IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 3, March 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

||Volume 13, Issue 3, March 2024||

|DOI:10.15680/IJIRSET.2024.1303217|

Secure Dispersal: An Innovative Approach to Encrypting Cloud Storage

T Sreenivasula Reddy [1],S Haseeb[2], T Charan Teja[3] , B Karthik[4], P Suneel Reddy[5]

[1]Assistant Professor, Department of CSE, AITS, Tirupati, India

[2, 3,4,5]Student, Department of CSE, AITS, Tirupati, India

ABSTRACT: Distributed storage administration has been instrumental in advancing cloud computing by effectively managing data across multiple locations. However, despite its benefits, security incidents continue to occur due to oversight and malicious attacks, resulting in significant breaches. To address these challenges, we propose the Secure Dispersal: An Innovative Approach to Encrypting Cloud Storage (CSSM), designed to enhance data confidentiality in the cloud. CSSM combines data dispersal and distributed storage techniques to encrypt, fragment, and distribute data, thus reducing the risk of breaches. The CSSM cloud secure storage mechanism utilizes hierarchical management and integrates user passwords with secret sharing to thwart the unauthorized exposure of cryptographic material. Empirical findings indicate that CSSM adeptly fortifies data at the storage layer while incurring minimal time overhead. For instance, the process of uploading or downloading a 5GB file via CSSM consumes only 646 or 269 seconds, respectively, rendering it satisfactory for users.

KEYWORDS: Cloud computing, data dispersal, data encryption, key management, storage security.

I.INTRODUCTION

The distributed computing has witnessed remarkable advancements, particularly with the emergence of storage-as-a-service, which has become crucial for various applications such as pattern recognition, image analysis, and plagiarism detection. However, despite the invaluable services provided, the OpenStack Swift framework, a cornerstone in this field, is confronted with significant security threats. Issues such as user data leakage, often stemming from management negligence and malicious attacks, persist. Moreover, default configurations that store data in plaintext further escalate the risk of unauthorized access to user data. While various encryption schemes have been proposed to mitigate data leakage during AI processes, they necessitate robust key management systems to safeguard cryptographic materials.
In addressing these challenges, a secure distributed storage system based on the Hadoop framework, aiming to ensure data confidentiality through dispersal and encryption. However, the reliance on third-party entities for key management introduces additional security concerns. To mitigate these challenges, this paper proposes SDIAECS (Secure Dispersal: An Innovative Approach to Encrypting Cloud Storage), a novel approach that integrates data dispersal and encryption to securely store cloud data and keys in fragmented ciphertexts. Additionally, SDIAECSleverages user passwords and secret sharing techniques to enhance key security. The implementation of SDIAECSon the OpenStack Swift framework underwent rigorous testing.

II.RELATED WORKS

[1] For the purpose of monitoring, controlling, and automating intricate processes and infrastructure that are incorporated into vital industrial sectors and have an impact on our daily lives, modern control frameworks are indispensable. Corporate infrastructure has moved from being isolated and independent to being centralized as networking and automation have advanced. This change has left them open to behavior-based cybersecurity threats, though, as conventional defenses like intrusion detection systems and web application firewalls might not be enough. These attacks alter processes and control flow, possibly completely stopping these systems from operating. This study assesses the efficacy of signature-based detection techniques and focuses on applying process analysis to identify threats in industrial control infrastructure systems. In order to detect behavior-based attacks in real-time and identify aberrant behavior in industrial control device logs, the proposed study introduces a pattern recognition method named "Catching the-Undetectable (CTI)".

[2] In the digital age of today, where computer-generated images are common in ads, publications, websites, televisions, and more, picture forensics based on lighting assessment is essential. Nonetheless, the increasing usage of

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

||Volume 13, Issue 3, March 2024||

|DOI:10.15680/IJIRSET.2024.1303217|

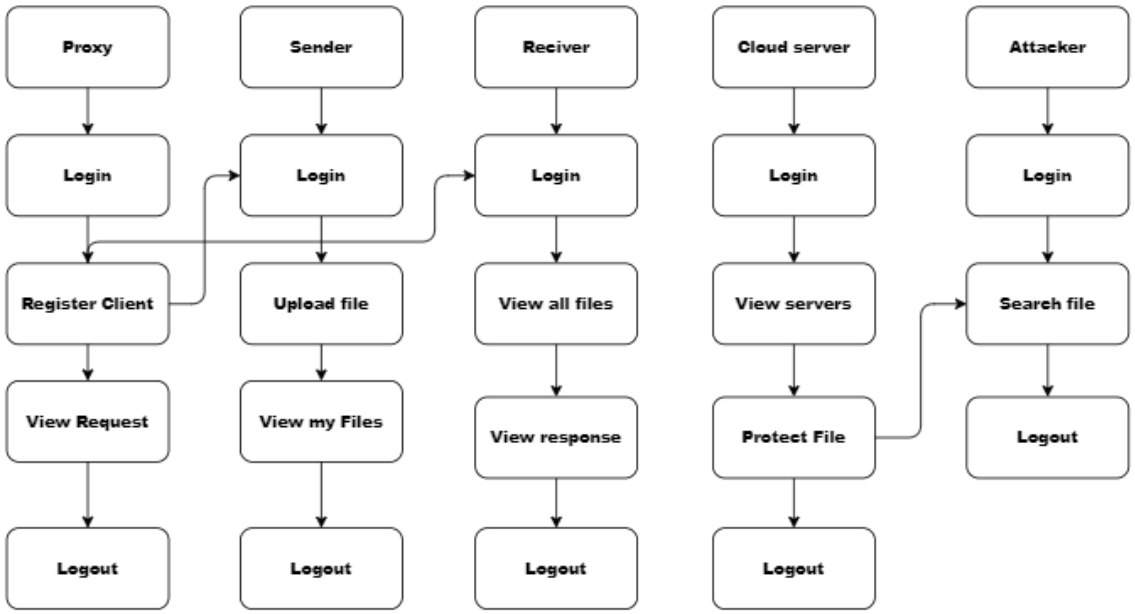
digital photographs has facilitated the transmission of false information, image modification, and deceit thanks to image editing software. The goal of this suggested technique is to correctly spot impersonations and fraud in digital photos. Existing methods concentrate on different aspects of digital image editing such as source, metadata, image cloning, and composition; in contrast, the suggested method is based on physics and involves less human interaction. It picks for areas of the image with comparable intensity and functions with any kind of item in the scene, not just faces. The suggested method determines the angle of incidence in relation to the direction of the light source and identifies modified items by assessing lighting properties. On an image dataset with a variety of altered image kinds, experimental results show a 92% recognition rate.

[3] Oblivious RAM (ORAM) is essential for applications requiring the concealment of access patterns. While many ORAM schemes exist, most are designed to store blocks of fixed sizes. These techniques usually pad variable-length data blocks to the same length prior to uploading, which increases the amount of storage space and network bandwidth used. We propose "DivORAM", which restructures the tree-based ORAM architecture to overcome this limitation and produce the first working ORAM with variable block sizes. It accomplishes this by reducing network capacity by 30% when compared to Ring ORAM and 40% when compared to HIRB ORAM. Under realistic conditions, experimental results show that DivORAM's response time is 10 times faster than Ring ORAM.

III.PROPOSED WORK

In order to improve security at the storage layer in cloud environments, this paper presents Secure Dispersal: An Innovative Approach to Encrypting Cloud Storage. In order to ensure encrypted, fragmented, and distributed storage and impede unwanted access attempts, CSSM integrates both data dispersal and distributed storage techniques. In addition, CSSM uses secret sharing methods and hierarchical administration to reduce the possibility of cryptographic material leaks. This innovative approach, CSSM, enhances data security in cloud storage by dispersing data across multiple locations and controlling access through password authentication and secret sharing. Even in the event of a compromised storage component, CSSM ensures the overall security of the data. In conclusion, CSSM provides a robust defense against data breaches in cloud storage through the implementation of advanced security measures.

PROJECT FLOW



|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

||Volume 13, Issue 3, March 2024||

|DOI:10.15680/IJIRSET.2024.1303217|

3.1 Algorithm Steps

1. **Key Expansion:**
   A key schedule is created by expanding the original key, resulting in several round keys. A certain key schedule algorithm is used to produce each round key from the initial key.
2. **Initial Round:**
   AES divides plaintext into blocks, each of which is typically 128 bits in size. The round key and the plaintext are merged in the first round. Each byte in the block is subjected to an XOR operation with the matching byte of the round key during this process.
3. **Rounds:**
   The number of rounds that the AES algorithm runs through varies depending on the size of the key. It uses 10 rounds for a 128-bit key, 12 rounds for a 192-bit key, and 14 rounds for a 256-bit key, specifically.

Each round comprises four primary steps:
Here are the steps involved in the AES encryption process:

- SubBytes: In this phase, a corresponding byte from a specified S-box (substitution box) is used to replace each byte in the block.
- Shift Columns: In this step, the bytes in each line of the block are consistently moved to one side. The main column stays unaltered, the subsequent line shifts by one byte, the third column by two bytes, and the fourth line by three bytes.
- MixColumns: Every section of the block is treated as a polynomial, and increase modulo a proper polynomial is performed. This step presents dispersion.
- AddRoundKey: At last, every byte of the block is XORed with the relating byte of the round key.

4. **Final Round:**
   During the final round of the AES algorithm, the MixColumns step is excluded. However, the SubBytes, ShiftRows, and AddRoundKey steps are performed as usual.
5. **Output:**
   After the final round, the resulting ciphertext is obtained.To decrypt the ciphertext, the process is reversed using the inverse operations of AES. The round keys are utilized in reverse order.

IV.RESULTS AND DISCUSSION

Result:
The result of our project is to secure the data and protect that by using the AES algorithm, here we are uploading the files by using the AES encryption algorithm, so when we will encrypt the data, it will convert into the cyphertext. If the user wants to decrypt the they need a secrete key, to decrypt the files, so when we will decrypt with AES it will convert cyphertext into the readable format data.
Discussion:
Implementing AES encryption adds a layer of security to sensitive data. By encrypting files before uploading them, you mitigate the risk of unauthorized access during transmission and storage. AES is a widely accepted encryption standard due to its robustness and efficiency. However, it's crucial to manage encryption keys securely. Without the secret key, decryption becomes practically impossible, ensuring data confidentiality. Decrypting files using AES requires the correct key, transforming ciphertext back into its original plaintext form. This process ensures that only authorized users with the appropriate key can access and interpret the data, enhancing overall data protection.

V. CONCLUSION

The paper presents a deep learning approach for Picture Denoising, utilizing Convolutional Neural Network (CNN). The method involves denoising a given image by passing it through a CNN architecture. First, a noisy input image is considered, which needs to be denoised. Noise is added to the original image to simulate real-world conditions. This noisy image is then fed into the CNN network, which is divided into encoder and decoder parts. Through training, the CNN learns to denoise the image by processing it through these layers. Finally, after training, the image is denoised by passing it through the CNN's encoder and decoder layers.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

||Volume 13, Issue 3, March 2024||

|DOI:10.15680/IJIRSET.2024.1303217|

REFERENCES

[1] A. Bhardwaj, F. Al-Turjman, M. Kumar, T. Stephan, and L. Mostarda, ''Capturing-the-invisible (CTI): Behavior-based attacks recognition in IoT-oriented industrial control systems,'' IEEE Access, vol. 8, pp. 104956–104966, 2020.
[2] M. Kumar, A. Rani, and S. Srivastava, ''Image forensics based on lighting estimation,'' Int. J. Image Graph., vol. 19, no. 3, Jul. 2019, Art. no. 1950014.
[3] M. Kumar, S. Srivastava, and N. Uddin, ''Image forensic based on lighting estimation,'' Austral. J. Forensic Sci., vol. 51, no. 3, pp. 243–250, Aug. 2017.
[4] J. Li, Y. Zhang, X. Chen, and Y. Xiang, ''Secure attribute-based data sharing for resource-limited users in cloud computing,'' Comput. Secur., vol. 72, pp. 1–12, Jan. 2018.
[5] Y. Zhang, X. Chen, J. Li, D. S. Wong, H. Li, and I. You, ''Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing,'' Inf. Sci., vol. 379, pp. 42–61, Feb. 2017.
[6] The OpenStack Project. OSSA-2015-006: Unauthorized Delete of Versioned Swift Object. Accessed: Apr. 14, 2015. [Online]. Available: https://security.openstack.org/ossa/OSSA-2015-006.html
[7] The OpenStack Project. OSSA-2015-016: Information Leak Via Swift Tempurls. Accessed: Aug. 26, 2015. [Online]. Available: https://security. openstack.org/ossa/OSSA-2015-016.html
[8] The OpenStack Project. Possible Glance Image Exposure Via Swift. Accessed: Feb. 23, 2015. [Online]. Available: https://wiki. openstack.org/wiki/OSSN/OSSN-0025
[9] Cloud Security Alliance. Top Threats to Cloud Computing: Deep Dive. Accessed: Aug. 8, 2018. [Online]. Available: https://downloads. cloudsecurityalliance.org/assets/research/top-threats/top-threats-to-cloudcomputing-deep-dive.pdf
[10] The OpenStack Project. OpenStack Security Advisories. Accessed: Feb. 2, 2015. [Online]. Available: https://security.openstack.org/ossalist. html
[11] Common Vulnerabilities and Exposures. CVE-2015-5223. Accessed: Jul. 1, 2015. [Online]. Available: https://cve.mitre.org/cgi-bin/cvename. cgi?name=CVE-2015-5223
[12] Common Vulnerabilities and Exposures. CVE-2016-9590. Accessed: Nov. 23, 2016. [Online]. Available: https://cve.mitre.org/cgi-bin/cvename. cgi?name=CVE-2016-9590
[13] S. Y. Shah, B. Paulovicks, and P. Zerfos, ''Data-at-rest security for spark,'' in Proc. IEEE Int. Conf. Big Data (Big Data), Washington DC, USA, Dec. 2016, pp. 1464–1473.
[14] Z. Liu, Y. Huang, J. Li, X. Cheng, and C. Shen, ''DivORAM: Towards a practical oblivious RAM with variable block size,'' Inf. Sci., vol. 447, pp. 1–11, Jun. 2018.
[15] X. Zhang, X. Chen, J. Wang, Z. Zhan, and J. Li, ''Verifiable privacypreserving single-layer perceptron training scheme in cloud computing,'' Soft Comput., vol. 22, no. 23, pp. 7719–7732, Dec. 2018.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details