and triangle below diagonal by adding the keys with the ASCII value respectively as shown in Fig. 4. A new matrix M2 is formed shown in Fig.5.

Key K1 =10, K2 = 20, K3 = 40

65 + 20	117 + 10	114 + 10	111 + 10
32 + 40	85 + 20	110	105 + 10
118 + 40	101 + 40	114 + 20	115 + 10
105 + 40	116 + 40	121 + 40	88 + 20

85	127	124	121
72	105	110	115
158	141	134	125
145	156	161	108

(Matrix M2)

Fig. 5. Keys added with elements

Step-7: Divide the new matrix into outer circle, middle and inner circle shown in fig. 6

85	127	124	121
72	105	110	115
158	141	134	125
145	156	161	108

Fig. 6. Matrix with outer and inner circle

Step-8: Using key 1, key 2 and key 3 substitute outer circle, middle circle and inner circle as shown in Fig 7.

A new matrix will be formed M3 as shown in fig. 8.

K1 =10, K2 = 20

85 + 10	127 + 10	124 + 10	121 + 10
72 + 10	105 + 20	110 + 20	115 + 10
158 + 10	141 + 20	134 + 20	125 + 10
145 + 10	156 + 10	161 + 10	108 + 10

95	137	134	131
82	125	130	121
168	161	154	132
155	166	171	118

Fig. 7. Resulting matrix M3

Step-9: Key 4 will be used to apply transposition on M3. The length of the key 4 will depend on the size of the diagonal of the matrix. Here the diagonal size is 4, so the keys will be a combination of 0, 1, 2 and 3 i.e., each digit in the key should be less than the diagonal size. Also, the digits can't be repeated. The column in the matrix is rearranged as per the digits in the key K4 as shown in Fig. 9.

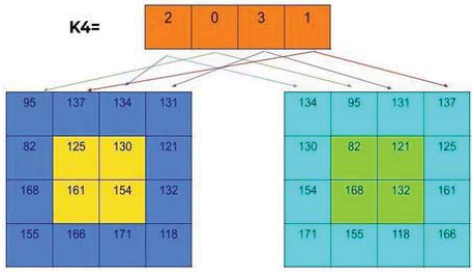

Fig. 8.

Fig. 9. Column rearranged as per Key-k4

Length of key 4 depends on diagonal size of M3.

The digits of the key 4 will be less than length of key 4 and the digits won't repeat.

The columns of M3 are swapped as per the digits of key 4. A new matrix M4 has been formed.

Step-10: Read the values of the M4 row wise as depicted in Fig. 10. Convert the ASCII to equivalent character and this is our cipher as shown in Fig. 11:

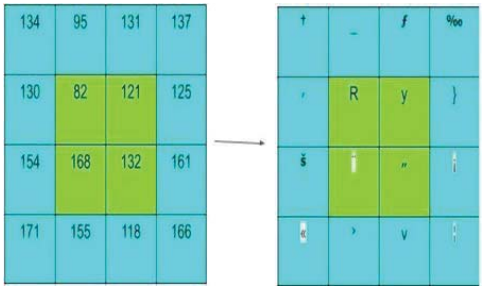

Fig. 10. Matrix M4

Fig. 11. Final Cipher

134 95 131 137 130 82 121 125 154 168 132 161 171 155 118 166

Store the cipher in the database with a unique id no.

V. Analysis of Proposed Technique

In the proposed algorithm keys are generated only with numbers. k1, k2, k3 and k4 where k1, k2 and k3 are formed of two digits and size of k4 depend on the order of the matrix. Since the length of the keys k1, k2 and k3 are two, the number

of digits will be 0- 9 that is number of possible digits will be 10. The possible combination of the keys will be (10)2..The size of k4 depends on the order of the matrix, so if the order of the matrix is M=5, then possible combination of keys will be (5)5. k1, k2, k3, k4 together will be (10)2 x (10)2 x (10)2 x (5)5 = 3.125x (10)9. It becomes difficult for the attacker to cryptanalyze and will take a huge amount of time to check the keys and get the correct ones.

VI. Conclusion

To conduct our day-to-day e-commerce and other general regular online operations, we make use of the internet-based computing known as cloud computing. After reviewing various challenges and existing solutions proposed by researchers, we proposed and designed a novel encryption algorithm to address this issue in a quite simple manner. The proposed encryption technique is very simple in nature as single key is used for the encryption and decryption process for the cloud computing environment. This technique would be beneficial in enhancing the level of security that is now offered through the clouds. In the not-too-distant future, we intend to build and deploy this innovative method on the cloud in order to further refine it.

References

[1] "The NIST Defeinition of Cloud Computing", https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf

[2] Singh, A. (2019). Security concerns and countermeasures in cloud computing: a qualitative analysis. International Journal of Information Technology, 11, 683-690.

[3] J. P. Singh, Mamta, and S. Kumar, "Authentication and encryption in Cloud Computing," 2015 Int. Conf. Smart Technol. Manag. Comput. Commun. Control. Energy Mater. ICSTM 2015 - Proc., no. May, pp. 216–219, 2015, doi: 10.1109/ICSTM.2015.7225417.

[4] K. Timraz, T. Barhoom and T. Fatayer, "A Confidentiality Scheme for Storing Encrypted Data through Cloud," 2019 IEEE 7th Palestinian International Conference on Electrical and Computer Engineering (PICECE), Gaza, Palestine, 2019, pp. 1-5, doi: 10.1109/PICECE.2019.8747193.

[5] S. William, Cryptography and Network Security: Principles and Practice, 2nd edition, Prentice-Hall, Inc., 1999 pp 23-50.

[6] S. Kumar, J. Shekhar, and J. P. Singh, "Data security and encryption technique for cloud storage," in Conference: CSI-2015;50th Golden Jubilee Annual Convention on Digital Life, 2018, vol. 729, pp. 193–199, doi: 10.1007/978-981-10-8536-9_19/COVER/

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

[8] S. Kumar, J. Shekhar, and H. Gupta, "Agent based security model for cloud big data," ACM Int. Conf. Proceeding Ser., vol. 04-05-Marc, 2016, doi: 10.1145/2905055.2905202.

[9] R. V. Rao and K. Selvamani, "Data security challenges and its solutions in cloud computing," Procedia Comput. Sci., vol. 48, pp. 204–209, 2015.

[10] Mohammadian, M., Hatzinakos, D. A hierarchical fuzzy logic systems frame work for data security. Int. j. inf. tecnol. 9, 147–157 (2017). https://doi.org/10.1007/s41870-017-0023-x

[11] F. Ahmadi Sonia G. Gupta S. R. Zahra P. Baglat and P. Thakur "Multi-factor Biometric Authentication Approach for Fog Computing to ensure Security Perspective" 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom) pp. 172-176 2021.

[12] M. Arora and Sonia "The Latest Trends in Collaborative Security System" 2021 4th International Conference on Recent Innovations in Computing (ICRIC-2021) vol. 2 2021

[13] Y. Yang, X. Zheng, and B. Lin, "Type based keyword search for securing big data," Proc. - 2013 Int. Conf. Cloud Comput. Big Data, CLOUDCOM-ASIA 2013, pp. 354– 359, 2013, doi: 10.1109/CLOUDCOM-ASIA.2013.107.

[14] V. Kumar, A. M. A. L. I. Al-tameemi, A. Kumari, M. W. Falah, and A. A. A. B. D. El- latif, "PSEBVC : Provably Secure ECC and Biometric based Authentication Framework using Smartphone for Vehicular Cloud Environment," IEEE Access, vol. PP, p. 1, 2022, doi: 10.1109/ACCESS.2022.3195807.

[15] S. P. Praveen, S. Sindhura, A. Madhuri and D. A. Karras, "A Novel Effective Framework for Medical Images Secure Storage Using Advanced Cipher Text Algorithm in Cloud Computing," 2021 IEEE International Conference on Imaging Systems and Techniques (IST), Kaohsiung, Taiwan, 2021, pp. 1-4, doi: 10.1109/IST50367.2021.9651475.

[16] Chaudhary, R.R.K., Chatterjee, K. A lightweight security framework for electronic healthcare system. Int. j. inf. tecnol. 14, 3109–3121 (2022). https://doi.org/10.1007/s41870-022-01034-4.

[17] S. Kumar, B. P. Singh and V. Kumar, "A Semantic Machine Learning Algorithm for Cyber Threat Detection and Monitoring Security," 2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), Greater Noida, India, 2021, pp. 1963-1967, doi: 10.1109/ICAC3N53548.2021.9725596.

[18] Sonia A. Alsharef P. Jain M. Arora S. R. Zahra and G. Gupta "Cache Memory: An Analysis on Performance Issues" 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom) pp. 184-188 2021.

[19] Bhakuni, M., Kumar, K., Sonia, Iwendi, C., & Singh, A. Evolution and Evaluation: Sarcasm Analysis for Twitter Data Using Sentiment Analysis. Journal of Sensors, vol. 2022, Article ID 6287559, 10 pages, 2022. https://doi.org/10.1155/2022/6287559

[20] J. Sharma, M. Arora, Sonia and A. Alsharef, "An illustrative study on Multi Criteria Decision Making Approach: Analytical Hierarchy Process," 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2022, pp. 2000-2005, doi: 10.1109/ICACITE53722.2022.9823864.

[21] Ahmad, Musheer & Alam, Mohammad & Umayya, Zeya & Khan, Sarah & Ahmad, Faiyaz. (2018). An image encryption approach using particle swarm optimization and chaotic map. International Journal of Information Technology. 10. 10.1007/s41870-018-0099-y.

[22] Ghosh, P., Thakor, V. (2019). Optimization of Hybrid Encryption Algorithm for Secure Communication System. In: Yang, XS., Sherratt, S., Dey, N., Joshi, A. (eds) Third International Congress on Information and Communication Technology. Advances in Intelligent Systems and Computing, vol 797. Springer, Singapore. https://doi.org/10.1007/978-981-13-1165-9_89

[23] Min Zhao E, Yang Geng, Homomorphic Encryption Technology for Cloud Computing, Procedia Computer Science, Volume 154, 2019, Pages 73-83, ISSN 1877-0509,https://doi.org/10.1016/j.procs.2019.06.012.

[24] P. Ajay, Ruihang Huang, "Wearable Sensor Data for Classification and Analysis of Functional Fitness Exercises Using Unsupervised Deep Learning Methodologies", Security and Communication Networks, vol. 2022, Article ID 8706784, 9 pages, 2022. https://doi.org/10.1155/20no mam 22/8706784.

[25] P. Ajay, B. Nagaraj, J. Jaya, "Algorithm for Energy Resource Allocation and Sensor-Based Clustering in M2M Communication Systems", Wireless Communications and Mobile Computing, vol. 2022, Article ID 7815916, 11 pages, 2022. https://doi.org/10.1155/2022/7815916.

[26] Ajay. P, Nagaraj. B, Ruihang Huang, "Deep Learning Techniques for Peer-to-Peer Physical Systems Based on Communication Networks", Journal of Control Science and Engineering, vol. 2022, Article ID 8013640, 12 pages, 2022. https://doi.org/10.1155/2022/8013640.

[27] Kumar, R.S., Nagaraj, B., Manimegalai, P. and Ajay, P., 2022. Dual feature extraction based convolutional neural network classifier for magnetic resonance imaging tumor detection using U-Net and three-dimensional convolutional neural network. Computers and Electrical Engineering, 101, p.108010.