International Journal of Engineering Research and Technology. ISSN 0974-3154, Volume 16, Number 1 (2023), pp. 10-13
© International Research Publication House. http://www.irphouse.com

# A New Encryption Algorithm Helps To Secure The Cloud Storage

**Aritra Dutta[1], Dr. Rajesh Bose[2], Dr. Sandip Roy[2, *] and Shrabani Sutradhar[3]**

*[1] Ph.D., Students, Department of Computational Sciences, Brainware University, India.*
*[2]Professor, Department of Computational Sciences, Brainware University, India.*
*[3]Assistnat Professor, Department of Computational Sciences, Brainware University, India.*

**Abstract**

It is true that cloud computing has become an integral part of various industries, including military, healthcare, education, and more, due to its ability to store large amounts of data and provide easy access to it. However, the issue of data security and privacy is a significant concern for many clients who entrust their sensitive and confidential data to third-party cloud providers. Various cryptographic algorithms are designed to address the security issues in cloud storage frameworks. The Advanced Encryption Standard (AES) algorithm with S-box and NTRU are two such algorithms that can be used to ensure the confidentiality, integrity, and availability of data stored in the cloud. These algorithms are widely used for secure data transmission over a network and storing data in a non-human-readable form. The proposed system that utilizes these algorithms is designed to ensure that the data stored in the cloud is transferred, segmented, encrypted, merged, decrypted, and recovered in a secure and efficient manner. By employing these algorithms, the proposed system aims to enhance the security of multi-cloud storage infrastructures, making it difficult for unauthorized users to access and read the data.

**Keywords:** Advanced Encryption Standard (AES), Cloud Service Providers (CSP), Cryptography, Denial-of-Service, NTRU, S-Box

## I. INTRODUCTION

The cloud refers to a network of remote servers that can store, manage, and process data, and it is often used for storing large amounts of data such as images. Given the sensitive nature of some image data, it is important to ensure that it is protected when it is stored and transmitted. One way to do this is by using encryption, which involves encoding the data so that it can only be accessed by authorized parties who have the encryption key. Cloud computing can be a useful tool for managing large amounts of image data, as it provides access to a wide range of computing resources. However, it is important to ensure that the cloud service provider has appropriate security measures in place to protect the data from unauthorized access or data breaches [1]. Cloud computing is a widely used technology that provides various services like storage, software, and infrastructure. However, as with any technology, there are always potential security risks that need to be addressed [2]. One of the major security risks in cloud computing is denial-of-service (DoS) attacks. In a DoS attack, an attacker floods a system or network with a large number of requests, overwhelming the system and making it unavailable to legitimate users. DoS attacks can be very disruptive and can result in significant downtime and financial losses for businesses. Cloud service providers typically implement various security measures, such as firewalls, intrusion detection systems, and traffic filtering, to mitigate the risks of DoS attacks [3, 4]. However, it is important for users of cloud computing services to also take steps to protect themselves against DoS attacks. This includes using strong passwords, regularly updating software and security patches, and implementing multi-factor authentication to prevent unauthorized access to cloud resources. cloud computing has indeed become an essential part of various industries due to its ability to store large amounts of data and provide easy access to it. Various cryptographic algorithms, including AES with S-box and NTRU, are designed to address the security issues in cloud storage frameworks. These algorithms ensure the confidentiality, integrity, and availability of data stored in the cloud and are widely used for secure data transmission over a network and storing data in a non-human-readable form. The proposed system that utilizes these algorithms aims to enhance the security of multi-cloud storage infrastructures, making it difficult for unauthorized users to access and read the data. By employing the AES algorithm with S-box and NTRU, the system can transfer, segment, encrypt, merge, decrypt, and recover data stored in the cloud in a secure and efficient manner. Cryptography is a critical aspect of secure communication systems, and the strength of encryption largely depends on the security of the S-box used in block ciphers. An S-box is a crucial component of a block cipher that performs substitution of plaintext bits with cipher text bits. To ensure the highest level of security, it is essential to design an S-box that meets several cryptographic properties, such as high nonlinearity, low differential uniformity, and complex algebraic expression [5, 6]. High nonlinearity in S-boxes is necessary to prevent linear attacks, which are attacks where the attacker tries to find a linear relation between the plaintext and cipher text bits. Low differential uniformity is required to prevent differential attacks, which are attacks that exploit the differences between plaintext and cipher text pairs. Complex algebraic expressions in S-boxes make it difficult for attackers to analyze and decipher the encryption [7, 8]. Researchers have proposed several approaches to designing S-boxes that are both dynamic and strong. For instance, the Latin Square S-box approach generates new Latin square S-boxes using a secret key of length 128 bits. The Latin square doubly stochastic matrix is used to construct dynamic S-boxes, while spatiotemporal chaotic systems are utilized to generate hyper-chaotic sequences for constructing S-boxes [9].

## II. CONTRIBUTION OF THE STUDY

The main three contributions of the proposed encryption method algorithm are:

1) Multi-layered approach: The proposed algorithm uses a multi-layered approach to secure data in the cloud. It involves using two encryption techniques (AES and S-BOX) and a public key encryption algorithm (NTRU) to provide high levels of security. This approach makes it difficult for attackers to access the original data even if they manage to break one layer of encryption.
2) Password protection: The proposed algorithm includes a mechanism to protect the encrypted data with a password using NTRU. This step ensures that only authorized users who have the correct key and password can access the original data. The password protection also adds an extra layer of security to the algorithm, making it more difficult for attackers to access the data.
3) Fake data protection: The proposed algorithm includes a mechanism to prevent attackers from accessing the data even if they manage to guess the password. In such a scenario, the attacker will be given fake data instead of the original data, which further enhances the security of the algorithm. This feature ensures that even if the attacker manages to access the encrypted data, they cannot retrieve the original data, making the algorithm more robust.

## III. RELATED WORK

The algorithm developed by Viswanath and Krishna [10] for loading data into a cloud environment. It's great to know that they were able to develop a secure method for uploading data to the cloud. It’s interesting that the authors used a real-time medical dataset to test the performance of their algorithm. Using real-world data is always important to validate the effectiveness of any algorithm or method. The fact that the authors were able to encrypt a 2630KB data set is also impressive. Encryption is an important step in ensuring the security of data that is being uploaded to the cloud. Li, Yu, and Wang, proposed [11] a method for compressing images using compressive sensing (CS), which can save on storage costs. They also introduced an encryption algorithm and authentication method to protect the privacy of images using chaotic systems. The proposed encryption technique likely involves using a chaotic system to generate a key that is used to encrypt the image data. This can help ensure that only authorized parties can access the image data. In paper [12] authors proposed a parallel algorithm for image decoding in the cloud, which utilizes complex symmetry properties of Discrete Fourier Transform (DFT) and a private arbitrary phase key for encryption. The proposed algorithm differs from existing transformation-based encryption systems in that it provides double-key security, which increases the complexity of decoding without the keys. Additionally, the equal methodology used in the algorithm allows the first cycle to consume a share of the time, instead of the decoding algorithm consuming all of the time. The use of DFT in the proposed algorithm is based on the fact that images can be represented as a set of frequencies. By applying DFT to an image, it can be transformed into its frequency domain representation, which can then be encrypted using a private arbitrary phase key. The decryption process involves using the same key to recover the original image from its encrypted frequency domain representation. The double-key security feature of the proposed algorithm adds an extra layer of protection to the encryption process, making it more difficult for unauthorized users to access the encrypted data. The equal methodology used in the algorithm also helps to reduce the time required for the decryption process, making it more efficient for use in the cloud. Overall, the proposed algorithm provides a novel approach to image encryption that takes advantage of the properties of DFT and private arbitrary phase keys to provide a high level of security and efficiency. The authors of the paper [13] "Garg, P., Sharma, M., Agrawal, S., & Kumar, Y." [6] discussed the three main types of cloud services, which are Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). They also explored the concepts of cryptography and steganography and introduced a split algorithm that helps to ensure the security of content stored or transferred to the cloud. Cryptography is the practice of secure communication in the presence of third parties, while steganography is the practice of concealing messages or information within other messages or information. The split algorithm introduced by the authors is a security measure that divides a message into several parts and encrypts each part separately before sending it to the cloud. This ensures that even if an attacker manages to intercept one part of the message, they will not be able to decipher the entire message. The authors also discussed the importance of security measures in cloud computing, as the transfer and storage of sensitive information on the cloud can pose a significant risk. They proposed that using cryptography and steganography, along with the split algorithm, can help to ensure the security of content stored or transferred to the cloud. Bale, Kamboj, and Luthra's paper [14] discusses different block-wise encryption algorithms, namely AES, BRA, RC4, and Blowfish, all of which are part of symmetric cryptography and use a single key for both encoding and decoding.

The authors also proposed a multithreading process to reduce the delay parameter and achieve a low delay time. According to the authors, their proposed method was able to encode text files in around 20% less time than the AES algorithm. However, without further details or context, it is difficult to provide more specific information or analysis on their findings. Olanrewaju, Abdullah, and Darwish proposed [15] a hybrid algorithm that combines the AES and Blowfish algorithms to provide strong encryption for data stored on the cloud with increased performance and reliability compared to AES alone [16]. On the other hand, Bhardwaj, Subrahmanyam, Awasthi, and Sastry discussed [17] various concepts related to cryptography, such as block ciphers, stream ciphers, symmetric and asymmetric algorithms. They also talked about the RSA algorithm and the Diffie-Hellman Key Exchange algorithm, and how they are used in security [18]. Additionally, they compared different algorithms of symmetric and asymmetric cryptography and concluded that MD5 is faster than others when encoding.

```
iv = CT_aes_decrypt[:16]
cipher = AES.new(q, AES.MODE_CBC, iv)
decrypted_data =
unpad(cipher.decrypt(CT_aes_decrypt[16:]), AES.block_size
```

## VIII. USECASE

A financial institution wants to securely store sensitive customer information such as social security numbers, financial statements, and personal identification documents in the cloud. They want to ensure that the data is protected against unauthorized access, theft, and cyber-attacks [19, 20]. To achieve this, the institution decides to implement the encryption algorithm described above. They first generate a private key 'q' and use it to encrypt the data file using the AES algorithm. The resulting cipher-text 'CT' is then re-encrypted using S-Box to provide an additional layer of security. To further enhance the security of the encrypted data, the institution decides to use the NTRU encryption algorithm to encrypt the data with a password. This ensures that even if an attacker gains access to the encrypted data, they will not be able to decrypt it without the correct password. When authorized personnel need to access the original data, they use the private key and password to decrypt the data. The institution can also implement access control measures to ensure that only authorized personnel can access the data.

By implementing this encryption algorithm, the financial institution can store sensitive customer information in the cloud without compromising security. The multi-layered approach provides robust protection against cyber threats, ensuring that customer information remains confidential and secure.

## IX. RESULTS AND DISCUSSION

The proposed algorithm uses a combination of AES, S-Box, and NTRU encryption techniques, while other well-known encryption algorithms include RSA, Blowfish, and Twofish [3].

AES is a widely used encryption standard and is known for its strong security and speed, while RSA is a public key encryption algorithm that is often used for secure communication over insecure networks. Blowfish and Twofish are also symmetric key encryption algorithms that are known for their fast encryption and decryption times.

The use of S-Box and NTRU in the proposed algorithm provides an additional layer of security and ensures that even if one encryption technique is compromised; the data remains secure. However, it is worth noting that the effectiveness of any encryption algorithm depends on its implementation and the strength of its keys [4].

Here's a brief comparison between the proposed algorithm using AES, S-Box, and NTRU encryption techniques and other well-known encryption algorithms such as RSA, Blowfish, and Twofish, based on the parameters of Encryption/Decryption Speed, Key Size, Memory Usage, and Network Latency:

1. Encryption/Decryption Speed: The encryption/decryption speed of an algorithm is an important factor to consider, especially when large amounts of data need to be encrypted or decrypted. AES, Blowfish, and Twofish are all symmetric encryption algorithms that are faster than asymmetric encryption algorithms like RSA. The proposed algorithm that combines AES, S-Box, and NTRU encryption techniques may have a slightly slower encryption/decryption speed compared to AES, Blowfish, and Twofish, but it is still faster than RSA [3].
2. Key Size: The key size determines the level of security provided by an encryption algorithm. A larger key size provides stronger security but also increases the complexity and computational requirements of the algorithm. AES, Blowfish, and Twofish all support key sizes of up to 256 bits, while RSA supports key sizes of up to 4096 bits. The proposed algorithm that combines AES, S-Box, and NTRU encryption techniques supports a key size of 512 bits, which is larger than the key size supported by AES, Blowfish, and Twofish but smaller than the key size supported by RSA.
3. Memory Usage: Memory usage is an important factor to consider when implementing encryption algorithms, especially in resource-constrained environments such as mobile devices or embedded systems. AES, Blowfish, and Twofish are all relatively lightweight in terms of memory usage, while RSA is more memory-intensive. The proposed algorithm that combines AES, S-Box, and NTRU encryption techniques may require more memory than AES, Blowfish, and Twofish due to the additional encryption steps.
4. Network Latency: Network latency is the amount of time it takes for data to travel from one point to another over a network [21]. This is an important factor to consider when implementing encryption algorithms for network communication. AES, Blowfish, and Twofish are all well-suited for network communication due to their relatively low computational requirements and small message size. RSA is less suited for network communication due to its higher computational requirements and larger message size. The proposed algorithm that combines AES, S-Box, and NTRU encryption techniques may have a slightly larger message size due to the additional encryption steps, but it is still well-suited for network communication.

In summary, the proposed algorithm that combines AES, S-Box, and NTRU encryption techniques provides a good balance between encryption/decryption speed, key size, memory usage, and network latency. It may be slightly slower than AES, Blowfish, and Twofish but faster than RSA, and supports a key size that is larger than AES, Blowfish, and Twofish but smaller than RSA. The memory usage may be higher than AES, Blowfish, and Twofish due to the additional encryption steps, but it is still well-suited for resource-constrained environments. Finally, the network latency may be slightly higher due to the larger message size, but it is still suitable for network communication.

## X. CONCLUSION AND FUTURE WORK

In conclusion, the proposed system utilizing the AES algorithm with S-Box and NTRU can enhance the security of multi-cloud storage infrastructures and protect sensitive data from unauthorized access. By employing a multi-layer encryption approach, the system can ensure the confidentiality, integrity, and availability of data stored in the cloud. The system's efficiency and security can be further improved by implementing additional security measures, such as access control mechanisms, intrusion detection systems, and data backup strategies.

Future work can focus on enhancing the system's scalability and flexibility, considering the rapid growth of data volumes and the increasing complexity of cloud storage frameworks. The system can also be extended to support secure data sharing and collaboration among different cloud users while maintaining data confidentiality and integrity. Additionally, the system can incorporate machine learning and artificial intelligence techniques to provide advanced threat detection and mitigation capabilities. Overall, the proposed system presents a promising solution to the challenges of cloud data security and privacy.

## REFERENCES

[1] Viswanath, G., & Krishna, P. V. (2021). Hybrid encryption framework for securing big data storage in multi-cloud environment. *Evolutionary Intelligence*, *14*, 691-698.

[2] Zhou, M., Zhang, R., Xie, W., Qian, W., & Zhou, A. (2010, November). Security and privacy in cloud computing: A survey. In *2010 Sixth International Conference on Semantics, Knowledge and Grids* (pp. 105-112). IEEE.

[3] Sutradhar, S., Karforma, S., Bose, Rajesh., & Roy, S. (2023). A Dynamic Step-wise Tiny Encryption Algorithm with Fruit Fly Optimization for Quality of Service improvement in healthcare, Healthcare Analytics, 3(2023):1-15.

[4] Nizam Chew, L. C., & Ismail, E. S. (2020). S-box construction based on linear fractional transformation and permutation function. Symmetry, 12(5), 826.

[5] Leng, Y., Chen, J., & Xie, T. (2020). More Low Differential Uniformity Permutations over [mathematical expression not reproducible] with k Odd. Mathematical Problems in Engineering, 2020.

[6] Al Solami, E., Ahmad, M., Volos, C., Doja, M. N., & Beg, M. M. S. (2018). A new hyperchaotic system-based design for efficient bijective substitution-boxes. entropy, 20(7), 525.

[7] Bansal, B., Jenipher, V. N., Jain, R., Dilip, R., Kumbhkar, M., Pramanik, S., ... & Gupta, A. (2022). Big Data Architecture for Network Security. *Cyber Security and Network Security*, 233-267.

[8] Isa, H., Jamil, N., & Z'aba, M. R. (2013, November). S-box construction from non-permutation power functions. In Proceedings of the 6th International Conference on Security of Information and Networks (pp. 46-53).

[9] Wang, X., & Yang, J. (2020). A novel image encryption scheme of dynamic S-boxes and random blocks based on spatiotemporal chaotic system. *Optik*, *217*, 164884.

[10] Viswanath, G., & Krishna, P. V. (2021). Hybrid encryption framework for securing big data storage in multi-cloud environment. *Evolutionary Intelligence*, *14*, 691-698.

[11] Li, H., Yu, C., & Wang, X. (2021). A novel 1D chaotic system for image encryption, authentication and compression in cloud. *Multimedia Tools and Applications*, *80*(6), 8721-8758.

[12] Rad, P., Muppidi, M., Jaimes, A. S., Agaian, S. S., & Jamshidi, M. (2015, April). A novel image encryption method to reduce decryption execution time in cloud. In *2015 Annual IEEE Systems Conference (SysCon) Proceedings* (pp. 478-482). IEEE.

[13] Garg, P., Sharma, M., Agrawal, S., & Kumar, Y. (2019). Security on cloud computing using split algorithm along with cryptography and steganography. In *International Conference on Innovative Computing and Communications: Proceedings of ICICC 2018, Volume 1* (pp. 71-79). Springer Singapore.

[14] Bala, B., Kamboj, L., & Luthra, P. (2018). Secure File Storage In Cloud Computing Using Hybrid Cryptography Algorithm. *International Journal of Advanced Research in Computer Science*, *9*(2), 773-776.

[15] Olanrewaju, R. F., Abdullah, K., & Darwis, H. (2018, November). Enhancing cloud data security using hybrid of advanced encryption standard and blowfish encryption algorithms. In *2018 2nd East Indonesia Conference on Computer and Information Technology (EIConCIT)* (pp. 18-23). IEEE.

[16] Chatterjee, P., Bose, R., & Roy, S. (2020). A review on architecture of secured cloud based learning management system. *Journal of Xidian University*, *14*(7), 365-376.

[17] Bhardwaj, A., Subrahmanyam, G. V. B., Avasthi, V., & Sastry, H. (2016). Security algorithms for cloud computing. *Procedia Computer Science*, *85*, 535-542.

[18] Sahana, S., Bose, R., & Sarddar, D. (2016). Harnessing RAID mechanism for enhancement of data storage and security on cloud. *Brazilian Journal of Science and Technology*, *3*, 1-13.

[19] Bose, R., & Sarddar, D. (2015). A secure hypervisor-based technology create a secure cloud environment. *International Journal of Emerging Research in Management & Technology*, *4*(2), 44-49.

[20] Dey, R. K., Roy, S., Bose, R., & Sarddar, D. (2021). Assessing commercial viability of migrating on-premise mailing infrastructure to cloud. *Int. J. Grid Distrib. Comput*, *14*, 1-10.

[21] Chakraborty, S., Bose, R., Roy, S., & Sarddar, D. (2019). Auditing deployed software licenses on cloud using a secure loopback protocol. Int. J. Recent. Technol. Eng, 8(3), 1-5.

[22] Bose, R., Roy, S., & Sarddar, D. (2017). On Demand IOPS Calculation in Cloud Environment to Ease Linux-Based Application Delivery. In *Proceedings of the First International Conference on Intelligent Computing and Communication* (pp. 71-77). Springer Singapore.