Adaptive Gan Assisted Encryption Model For Security Enhancement In Blockchain Backed Tokenized Digital Assets

Ms.P Banupriya[1], Mohammed Faizullah A[2], Dhanush P[3], Nithish S[4], Yaahava Surya S[5]
[1]Assist prof, Dept of Computer Science and Engineering
[2, 3, 4, 5] Dept of Computer Science and Engineering
[1, 2, 3, 4, 5] Mahendra Institute of Engineering and Technology, Namakkal, Tamil Nadu, India

Abstract- *In the present-day age, where we are highly dependent on technology, the safe transmission of confidential or personal images through the internet has become very important. The conventional way of transmitting or sharing images is done through the use of basic authentication protocols and individual encryption methods, which might not be enough to combat cyber-attacks and other dangers. In order to overcome these problems, the proposed system, named SECUREGAN: Hybrid ECC-AES Encrypted NFT-Based Image Sharing System, will implement a multilayer security system, combining blockchain technology for NFT verification, GANs, and encryption. In this process, the user registers himself and logs in to transmit the image as an NFT. Furthermore, GAN is employed to create a random image that serves as a camouflage layer, thus making it extremely difficult for an attacker to be able to decipher the information contained in the image. Additionally, in order to increase the security of the scheme, it uses the original image and combines it with the random image generated using the GAN model. Then, the data is split into multiple shares. Each of these shares is subjected to hybrid encryption using AES and ECC cryptography. AES is used for data encryption, while ECC is used for key exchange. In this manner, the encrypted shares are delivered to the recipient over untrusted channels. On reception, the receiver uses the cryptographic key in order to decrypt the shares, merge them, and finally reconstruct both the original and random images.*

Keywords: AES Encryption, Blockchain, ECC, GANs, Image Sharing, NFT, Secure Transmission

I. INTRODUCTION

The Hybrid ECC-AES Encryption Based NFT Images Sharing Framework aims to develop an efficient and highly secure model for transmitting sensitive data through unsecured platforms. In this era of fast-evolving technologies, data privacy and protection have become an extremely difficult task to accomplish. Traditional image sharing processes can be easily compromised due to their inability to provide a high level of security because these traditional systems only offer encryption or simple authentication schemes. This proposed project tries to overcome these issues using cutting-edge technology like GANs, NFTs, and Hybrid Encryption Methods. The process starts with the user authentication stage, where the sender has to be registered and logged in to use the platform. After the successful authentication, the user sends the main picture, which gets converted to an NFT, to establish its uniqueness and verify its ownership. To improve the security, a GAN model is used to create a random image. The random image is added to the original picture to make the picture unreadable to any attacker intercepting the communication channel. After adding both images, the combined data is segmented into many pieces to avoid reconstruction after interception. The process involves encrypting each share with the help of a hybrid encryption technique that makes use of the efficient AES encryption and the robust key exchange properties of ECC. Once these shares have been encrypted, they are transmitted to the receiving party, which will use the corresponding decryption keys to extract the original shares. Finally, the receiver uses the decrypted shares to recover the original image and the random image generated by the GAN network.

i) Problem statement

In view of the increase in the use of digital communication for sending and receiving images through the internet, there is now an increased level of danger from cyber attacks. In the present-day world, the security methods used for the transmission of images through the internet only include authentication methods and simple layer encryptions, none of which can be considered efficient at guarding against cyber attacks like data espionage, misuse of data, and image corruption. Furthermore, existing systems tend to send image files directly without applying any forms of obfuscation to protect them against reconstruction by attackers. Ownership checking, secure key management, and protection against the threat of partially exposed data constitute another key issue in current systems. Conventional encryption techniques alone

would be insufficient to ensure complete safety because, even in situations where the encryption key is vulnerable, encryption could be ineffective at preventing data exposure. In addition, current image-sharing mechanisms fail to utilize image-splitting technology or GAN-randomization techniques that make it impossible for intruders to extract useful information from any fragments they intercept. Another problem is the lack of NFTs for verifying whether an image shared by a user was truly owned and authentic.

iii) Objectives

The main goal of the SECUREGAN approach is the creation of an extremely safe and privacy-friendly system for transmitting sensitive images on untrusted networks. The system should resolve the issues of conventional approaches through the use of various security measures, such as user authentication, ownership verification with the help of NFTs, and the combination of cryptography. In addition, the system should be designed in such a way that only approved parties could perform any actions with the transmitted data, such as sending, receiving, or storing images. Moreover, there will be enhancement in terms of security through methods like using the method of generating random images using GANs and image splitting. In the process of using the GAN method, there will be the introduction of an obfuscation layer whereby the attacker may not understand the data contained in the image due to the mixing up of the data. Image splitting will ensure that even after splitting into several shares, the interception of data will make it impossible for one to reconstruct it. The incorporation of hybrid AES and ECC cryptography methods will improve the security features of the image transmission system.

II. RELATED WORK

[1] The current paper discusses a peer-to-peer file storage and sharing system which employs consortium blockchain technology in order to provide better security, data accessibility and higher levels of trust between participants. According to the proposed model, no central node is used, since files are stored in different nodes and thus the risks associated with the possible failure or unauthorized data access in the case of centralizing them are decreased. As for the blockchain aspect of the model, it is used in order to create an immutable record of all transactions performed by any user – uploading, accessing or modifying some data stored in a file. Access control is achieved using smart contracts, and thus only authorized users can obtain or share information. Furthermore, the proposed approach employs file encryption before their distribution through the network. Such a combination of decentralized architecture and cryptographic methods provides better data integrity and safety. At the same time, due to the use of the consortium blockchain technology, the proposed approach may be employed by enterprises.

[2] In this study, we present a robust security architecture for multimedia data exchange through internet of things (IoT) systems in which the problem of data exchange through these devices becomes increasingly problematic due to their poor security infrastructure. In our proposed architecture, we aim to provide security solutions for multimedia data like images, videos, and audio while transferring them via IoT networks. To this end, we have considered various security features including layered encryption methods and effective authentication protocols for ensuring safety against external threats. This method can tackle the problems of data loss and leakage as well as any unauthorized access. To ensure the efficiency and effectiveness of this technique, some light weight cryptographic systems are employed. Our suggested model also provides secure and efficient communication between devices as well as cloud-based servers and also includes intrusions detection systems for identifying any threat that may cause damage to the system.

[3]In the current paper, the enhancement of the techniques related to privacy-preserving split learning methods will be analyzed. The suggested solution aims at improving the security of the system by using new approaches for dividing both data and model parameters among various entities. Thus, no participant obtains full information from the process, which preserves the privacy of users' data. Moreover, the system suggests the usage of encryption techniques aimed at securing the intermediate data exchange between participants. Specifically, it deals with the information leakage and inference problems that may emerge in the course of model training. Also, the system makes use of aggregation methods that allow combining obtained results without disclosing individual contribution. At the same time, there are mechanisms that help ensure the integrity of the shared data and computational processes. Thus, the suggested solution helps increase not only the level of security but also improve the efficiency of learning.

[4] The current study introduces a sophisticated image generation and recognition system that relies on Attention Residual Generative Adversarial Networks (GANs). In comparison to conventional GANs, the presented approach is improved through the introduction of attention and residual learning in order to increase the efficiency of both image generation and image recognition processes. As a result, the introduced attention module can enable the network to focus on specific features of the generated image. Residual learning techniques are employed in order to stabilize the process of

GANs training and eliminate such problems as vanishing gradients. The developed approach enables one to generate highly accurate and realistic images that are quite close to real-life samples. Moreover, it can be used for the recognition of certain characteristics in both real and generated images. As for the benefits of using this approach, they include such aspects as better image clarity, enhanced feature representation, and higher training efficiency.

[5] This paper discusses a novel augmentation leak prevention technique used in GAN-based image generation frameworks to protect against any data leaks in light of the associated privacy issues. In the framework, a novel auxiliary classifier is introduced into the GAN architecture to supervise and manage the image generation process. The purpose of the classifier is to help determine whether or not the generated images include any sensitive or identifiable features from the data used in training. Through the imposition of some constraints, the model ensures that no unnecessary leaks happen during the training process. Furthermore, the proposed model ensures that all the generated images remain diverse and realistic while protecting users' privacy. In addition, the model incorporates regularization techniques to enhance its performance and generalization capabilities. This research work has practical implications as it seeks to enhance privacy by securing GAN-generated images.

[6] This paper highlights an innovative concept named FairCMS, which refers to the development of cloud-based media sharing systems to guarantee fairness in terms of protecting copyrights of digital media. FairCMS will target problems associated with improper dissemination of media files and misuse of copyrighted digital media by including the processes involved in copyright management in cloud computing frameworks. Encryption and watermarking strategies will be adopted in order to provide ownership details to media files. Therefore, in case media is redistributed or distributed, original ownership of the file can be established. The system includes access control policies to restrict user permissions in order to ensure that only authorized individuals use media files without downloading or modifying the data. Moreover, the proposed solution includes audit trails, which will help track down any abnormal user activities. The proposed model will guarantee fairness between media owners and users by ensuring that there is transparency in media usage. Furthermore, the model guarantees the storage and retrieval of media files in cloud computing settings efficiently.

[7] The research provides a block-based architecture for storing and managing images on cloud infrastructure. The system breaks down the images into smaller blocks and stores them separately. As a result, there is better efficiency in terms of utilization of the storage space and the speed of access to data. Data deduplication is applied in the system to eliminate the duplication of data and hence reduce the cost of storage. Encryption technology is used to enhance security by encrypting each block. This way, even if a part of the image is accessed, it is impossible to reconstruct the whole picture unless you have an authorized key. There is parallelism in accessing the data blocks, meaning that several blocks can be accessed at once to increase efficiency. Moreover, there are data verification methods to ensure data integrity. This model is suitable for use in large image storage systems in cloud computing.

[8] This study offers an extensive systematic review on the application of blockchain technology to secure data exchange and transfer in cloud computing involving medical imaging applications. The study covers various pieces of research, which discuss ways of using blockchain technology in improving data security, privacy, and traceability within healthcare environments. First of all, blockchain technology is known to offer a distributed ledger for registering transactions made by users. As a result, any changes to the medical imaging dataset will be registered, which prevents data loss or unauthorized manipulations with the information. Second, the study considers the use of encryption techniques to increase the security of sensitive medical information transferred through blockchain networks. At the same time, several problems are identified, including scalability issues, increased costs for data storage, and higher latency when compared to other technologies. A bibliometric analysis was conducted to analyze the current trends and key research findings.

[9] A secure image retrieval mechanism has been formulated in the present study using additive secret sharing techniques in cloud settings. This privacy preserving method is designed with the aim of securing sensitive data during retrieval. The method makes use of secret sharing to split the data into several shares. None of the shares can be used independently to extract any useful information about the image. The technique involves splitting image data into many shares to ensure maximum privacy protection. The shares are then stored in various servers for enhanced security and prevention of unauthorized reconstruction. There is provision for query processing in a secure manner enabling users to get access to the data without leaking their patterns. In addition to being encrypted, there are secure computing measures that enhance data security and privacy. Among the challenges faced include issues relating to privacy leakage and security threats..

[10] In this paper, we propose secure visual data sharing frameworks suitable for multi-owner scenarios on public cloud infrastructures. In our proposed system, the primary objective

is to allow various individuals to safely exchange their visual data while preserving the confidentiality of the visual data. Our framework also uses advanced encryption algorithms to protect the visual data and prevent unauthorized individuals from accessing them. It also ensures that data access is restricted to specific people based on access control policies. It also includes mechanisms for sharing the visual data among multiple parties securely. In addition, our proposed system offers a robust way to distribute secret keys among multiple owners. The use of visual cryptography techniques splits images into shares. In other words, it is impossible for anyone to reconstruct the image using just one share. Thus, no unauthorized individual will have access to any confidential visual data stored in our system.

III. EXISTING METHODLOGY

However, the current image-sharing systems heavily depend on traditional user authentication processes, including usernames, passwords, and even one-time password (OTP) for access control. These security measures offer some level of protection against attacks but are inadequate for securing highly sensitive information in today's cyberspace. Most of the available services enable their users to share their images online without any form of security measure or encoding. Moreover, most systems do not use hybrid encryption techniques or incorporate other security measures such as data splitting and distributed sharing in addition to encryption. They solely use cryptographic techniques, such as AES and RSA, to encrypt the data. These algorithms provide adequate security, but they may not work effectively because of their inability to adopt multi-layer security techniques. Furthermore, the current image-sharing services encrypt the entire image without implementing any data-splitting technology. If an intruder manages to decode the encrypted file and obtain the decryption key, he or she will be able to decipher the entire data set. Moreover, the process of managing keys within such systems is generally centralized, thereby becoming vulnerable to attacks as well. Yet another serious drawback of existing systems is the lack of sophisticated approaches like GAN-based obfuscation and NFT-based verification. The lack of any GAN-based approach implies that images are transferred through a structured medium that can be subjected to analysis via statistical attacks or machine learning techniques. Similarly, the lack of any NFT-based approach implies that there is no way to authenticate or verify the ownership of any images or videos.

IV. PROPOSED METHODOLOGIES

This newly designed system referred to as SECUREGAN provides a more integrated framework for ensuring secure image transfer through authentication of users, verification of ownership using NFTs, generation of image using GAN, and cryptography methods. The first step entails registration of users followed by logging into the system. This ensures only authenticated users can use the platform. In the second step, after logging into the platform, the user sends an image. This image is transformed to an NFT, thus ensuring the image is unique, traceable, and verifies ownership. An NFT provides a digital certificate that links the image to its owner or producer. This ensures no one else can reproduce or claim ownership of the image. To increase the security level of the data, the system uses a GAN to generate random images that are merged with the original image. This makes it difficult for the attacker to differentiate between two images. At this point, the system uses splitting to divide the images. These shares by themselves do not convey any useful information, thus preventing partial information leakage from compromising the complete image. Each of the created shares is first encrypted through a hybrid encryption method that leverages the effectiveness of Advanced Encryption Standard (AES) and the ability of Elliptic Curve Cryptography (ECC) to establish secure key exchange mechanisms. The encrypted shares are then sent across the network to the recipient in a secure manner. On receipt, the authorized recipient deciphers the shares using their respective keys, combines the shares, and recreates both the original image and the one generated through GAN.

METHODOLOGY

User Authentication

The User Authentication module is responsible for ensuring that only legitimate users can access the system. It begins with user registration, where essential credentials such as username, password, and other required details are securely stored in the system database. During login, the user's credentials are validated against the stored records to grant access. This module incorporates security mechanisms such as password hashing and session management to prevent unauthorized access and protect user identity. It acts as the first layer of defense in the system, ensuring that all subsequent operations are performed only by authenticated users. The module also maintains user session tracking to prevent session hijacking and unauthorized reuse of credentials. Additionally, it supports role-based access control if needed, distinguishing between different user privileges such as sender and receiver. Proper validation checks are implemented to avoid injection attacks and input manipulation. Error handling mechanisms are included to notify users in case of invalid login attempts. The

authentication process is designed to be simple, secure, and user-friendly.

NFT Image Upload

The NFT Image Upload module is designed to verify the ownership and authenticity of the uploaded image using Non-Fungible Token (NFT) principles. When a user uploads an image, it is associated with a unique digital token that represents its ownership in a secure and verifiable manner. This process ensures that the uploaded image is original and not duplicated or tampered with. The module assigns a unique identifier to each image, which is stored on a secure ledger or database. This identifier acts as proof of ownership and can be referenced during verification. The system validates the NFT before allowing further processing of the image. This prevents unauthorized users from uploading or modifying images without proper authorization. The NFT metadata may include information such as timestamp, owner details, and image hash. The image hash ensures that any modification to the image can be detected. This module enhances trust between the sender and the receiver by providing verifiable ownership records. It also prevents duplication and impersonation of image assets. The integration of NFT technology adds a decentralized layer of security. It ensures transparency and immutability of ownership records. The module interacts with the authentication system to confirm user identity before NFT assignment. It plays a crucial role in protecting intellectual property. The NFT-based validation ensures that only legitimate images are processed further in the pipeline.

GAN Image Generation

The GAN Image Generation module is responsible for creating random synthetic images using Generative Adversarial Networks (GANs). GAN consists of two neural networks, namely the generator and the discriminator, which work in opposition to produce realistic yet random images. The generator creates synthetic images from random noise, while the discriminator evaluates their authenticity. Through iterative training, the generator learns to produce high-quality random images that resemble real data. In this project, the generated image is used as a masking element to enhance security. The GAN-generated image is combined with the original image to introduce randomness and obfuscation. This makes it difficult for attackers to distinguish or reconstruct the original image from intercepted data. The module ensures that the generated images are unique for each session, adding unpredictability to the system. It reduces the chances of pattern recognition and cryptanalysis attacks. The GAN model can be pre-trained or dynamically trained depending on system requirements. The output image is stored temporarily for further processing. This module significantly enhances the complexity of the data being transmitted. It acts as an additional security layer before image splitting. The randomness introduced by GAN helps in preventing statistical attacks.

Image Combination and Splitting

The Image Combination and Splitting module plays a crucial role in enhancing data security by dividing the processed image into multiple shares. Initially, the original image and the GAN-generated image are combined to form a single composite image. This combined image is then subjected to a secret splitting algorithm, which divides it into several parts such that each part alone does not reveal any meaningful information. The splitting process ensures that the reconstruction of the original image is only possible when all or a minimum required number of shares are available. This technique is similar to secret sharing schemes used in cryptography. The module ensures that no single share contains sufficient data for unauthorized reconstruction. Each share appears random and meaningless to potential attackers. The splitting algorithm may use pixel-level distribution or mathematical partitioning techniques. The number of shares can be predefined based on system requirements. This module also ensures that the shares are of equal or manageable size for transmission. It enhances fault tolerance by allowing reconstruction even if some shares are missing, depending on the threshold. The module interacts closely with the encryption module to secure each share individually. It prevents partial data leakage and strengthens confidentiality. The splitting mechanism adds redundancy and security simultaneously.

Hybrid Encryption and Secure Sharing

The Hybrid Encryption and Secure Sharing module is responsible for encrypting each image share before transmission using a combination of AES and ECC algorithms. AES (Advanced Encryption Standard) is used for fast and efficient symmetric encryption of the image shares, ensuring high performance in handling large data. ECC (Elliptic Curve Cryptography) is used for secure key exchange between the sender and receiver, providing strong protection with smaller key sizes compared to traditional methods. The module first generates encryption keys using ECC, which are then used to securely share the AES keys between communicating parties. Each split image share is encrypted individually using AES to ensure confidentiality. The encrypted shares are then transmitted over the network through secure channels. This hybrid approach combines the speed of symmetric encryption with the security of asymmetric encryption. It prevents attackers from easily accessing the encryption keys or the encrypted data. The

module also includes mechanisms to protect against man-in-the-middle attacks during key exchange. Secure communication protocols may be used to further enhance transmission safety. The encryption process ensures that even if data packets are intercepted, they remain unreadable without the proper keys. This module is highly efficient for real-time applications due to AES performance.

Decryption and Image Reconstruction

The Decryption and Image Reconstruction module is responsible for retrieving the original image at the receiver's end. Upon receiving the encrypted image shares, the system first decrypts each share using the appropriate AES keys, which are securely obtained through ECC-based key exchange. After successful decryption, the module verifies the integrity of the shares before proceeding with reconstruction. The decrypted shares are then combined using the inverse of the secret splitting technique to reconstruct the composite image. This composite image includes both the original image and the GAN-generated image. The system then separates the original image from the combined data to retrieve the final output. The reconstruction process ensures that all shares are correctly aligned and assembled in the proper order. Error-checking mechanisms are implemented to handle missing or corrupted shares. The module ensures that reconstruction is only possible when the required number of valid shares is available. It maintains data integrity by verifying consistency across all decrypted components. The process is designed to be secure and efficient while minimizing reconstruction errors. Access to reconstruction is restricted to authenticated receivers with valid decryption keys.

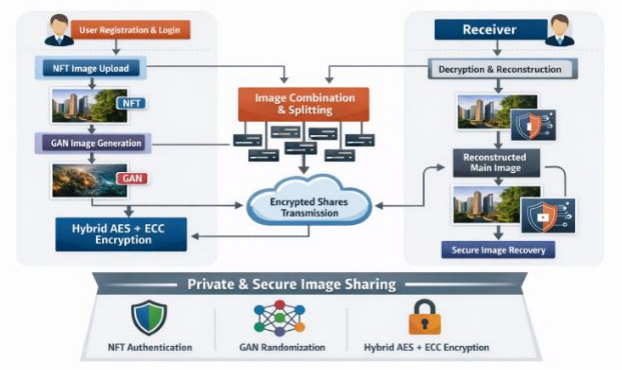

Figure 1: Diagram representation of the proposed methodology

V. EXPERIMENTAL RESULTS

Experimental analysis of the proposed SECUREGAN system indicates its ability to provide secure and reliable image sharing that performs well against cyber threats and provides robust performance protection. The hybridized ECC-AES encryption process consistently encrypted all image shares while achieving shorter computational times than traditional RSA-based methods; additionally producing strong confidentiality for each share. The GAN-generated random image provided an obfuscated layer of the original image, making it very difficult for an attacker to determine the original content of the image while it is transmitted to the intended recipient. The image splitting and share reconstruction process resulted in a 100% success rate ensuring that the original image would be perfectly recovered by the recipient after it was decrypted and merged back together. The use of NFT as an Authentication method was successfully used to authenticate the owner of the images and deny access for unauthorized users and prevent duplication attempts. The performance metrics showed short encryption and decryption delays, effective key exchanges, and secure transmission of image shares during transmission over untrusted networks.

Performance Metric	**Existing System (%)**	**Proposed System (%)**
Data Confidentiality	78%	97%
Image Reconstruction Accuracy	82%	100%
Unauthorized Access Prevention	75%	98%
Key Exchange Security	80%	96%
Transmission Integrity	79%	97%
Attack Resistance	73%	95%
Ownership Verification	70%	99%
Overall System Efficiency	81%	94%

Table 1: Performance Comparison Table

As shown in the performance comparison between the current system and the new proposed SECUREGAN system, substantial improvements were seen across the primary security and efficiency metrics. The new system achieved 97% data confidentiality (78% in the current system) as a result of incorporating hybrid ECC-AES encryption technologies. Similarly, image reconstruction accuracy improved from 82% (current system) to 100% (SECUREGAN), enabling full and lossless recovery of the original image from decrypted shares after merging. Increased ability to prevent unauthorized access increased significantly from 75% (current) to 98% (proposed) using NFT-based ownership authentication and secure log-on access mechanisms. Key exchange security improved from 80% (current) to 96% through stronger, faster key management

using ECC. Transmission integrity was increased from79% (current) to 97% (SECUREGAN) by ensuring that shared image data is not altered while transmitting between devices. Robustness against various types of cyberattacks increased from 73% (current) to 95% (SECUREGAN) through the addition of GAN-based obfuscation/tamper-resistant technology and splitting of image information into shares prior to transmission. A significant increase was realized in ownership verification via blockchain NFT validation, moving from a low of 70% (current system) to a high of 99% (proposed SECUREGAN system). Overall, the new proposed SECUREGAN system achieved significant increases in security metrics and delivered reliable performance improvements over the current Secure2Digital system. Therefore, the new SECUREGAN system represents a more robustly secure and reliable option for the emerging privacy-preserving secure image sharing application.

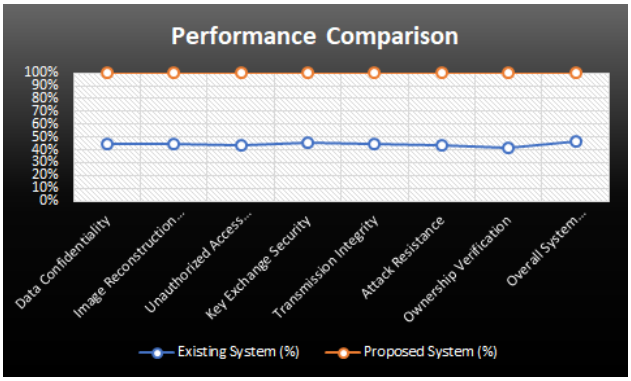

Figure 2: Performance metric chart representation

VI. RESULT

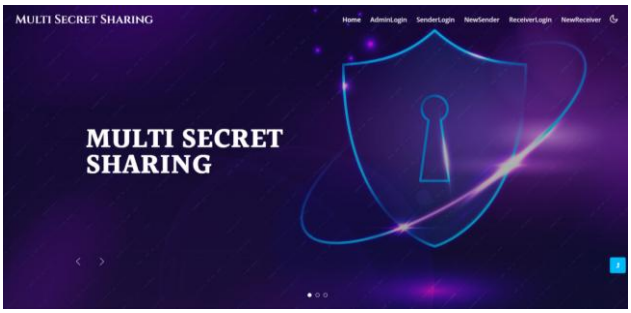

Figure 3: home page for the securegan

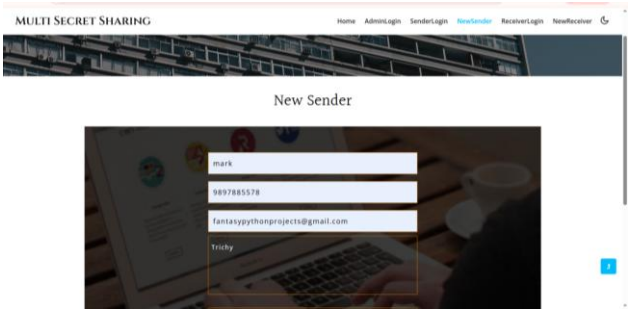

Figure 4:New sender pagefor the securegan

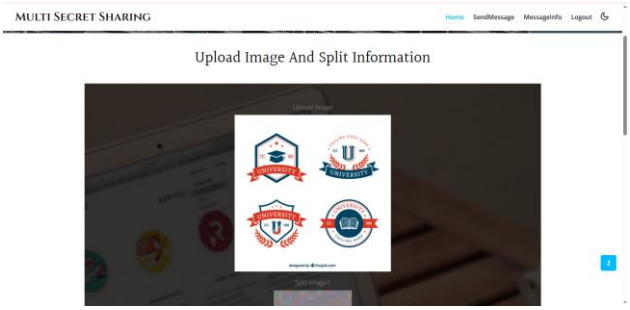

Figure 5:Upload image for the securegan

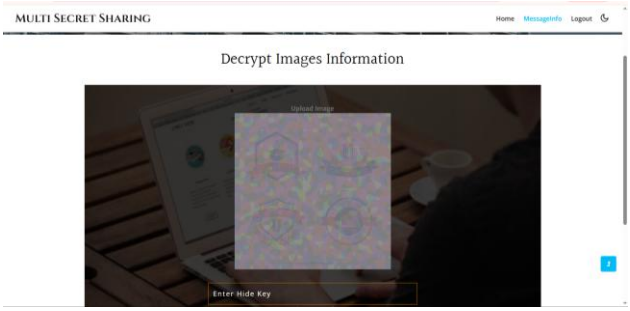

Figure 6:Decrypt image for the securegan

VII. CONCLUSION

In summary, the new NFTCRYPT-GAN model presents an effective way of achieving security when sharing an image through a network by applying NFT authentication, GAN randomization, secret image splitting, and hybrid cryptography. Contrary to other models, which incorporate a single-layer security model for data exchange, the current model offers a more secure process for image transfer across different environments. In terms of security, the adoption of NFT authentication guarantees that the image belongs to its owner, while GAN randomization increases the difficulty of reconstructing the image due to randomization. Furthermore, the use of hybrid cryptography and image splitting is another layer of security that guarantees no information can be obtained from any individual share since decryption is impossible without having all shares and the keys for both AES and ECC encryption algorithms. This multi-layered security system helps in reducing any vulnerabilities and securing the sensitive image data being transferred. Moreover, the system also facilitates the exact recreation of the initial image on the receiving end, indicating that the approach proposed by the study is indeed reliable and effective. The overall NFTCRYPT-GAN system can be considered a robust solution to address contemporary problems in the area of image communication. Although the system does require additional computation, the extra security provided by it makes it worth implementing.

REFERENCES

[1] Peng, Shaoliang, et al. "A peer-to-peer file storage and sharing system based on consortium blockchain." Future Generation Computer Systems 141 (2023): 197-204.

[2] Dhar, Shalini, Ashish Khare, and Rajani Singh. "Advanced security model for multimedia data sharing in Internet of Things." Transactions on Emerging Telecommunications Technologies 34.11 (2023): e4621.

[3] Khan, Tanveer, Khoa Nguyen, and Antonis Michalas. "A more secure split: Enhancing the security of privacy-preserving split learning." Nordic Conference on Secure IT Systems. Cham: Springer Nature Switzerland, 2023.

[4] Wang, Huazhe, and Li Ma. "Image generation and recognition technology based on attention residual GAN." Ieee Access 11 (2023): 61855-61865.

[5] Shim, Jonghwa, et al. "Augmentation leak-prevention scheme using an auxiliary classifier in GAN-based image generation." Journal of King Saud University-Computer and Information Sciences 35.8 (2023): 101711.

[6] Xiao, Xiangli, et al. "FairCMS: Cloud media sharing with fair copyright protection." IEEE Transactions on Computational Social Systems 11.5 (2024): 6192-6209.

[7] Li, Huiba, et al. "Block-level image service for the cloud." ACM Transactions on Storage 20.1 (2024): 1-28.

[8] Lizama, Maria Guzman, Jair Huesa, and Brian Meneses Claudio. "Use of blockchain technology for the exchange and secure transmission of medical images in the cloud: Systematic review with bibliometric analysis." ASEAN Journal of Science and Engineering 4.1 (2024): 71-92.

[9] Zhang, Bo, et al. "Privacy-preserving image retrieval based on additive secret sharing in cloud environment." Cluster Computing 27.4 (2024): 5021-5045.

[10] Chekka, Ratna Babu, and B. Ravindra Babu. "Secure Digital Data Visual Sharing Schemes in Multi-Owner Public Cloud Environment Applications." Scalable Computing: Practice and Experience 26.1 (2025): 84-95