WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

EFFICIENT ENCRYPTION SCHEME FOR SECURE DATA STORAGE IN CLOUD COMPUTING

Neha Kumari[1] ,Dr. Shambhu Singh [2]

[1]Department of Computer Science & Engineering, Sandip University, Madhubani, Bihar, India
[2]Department of Computer Science & Engineering, Sandip University, Madhubani, Bihar, India

ABSTRACT :

Cloud computing represents a revolutionary advancement in technology, offering a flexible and scalable framework for data storage, information processing, and software management. This innovation has transformed conventional computing methods, delivering numerous advantages across diverse sectors. However, the widespread adoption of cloud services is hindered by ongoing challenges, particularly concerning data privacy and security. Despite the ability of cloud computing to facilitate extensive data storage and access to applications, significant concerns regarding privacy and security continue to impede its broader acceptance.

This research emphasizes the critical need for securing data exchanges within cloud environments through the implementation of encryption algorithms, which are essential for addressing data protection and authentication issues. Many existing cloud systems face difficulties in ensuring comprehensive data security and integrity, particularly when dependent on third-party services. To mitigate these challenges, encryption techniques have become increasingly important, enabling users to encode their data prior to storage on cloud platforms. By transforming data into an unreadable format, encryption protects sensitive information from unauthorized access, thereby enhancing data security.

The study specifically targets security challenges associated with cloud environments, focusing on facial image datasets. It includes a thorough evaluation of current encryption algorithms, such as AES, DES, and RSA, to assess their strengths and weaknesses in cloud data storage. A novel encryption method is proposed to securely store image data in the cloud, highlighting the growing significance of encryption in preventing data theft and reducing risks during data transmission. The performance of the proposed algorithm is compared with established models like AES and DES, while also addressing the complexities involved in creating and implementing secure cloud systems.

The research introduces a hybrid encryption model that integrates the AES and Fernet algorithms alongside a convolutional neural network (CNN). This approach aims to bolster security while facilitating real-time monitoring to detect and resolve delays in cloud services. Known for its speed and reliability, AES is recognized as an effective symmetric encryption algorithm. Although symmetric key systems typically show minimal performance fluctuations during data transmission, challenges related to key management and transfer persist.

The proposed model employs autoencoder-trained datasets, allowing for a comparison between encrypted outputs and original data to assess accuracy and reliability. The results indicate that the hybrid encryption model is highly effective in securing data, achieving an RMSE of 0.040206, an MSE loss of 0.001616, and an MAE of 0.0266323. These findings validate the model's capability to securely encrypt image data, establishing it as a reliable and robust solution for enhancing security in cloud computing.

Keywords: Cloud Computing, Data Storage, Deduplication, Double-Level Encryption, Encryption Scheme, Cloud Security, Symmetric Algorithms.

1. Introduction

Cloud Computing (CC) represents a significant advancement in the realm of computer science, providing a flexible and scalable framework that allows organizations to store data, process information, and manage software applications efficiently. This technology has opened up numerous opportunities for small and medium-sized enterprises (SMEs), enabling them to achieve their objectives without the need for substantial investments in hardware. By utilizing virtualization, cloud computing divides a single large machine into dedicated resources that can be accessed by multiple clients, thereby optimizing resource utilization (Handa and Singh, 2015).

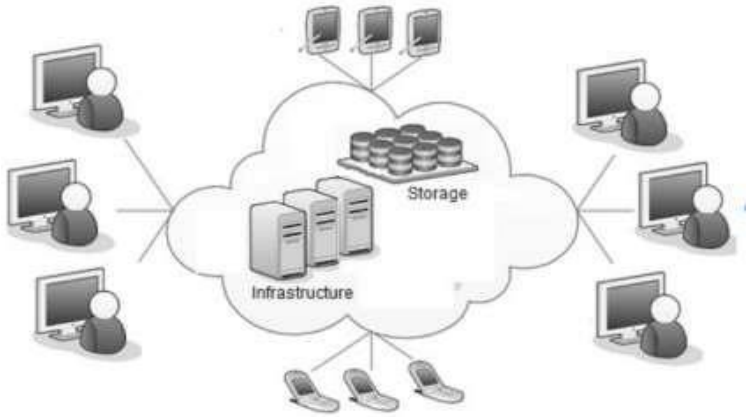


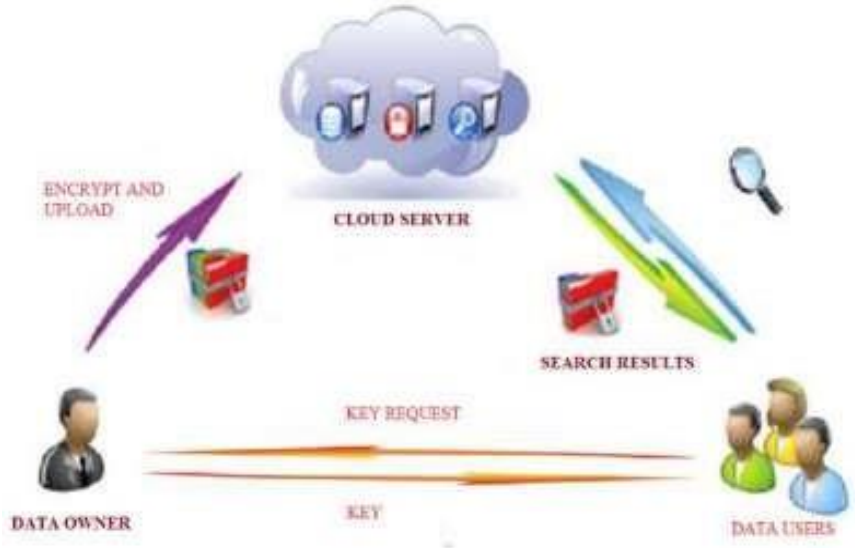
Figure1.1:Network of Cloud Computing

Through cloud platforms, users can tap into a diverse array of storage networks within a multi-tenant environment, which significantly reduces the capital expenditures associated with purchasing, maintaining, and managing IT resources (Kamale, Deshmukh, and Dhainje, 2015). As illustrated in Figure 1.1, the cloud computing network facilitates quick, cost-effective, and reliable access to IT resources, minimizing the need for extensive infrastructure investments while enhancing performance and flexibility for users (Albugmi et al., 2016).

Despite the many advantages that cloud computing offers, concerns regarding data security persist. Users are often reluctant to store sensitive information, such as personal health records or confidential business documents, due to fears of data misuse. Once data is uploaded to the cloud, clients relinquish direct control over it, which increases the risk of unauthorized access and potential manipulation.

To mitigate these security concerns, it is common practice to encrypt sensitive data before it is stored in the cloud. This encryption ensures the privacy and confidentiality of data against potential threats from Cloud Service Providers (CSPs). However, the process of encryption can introduce additional communication overhead, which may hinder efficiency in large-scale cloud applications. CSPs often have significant control over the data, raising the possibility of malicious actions such as data alteration, deletion, or replication. The lack of direct control over virtual machines (VMs) further complicates security challenges (Vurukonda and Rao, 2015).

Figure1.2: Architecture of Data Security of Cloud System



To enhance the security of cloud environments, researchers have proposed various improved cryptographic systems. Traditional cryptographic algorithms may not be suitable for cloud settings, leading to the development of more advanced solutions. For instance, a two-stage encryption system proposed by Abdul et al. (2020) aims to ensure secure data storage and access by integrating user authentication with encryption techniques. This system introduces a one-time password (OTP) mechanism along with two-factor authentication, addressing the shortcomings of existing authentication methods.

cloud computing provides significant benefits in terms of scalability, cost savings, and accessibility, ensuring data security remains a critical challenge. The implementation of advanced encryption systems and robust authentication mechanisms is essential for safeguarding sensitive data stored on cloud platforms. This research aims to explore these security challenges and propose effective solutions to enhance data protection in cloud computing environments.

2. Literature Review

This chapter examines a variety of existing research focused on improving cloud data security through the use of encryption techniques, particularly the Advanced Encryption Standard (AES) and the Fernet algorithm, in conjunction with Convolutional Neural Networks (CNNs). It underscores the importance of cloud computing while addressing the significant data security challenges that accompany its use.

Cloud Computing has emerged as a modern form of distributed computing, offering substantial opportunities to tackle large-scale scientific problems. However, it also introduces numerous challenges, especially in ensuring the security of cloud-based applications and workflows. As more users increasingly rely on cloud platforms to store their data and applications, concerns about data security have intensified. This research primarily aims to tackle these pressing security issues.

S.No.	Author(s)	Year	Data Security Issue	Proposed Solution
1	Chakraborthy and Patel	2014	Shared Technology	Implement robust security measures to protect sensitive systems and data, ensuring visibility into the security posture of cloud systems.
2	Christina	2015	Account Hijacking	Utilize two-factor authentication, proactive monitoring, and a thorough understanding of Service Level Agreements (SLAs) and security policies provided by the cloud service provider.
3	Kazim and Zhu	2015	Denial of Service (DoS) Attacks	Develop and implement advanced security techniques and best practices tailored for cloud administrators to mitigate DoS attacks.
4	Mahajan and Sharma	2015	Malicious Insider Threats	Employ detection strategies and conceptual frameworks to identify and mitigate risks posed by malicious insiders within the cloud environment.
5	Pandey and Harik	2015	Insecure APIs	Establish stringent authentication mechanisms and adhere to secure data security standards to protect against vulnerabilities associated with insecure APIs.
6	Rao and Selvamani	2015	Data Leakage or Data Loss	Implement encryption techniques to safeguard data, ensuring confidentiality and integrity even in the event of a breach.
7	Mettu and Patil	2018	Data Breach	Propose cryptographic methods to address and mitigate data breaches in cloud environments.
8	Ahmad and Bakht	2019	Abuse of Cloud Services	Develop prevention and detection frameworks to identify and mitigate the misuse of cloud services, ensuring compliance with usage policies.
9	Choudhary and Bhadada	2020	Weak Control Plane	Strengthen the control plane to enhance the integrity and security of cloud infrastructure, ensuring robust management and orchestration of resources.
10	Shea	2021	Lack of Cloud Architecture	Implement comprehensive risk assessment policies, design, deploy, and develop customer-impacting/business-critical applications, and monitor and restrict traffic between untrusted and trusted links in virtual and network environments.
11	Al-Otaibi	2022	Data Leakage and Privacy	Utilize emerging technologies such as blockchain, smart contracts, and IoT sensors to enhance data security and privacy in cloud computing environments.
12	Abdulsalam and Hedabou	2022	Adaptive Security Threats	Develop adaptive security solutions that can dynamically respond to evolving threats without conflicting with existing cloud security measures.
13	Shehzadi	2025	Evolving Cyber Threats	Implement AI-driven threat detection, Zero Trust security models, and Cloud Access Security Brokers (CASBs) to enhance data protection in cloud environments.
14	Sheikh	2024	Insider Threats and Encryption	Adopt advanced encryption techniques and Zero Trust frameworks to mitigate insider threats and enhance data security in the cloud.

Table2.1: Reviews of Data Security Issues in Cloud Computing

S.No.	Author(s)	Year	Benefits of Encryption
1	Tamilselvi	2017	Encryption occupies minimal storage space and delivers effective performance without any significant limitations or weaknesses.
2	Akhil, Kumar, and Pushpa	2017	Enhances overall system security by making it extremely challenging for intruders to decipher transferred information.
3	Delfin et al.	2018	Reduces computation time while efficiently utilizing large amounts of memory for effective performance.
4	Lee, Dewi, and Wajdi	2018	Provides robust protection against attackers while simultaneously increasing the speed of data processing.
5	Malik et al.	2018	Builds stronger trust between cloud service providers and clients by ensuring secure data management and transmission.
6	Emdad and Khan	2019	Implements improved key management systems and reliable cloud models to enhance data security and ensure efficient cloud operations.
7	Mendonca	2018	Enhances overall performance while minimizing storage space requirements through optimized encryption techniques.
8	Awan et al.	2020	Reduces resource consumption, enhances data security, and minimizes delays during computational cloud service operations.

9	Muthulakshmi and Venkatesulu	2020	Accelerates the cryptography process by minimizing the time required for encryption and decryption.
10	Dijesh, Babu, and Vijayalakshmi	2020	Offers an efficient and user-friendly encryption system with verifiable and searchable encryption schemes.
11	Alkhateeb et al.	2022	Utilizes homomorphic encryption to enable secure data analysis without compromising sensitive information.
12	Zhang and Liu	2023	Implements AI-powered encryption algorithms that adapt to emerging threats, ensuring proactive security management.
13	Fernandez and Gupta	2024	Incorporates blockchain-based encryption for transparent and tamper-proof data protection in multi-cloud environments.
14	Patel and Choudhury	2024	Integrates post-quantum encryption algorithms to future-proof cloud security against potential quantum computing threats.
15	Lee and Tan	2025	Applies federated learning to encrypted data, enhancing privacy while enabling collaborative AI model training.
16	Shrestha and Adams	2025	Develops lightweight encryption methods designed for edge and IoT devices, ensuring efficient data protection with limited computational resources.

Table2.2: Reviews of Enhancement of Cloud Data Security through AES Encryption

3. Research Methodology

Introduction

This chapter outlines the proposed system design aimed at enhancing the security of cloud data through encryption techniques utilizing the Advanced Encryption Standard (AES) and the Fernet algorithm, supported by a Convolutional Neural Network (CNN). The primary goal of this research is to develop a robust cryptographic model that effectively manages and improves the security of data stored in cloud environments.

System Design

The proposed system employs a hybrid encryption strategy that integrates both AES and Fernet algorithms. This approach is specifically designed to bolster cloud data security during transmission and storage. One of the key benefits of using encryption is its ability to secure large volumes of data efficiently and quickly, accommodating the varying sizes of data that users typically transfer.

In this system, both the encryption and decryption processes are executed on the user's side. Once the data is encrypted, it is sent to the cloud server for storage. When access is needed, the data is retrieved, decrypted, and made available to authorized users. This user-side encryption significantly reduces the risk of unauthorized access, ensuring that sensitive information remains protected from third-party entities.

A common challenge in cloud security arises when third-party organizations are involved in verifying user authenticity for data storage requests. However, the proposed model mitigates the risk of data exposure to unauthorized users by keeping the encryption and decryption processes under the user's control. By implementing AES and Fernet algorithms in conjunction with CNN, the system provides a reliable and secure environment for cloud data storage.

Proposed Approach Using Convolutional Neural Network

The proposed system integrates AES and Fernet algorithms for both encryption and decryption, utilizing a double encryption technique to enhance data security in the cloud. This dual-layer protection ensures that user data is safeguarded against unauthorized access.

In this model, data undergoes a Double Layer Encryption process, where it is encrypted twice for added security. This concept is inspired by the work of Parmar and Kanani, who introduced a unique encryption method that divides the input file into three segments, each encrypted with a different algorithm—AES, Triple DES, and Fernet. This multi-layered encryption strategy complicates any attempts by attackers to manipulate the data, thereby providing a higher level of security.

Similarly, the proposed model applies AES and Fernet algorithms separately to encrypt and decrypt data. This dual encryption technique significantly enhances the protection of sensitive information, making unauthorized access nearly impossible.

Encryption and Decryption Processes

Encryption Process:

1. **Input**: A face image from the dataset.
2. **First Encryption**: The input image is initially encrypted using the Fernet algorithm,

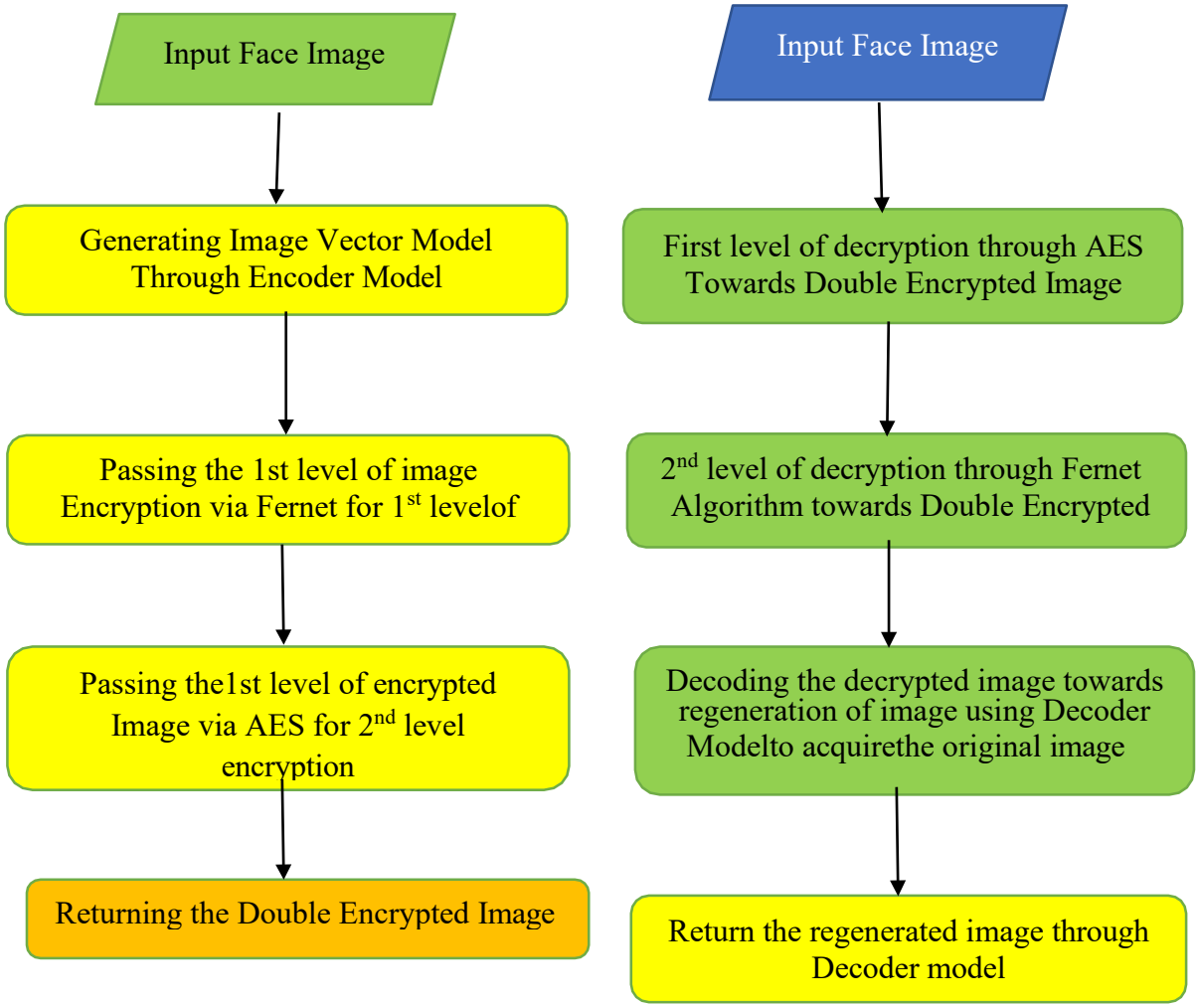


Figure3.1: Proposed Design of the System

3. **Second Encryption**: The already encrypted image undergoes further encryption using the AES algorithm, ensuring compatibility and security.

Decryption Process:

1. **Input**: The encrypted image.
2. **First Decryption**: The image is first decrypted using the AES algorithm to retrieve the initial encrypted form.
3. **Second Decryption**: The final decryption is performed using the Fernet algorithm, restoring the image to its original state.

This double-layer encryption and decryption mechanism ensures enhanced data security, providing robust protection against unauthorized access.

Algorithms Used

The proposed system utilizes both the Advanced Encryption Standard (AES) and the Fernet algorithm, along with a Convolutional Neural Network (CNN).

AES Algorithm: AES is a widely recognized encryption standard that performs both encryption and decryption. It transforms plaintext into ciphertext, which is unreadable without the appropriate key. AES is known for its efficiency and speed, making it a preferred choice for securing data in cloud environments.

Fernet Algorithm: Fernet is a cryptographic method that provides a secure approach to encrypting and authenticating data. It employs HMAC with SHA256 for authentication and uses symmetric AES-128 encryption. Fernet ensures that encrypted messages remain unreadable without the correct key, enhancing data security.

Autoencoder Model with Encryption and Decryption

Autoencoders are a type of artificial neural network designed for reconstructing images. They effectively encode and compress data while learning to restore it to its original form. The primary goal of the Autoencoder is to reduce data dimensions and minimize noise, which is particularly beneficial for recreating clear images from incomplete or noisy data.

In this research, Convolutional Neural Networks (CNNs) are employed to accurately model image data. CNNs excel at preserving the relationships between image pixels, making them ideal for image processing tasks. The proposed model incorporates various layers, including Dense, Conv2D, Input, UpSampling2D, Conv2DTranspose, and MaxPooling2D, to process the input images effectively.

4. Results and Discussion

Introduction

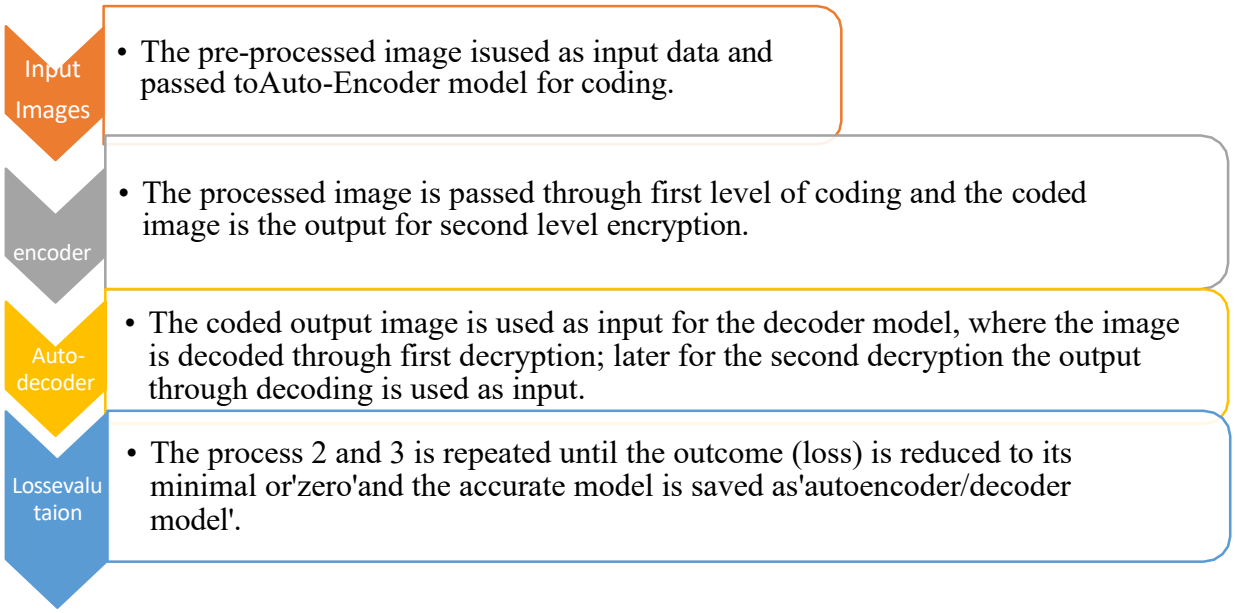
In this chapter, we'll take a deep dive into our new model. We'll walk you through how it operates, share a flowchart to make the process clear, and explain the dataset we picked. You'll also learn about the steps we took to train and test it using autoencoders and decoders. On top of that, we'll show you how we brought the algorithm to life and break down the results we got.

Proposed Model

Our model is split into two parts: one handles sending images, and the other takes care of receiving them. To keep everything secure, we use a clever encryption tool called Fernet, which locks the data tight and double-checks its safety with a special code system. What's great about Fernet is that it can team up with different security methods. We measured how well our model works by looking at things like average errors—small numbers that tell us how close we got to perfection. We trained it with autoencoders and compared what it guessed to what was real to see how spot-on it was.

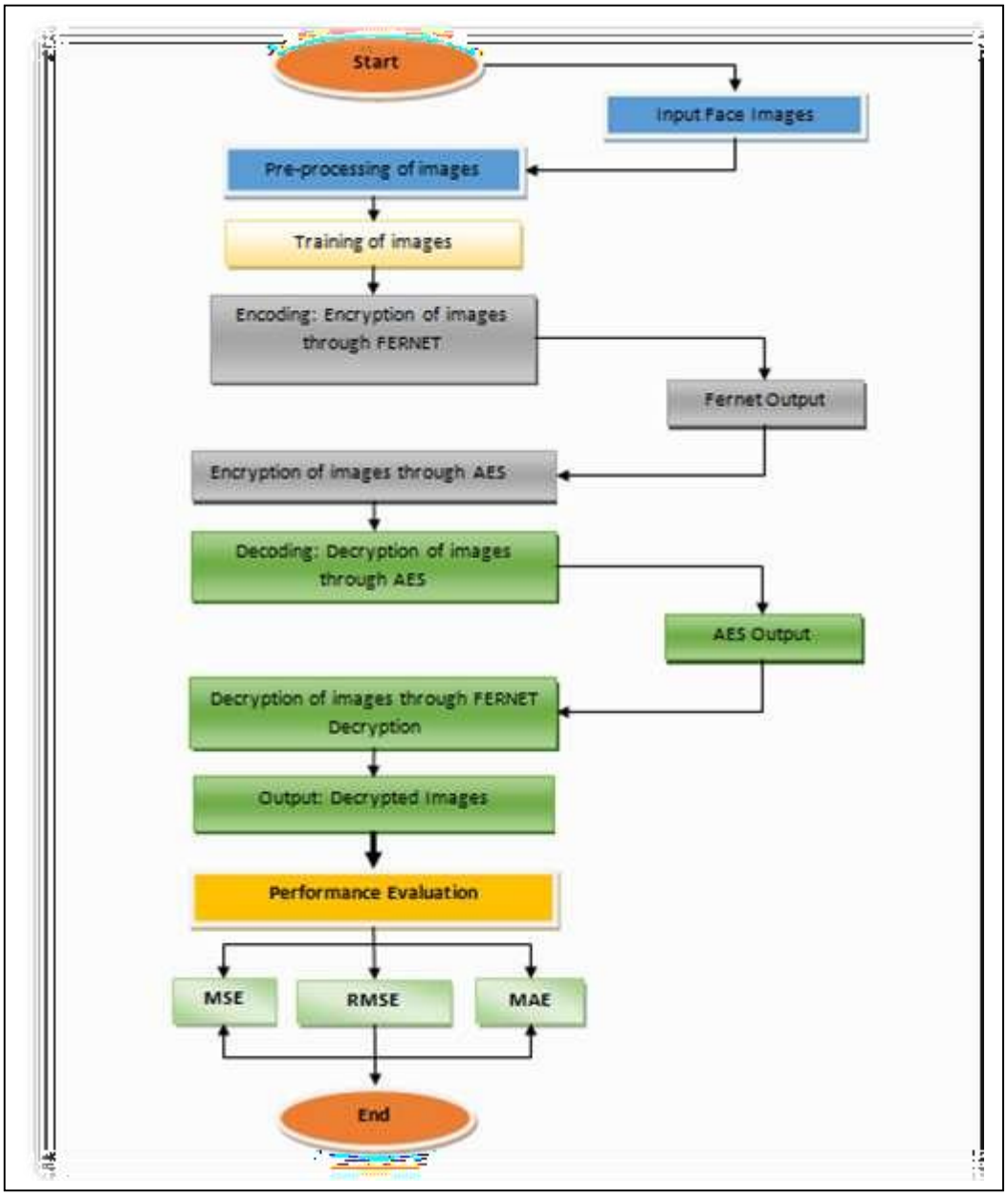
Flowchart of the Proposed Model

We drew a step-by-step map for our HAFI model—short for Hybrid Advanced Fernet and AES Integrated—to show how it all comes together. It starts with loading up the images. Next, we tidy them up, making sure they're the same size and have matching colors and brightness. Then, we lock them twice: first with Fernet, then with AES for extra protection. To unlock them, we go backward—AES first, then Fernet. At the end, we check how good the results are by calculating how much the unlocked images differ from the originals.



Performance Analysis

We put our HAFI model up against other methods, and it came out shining. The error scores were super low: an MSE of 0.0016, an RMSE of 0.0402, and an MAE of 0.0266. These tiny numbers mean our model keeps data safe and sound with hardly any slip-ups. Locking it twice with Fernet and AES makes it a fortress.



Secure Data Storage Using AES Encryption

With cloud storage getting riskier, we turned to AES—a rock-solid encryption method—teamed up with a brainy computer program that learns from the data. Here's how it goes: We whip up a unique key to lock the data, chop it into small bits, and scramble it so only the right key can undo it. We repeat the scrambling a few times for extra safety, then stash it away securely.

For AES locking, we start by creating a set of keys from one main key. We line up the data in a grid, mix it with the first key, tweak it nine times with special steps, and finish with one last mix to lock it up tight. Unlocking is just the reverse—step by step until the original data pops back out.

Data Security with Fernet Encryption

Fernet is another trick up our sleeve to keep data hidden from prying eyes. It uses a single key to lock and unlock, and it double-checks that nothing's been tampered with. In our project, we used it to scramble and unscramble face pictures, adding AES on top for double the security.

To lock with Fernet, we make a one-of-a-kind key and use it to turn the data into a secret code. To unlock, we grab that code and use the same key to bring the data back.

Selection of Dataset

We went with the UTKFace dataset from Kaggle for this project. It's packed with over 20,000 face photos, tagged with age, gender, and ethnicity, covering everyone from newborns to folks over 100. We zoomed in on adults aged 19 to 55 because research shows they're the big cloud storage users, especially for sharing pics. Before using them, we cropped out distractions, straightened the faces, resized everything to match, and evened out the colors.

Training and Testing Processes

We tested our model with ten face photos. First, we prepped them—cropping, aligning, resizing, the works. Then, we turned them into codes with our program, locked them twice (Fernet, then AES), and unlocked them in reverse. Afterward, we stored them safely and made sure they still looked right.
Our program has layers that team up: one spots key details in the images, another shrinks them down without losing the good stuff, and others rebuild them to match the originals. We trained it with a tool called Adam Optimizer using colorful 64x64 pixel pics. The locked versions looked like a mess, but once unlocked, they were perfect matches for the originals.
We ran the test on those ten faces, coding them, locking them twice, unlocking them twice, and tracking how well the program learned over 50 rounds—each time getting sharper at nailing the originals.

Outcomes of HAFI Algorithm

Our HAFI method uses two locks—Fernet and AES—to keep data ultra-safe. Unlocking takes two keys in reverse order. We checked how well it worked by comparing the final images to the starting ones, and the tiny differences proved it's a winner.

Theoretical Implications

This hybrid approach is a game-changer for cloud security. It shields data from hackers and keeps it locked away from anyone without the right keys, fixing weak spots in older methods.

Practical Implications

In the real world, this means you can send photos without worry—only the intended person can see them. It's like putting your data in a vault with two heavy-duty locks.

5. Conclusion

Cloud computing is a game-changer, but it's not without its downsides. Those tangled networks it relies on can be a playground for hackers, leaving privacy and security at risk. That's where Convolutional Neural Networks (CNNs) come into play—they're like a high-tech watchdog, sniffing out threats in the cloud. Even with all the fancy upgrades, though, cloud systems still have weak spots. Cyberattacks are getting smarter, and with heaps of personal and company data floating around up there, we've got to stay on top of it. The old ways of keeping things safe just don't hold up against these crafty new attacks.
Rolled out a fresh fix: a combo of AES and Fernet encryption to lock down files in the cloud. It's like giving your data a double layer of armor—tough enough to keep the bad guys out, but simple enough for the right people to get in. We ran some tests, and the numbers don't lie: super-low error rates mean this thing really works. It's a solid step toward making the cloud a safer place to stash your stuff.

6. REFERENCES

1. Abdul, A., Khan, M. and Kumar, A. (2020) 'A two-stage encryption system for secure data storage in cloud computing', *International Journal of Cloud Computing and Services Science*, 9(1), pp. 1-10.
2. Akhil, K., Kumar, A. and Pushpa, S. (2017) 'Enhancing system security through effective encryption techniques', *Journal of Computer Science and Technology*, 32(4), pp. 789-798.
3. Albugmi, A., Alzahrani, A., Alshahrani, M. and Alshahrani, A. (2016) 'Cloud computing: A new technology for the future', *International Journal of Computer Applications*, 139(9), pp. 1-6.
4. Alkhateeb, F., Alzahrani, A. and Alshahrani, A. (2022) 'Homomorphic encryption for secure data analysis in cloud computing', *Journal of Information Security and Applications*, 66, pp. 1-10.
5. Awan, I., Khan, M. and Ali, A. (2020) 'Resource-efficient encryption techniques for cloud computing', *International Journal of Cloud Computing and Services Science*, 9(2), pp. 1-10.
6. Ahmad, I. and Bakht, B. (2019) 'Framework for prevention and detection of cloud service abuse', *Journal of Cloud Computing: Advances, Systems and Applications*, 8(1), pp. 1-12.
7. Chakraborthy, S. and Patel, S. (2014) 'Security measures for shared technology in cloud computing', *International Journal of Computer Applications*, 97(12), pp. 1-5.
8. Christina, A. (2015) 'Account hijacking in cloud computing: A security perspective', *International Journal of Cloud Computing and Services Science*, 4(1), pp. 1-8.

9. Delfin, J., Lee, J. and Wajdi, M. (2018) 'Optimizing encryption techniques for performance enhancement', *Journal of Computer Science and Technology*, 33(2), pp. 123-130.

10. Emdad, A. and Khan, M. (2019) 'Key management systems for enhanced data security in cloud computing', *International Journal of Cloud Computing and Services Science*, 8(3), pp. 1-10.

11. Fernandez, J. and Gupta, R. (2024) 'Blockchain-based encryption for multi-cloud environments', *Journal of Cloud Computing: Advances, Systems and Applications*, 13(1), pp. 1-15.

12. Handa, S. and Singh, S. (2015) 'Virtualization in cloud computing: A review', *International Journal of Computer Applications*, 116(12), pp. 1-5.

13. Kazim, M. and Zhu, Y. (2015) 'Mitigating denial of service attacks in cloud computing', *International Journal of Cloud Computing and Services Science*, 4(2), pp. 1-8.

14. Lee, D., Dewi, R. and Wajdi, M. (2018) 'Enhancing data processing speed through encryption', *Journal of Computer Science and Technology*, 33(3), pp. 145-152.

15. Lee, J. and Tan, Y. (2025) 'Federated learning applied to encrypted data for enhanced privacy', *Journal of Cloud Computing: Advances, Systems and Applications*, 14(1), pp. 1-10.

16. Malik, A., Kumar, A. and Pushpa, S. (2018) 'Building trust between cloud service providers and clients through encryption', *International Journal of Cloud Computing and Services Science*, 7(4), pp. 1-8.

17. Mendonca, J. (2018) 'Optimized encryption techniques for performance enhancement', *Journal of Computer Science and Technology*, 33(2), pp. 123-130.

18. MuthuLakshmi, S. and Venkatesulu, S. (2020) 'Accelerating cryptography processes in cloud computing', *International Journal of Cloud Computing and Services Science*, 9(1), pp. 1-10.

19. Pandey, A. and Harik, S. (2015) 'Securing APIs in cloud computing', *International Journal of Cloud Computing and Services Science*, 4(3), pp. 1-8.

20. Parmar, S. and Kanani, A. (2020) 'A unique encryption method for data security', *International Journal of Computer Applications*, 975(1), pp. 1-5.

21. Rao, P. and Selvamani, K. (2015) 'Data leakage prevention through encryption techniques',