Educational Administration: Theory and Practice
2024,30(4), 2958-2972
ISSN:2148-2403
https://kuey.net/

Research Article

Deep Steg Block: Deep Learning-Enhanced Steganography for Secure Communication in IoT Devices Using Blockchain

V.Raja[1*], K.S. Suresh[2]

[1*]Department of Computer Science and Applications SRM Institute of Science and Technology, Vadapalani, Chennai, Tamil Nadu 600026. rajav@srmist.edu.in
[2]Assistant Professor, Department of Computer Science, Rajeswari Vedachalam Government Arts College, Chengalpattu- 603 001. ksampathsuresh@gmail.com

Citation: V.Raja, et al. (2024), Deep Steg Block: Deep Learning-Enhanced Steganography For Secure Communication In Iot Devices Using Blockchain, *Educational Administration: Theory and Practice*, *30*(4), 2958-2972,
Doi: 10.53555/kuey.v30i4.1963

ARTICLE INFO

ABSTRACT

DeepStegBlock introduces a cutting-edge framework that combines deep learning-enhanced steganography with blockchain technology for secure and imperceptible communication between Internet of Things devices. DeepStegBlock provides safe and undetectable encrypted message transfer between Internet of Things devices by fusing blockchain technology with deep learning-enhanced steganography. In a time when worries about security lapses and data privacy are on the rise, DeepStegBlock appears to be a powerful remedy that has the potential to completely transform the Internet of Things. DeepStegBlock's clever use of Convolutional Neural Networks allows it to discreetly send sensitive data via Internet of Things networks by hiding encrypted messages inside multimedia content. Combining steganographic methods with CNNs ensures undetectable embedding while maximizing computing capacity, which helps to overcome the limitations imposed by IoT devices. This research leverages the power of Convolutional Neural Networks for the intelligent embedding of encrypted messages into multimedia content, which is then securely transmitted across IoT networks. The incorporation of blockchain ensures immutable recording of data exchanges, providing a dual layer of security through both steganographic techniques and blockchain's ledger system. The framework is specifically designed to address the challenges of limited computational resources in IoT devices, employing lightweight CNN models for efficient real-time processing. DeepStegBlock offers a novel solution for enhancing data privacy and security in the rapidly expanding IoT ecosystem, ensuring that sensitive information remains protected against unauthorized access and tampering. Python is used to implement the suggested system. The suggested system accomplishes blockchain transaction durations of 7 minutes and processing times of 2.5 seconds.

Keywords: Block Chain; Convolutional Neural Network; Deep Learning; Internet of Things; Security.

1. Introduction

The term "Internet of Things" describes the idea of wired or wirelessly linked items and gadgets of all kinds connecting to the Internet. The Internet of Things, or IoT, is becoming more and more popular as a result of its many applications in corporate growth, training, transportation, and interactions. Internet of Things refers to the concept of a global network of individually accessible, networked items that use sensing characteristics, communication protocols, processing power, and data analysis capabilities. The fundamental idea behind the Internet of Things is that anything connected to it is capable of a multitude of tasks, including detecting, recognizing, and processing data. This allows the object to communicate with an extensive range of different devices and services over the Internet, therefore delivering services to mankind [1]. The idea of hyperconnectivity emerged because of IoT, allowing for easy communication between individuals and businesses even in faraway regions. An enormous number of "Things"—uniquely recognizable physical items with sensing, communication, and actuation capabilities—are connected over the Internet to form the Internet

of Things. As of right now, there are 5 billion smart things online, and by 2020, that number is predicted to reach 25 billion. It is difficult to integrate "Things" onto the Internet since they could have limitations on their memory, processing power, and energy usage. The majority of items were first created as closed, proprietary solutions that weren't compatible with other manufacturers' hardware. Yet, the current tendency is toward compatible and standardized procedures. Applications for IoT are multiplying. Smart cities, smart homes, infrastructure, intelligent farming and raising animals, industrial control, smart water, intelligent transport, environment surveillance, protection and crises, and more are all included. These Internet of Things apps manage private data about individuals and businesses, which shouldn't be shared with hackers or other unapproved parties[2] .

The quantity and competence of vulnerabilities versus IoT systems are increasing as the area of IoT develops. There are several areas into which IoT application domains may be divided, such as utilities, manufacturing and industry, supply chain and transportation, environmental and agriculture, health, and personal homes. A new movement called "Industry 4.0" is bringing big data, cloud computing, virtualization, IoT, cyber-physical systems, cloud computing, and the semantic web to the industrial sector [3]. Large service providers, companies, and sectors including healthcare, self-driving cars, energy management, digital farming, and many more have taken notice of the Internet of Things concept. Being a component of the industry 4.0 revolution, the Internet of Things will likely become more widely used by the end of 2020, allowing items to hear, listen, communicate, and act intelligently. The goal of attacks on IoT systems is to either steal confidential information, introduce fake information, or interfere with regular network and service operations. Attacks in the recent past have targeted weaknesses in medical equipment, smart automobiles, and intelligent refrigerators. Certain attacks carry a significant danger; for instance, compromising medical equipment might result in fatalities. Thus, it's crucial to defend vital IoT systems from hostile assaults and malfunctions to ensure their security. Information security generally addresses confidentiality, integrity, and accessibility. According to Schneier, attacks on reliability and accessibility in the Internet of Things are more significant than those on secrecy [4].
Infrequent usage, forgetting to update devices, and using outdated passwords have increased cybersecurity risks and allowed unauthorized programs to access private information on IoT networks. Such inadequate security protocols increase the risk of various hazards, including data leaks. The overwhelming majority of security professionals think that IoT is an ideal target for hackers because of its loose security regulations and processes. Security protocols are not well documented, even though a number of security processes have been developed to protect Internet of Things equipment from cyberattacks. Therefore, end users were unable to stop data thefts before they happened. Since the year 2008, hackers have created many types of malwares that target Internet of Things devices. They created a variety of phishing tactics to coerce workers or individuals into disclosing private information [5]. As a result, prominent hacks frequently result in breaches of privacy on both personal and business workstations. Device makers and security specialists can create an effective defensive mechanism to stop or eliminate cyberattacks if they appropriately identify the dangers. IoT-enabled gadgets have been employed for a variety of commercial and industrial uses. These companies are able to get a competitive advantage over their rivals due to the applications. However, because of the widespread use of smart devices that share and integrate data, most organizations are now very concerned about privacy and data breaches since they can disrupt work processes, operations, and network connectivity. To address these threat concerns, create thorough security policies and procedures, safeguard company assets, and guarantee service stability and continuity, experts are required. For instance, Internet of Things (IoT)-)-enabled smart kitchen gadgets that are linked to the neighbourhood network may be a point of compromise where hackers can get sensitive personal or corporate data, as well as modify and disrupt business operations [6].

New technologies are developed daily, while those that already exist undergo modifications. Take the most recent developments in 5G technology, for instance. It is anticipated that 5G will be crucial to Internet of Things applications and systems. However, because of the short wavelength, the infrastructure must alter, necessitating the installation of additional base station networks to cover the same region as previous wireless technologies. There are other dangers with this new arrangement, such as phony base stations. It is crucial to comprehend the security threats and possible fixes. However, because of the decentralized characteristics of IoT topologies and the resource constraints of IoT devices, traditional security measures frequently do not apply in the Internet of Things. Blockchain is a technique that is gaining a lot of interest right now and is potentially useful for IoT security [7]. Blockchain technology appears to be a potential method for protecting IoT and safeguarding user and data privacy because to its decentralized design, data permanence, and non-repudiation services. Steganography is a method for concealing secret data such that it cannot be discovered within a common, open file or message. Once it reaches its destination, the private data is subsequently retrieved. The method of concealing data within an image file is known as image steganography. The picture chosen for this use is known as the cover image, and the image that is produced following steganography is known as the stego image. Steganography and encryption together provide further data concealment and security. With little modifications to look, a full-sized color image (referred to as the Cover image) is hidden inside another image utilizing DCNN. The generated picture will then be combined with a "reveal" network to expose the concealed image. The least significant bits of the pictures are manipulated in some of the most

popular steganographic techniques to insert confidential data. This can be done uniformly or adaptively using basic replacement or more sophisticated techniques. Convolutional neural networks will be used in the research to conceal one picture inside another. The benefit is a more effective steganography [8].

When information is valued and must be kept secret, a working concept known as steganography is created. Its fundamental component is the subtly hidden information. Steganography is known to have been used historically and via a variety of techniques. As new prospects and technological advancements arise, steganography research is likewise moving in this way. Similarly, as the potential applications of blockchain technology become clearer, it becomes apparent that steganography may be utilized in conjunction with blockchain. Blockchain's distributed design [9], anonymity, and information protection have made it an attractive topic for steganography research. DeepStegBlock is a novel architecture that enables safe and undetectable communication between Internet of Things devices by fusing blockchain technology with deep learning-enhanced steganography. The framework effectively integrates encrypted messages into audiovisual information by utilizing lightweight Convolutional Neural Networks. This allows for fast real-time processing while overcoming the computing constraints of Internet of Things devices. Through the integration of blockchain technology, DeepStegBlock adds security layer by ensuring that data transactions are permanently recorded, protecting confidential information from alteration and illegal access. This creative solution gives an innovative way of secure communication in restricted resource contexts, improving data privacy and security inside the quickly growing IoT ecosystem.

The following is the proposed work's primary contribution:

- DeepStegBlock is a pioneer in the combination of blockchain technology and deep learning-enhanced steganography, providing a singular approach to secure Internet of Things communication.
- By utilizing lightweight CNN models, the framework effectively processes data in real-time while addressing the computational limitations of Internet of Things devices, all while maintaining privacy.
- Through effortlessly integrating encrypted communications into multimedia content, DeepStegBlock assures invisible transmission while protecting confidential data from unwanted access.
- The framework provides an additional layer of safety by utilizing blockchain technology, which enhances data protection by utilizing steganographic methods alongside blockchain's immutable ledger system.
- DeepStegBlock offers a unique method for improving data safety and confidentiality in the growing IoT environment by protecting private data against manipulation and eavesdropping.

The paper is laid out as follows. An introduction is given in Section 1. A related paper that compares present methods is provided in Section 2. Section 3 discusses the limits of the current system. The design and execution of the suggested DeepStegBlock are described in Section 4. Section 5 presents the results and comments. The summary and future application are given in Section 6.

2. Literature Review

Robert’s edge detection approach was presented alongside the Stego-chain method, which was put out by Sarkar et al. [10]. Conventional depict steganography encrypts the cover image with secret data and sends the resultant stego image across an unsecured channel to the designated recipient. The stego and cover pictures appear to be identical, making it difficult for the invaders to discern between them when they attempt to feel the channel. The reliability of the Stego picture, however, is the main worry since it might be intercepted by an adversary to impede covert communication. They have developed a blockchain-based system called "Stego-chain" to solve this problem. It makes use of an effective steganographic approach based on expanded Robert's edge detection. Expanding the edge area will enhance the embedding payload, which is the goal of the preceding approach. The generated stego picture is then broadcast among valid nodes in the form of frame segments after being encrypted using a shared secret key. The receiver takes the altered free frames, uses the secret key that was exchanged to rebuild the stego image, and then performs an extraction process to retrieve the secret data. The method by which additional nodes within the blockchain verify and log transactions, as well as the dependability rationale and incentive they suggest, have not been sufficiently detailed in technical terms. The study's blockchain is not well represented in the data tables and pictures that were provided.

Mohsin et al., [11] states that in hospital communication channels, safe updating and exchange of enormous quantities of medical data effectively and safely are crucial but difficult tasks. Two difficulties specifically come up when tackling the aforementioned challenges: network failure that might raise questions about data availability and the security and reliability of their health data. This paper suggests and analyses a new blockchain technique in the geographical domain that is based on steganography. The insertion and subtraction of additional particles from the particle swarm optimization (PSO) algorithm is the innovation of the suggested approach. Furthermore, hash functions with large embedding capacities and excellent image quality can conceal private clinical COVID-19 data within healthcare databases. Additionally, blockchain technology and stego photos with hash data are utilized for updating and exchanging medical COVID-19 data throughout

participating hospitals across the network to enhance privacy and safeguard the quality of healthcare COVID-19 data in grayscale pictures, guarantee data availability in the event of a network connection failure at a single point, and remove the network's central point—a third party—during transmission. Three steps of the suggested technique are covered. Initially, each host image's embedding ability is estimated during the pre-hiding step. Secondly, the PSO algorithm-associated hash function is used in the covert COVID-19 data concealment step. Finally, all network nodes (health centers) are updated during the transmission step, which uses blockchain technology to send the stego pictures.

Xu et al., [12] recommended blockchain in steganography. Using traditional steganography, covert data is embedded into an innocent object, such as a picture or video. An unsafe channel will be used to deliver the final stego object to the intended recipient. The channel monitors can intercept and modify items to disrupt covert communication even if he is unable to discern between ordinary objects and those carrying concealed information. Since a hacker is unable to interfere with Blockchain data after a block is generated—that is, a receiver is perpetually able to completely extract the private information with the secret key—it motivates us to propose new steganography to solve the aforementioned issue. In the proposed technique, the miner plays the role of the steganographer, inserting confidential information into operations within a block as the block is being generated. To safeguard the process of embedding data within a block, they select a subset of transactions based on a secret key and incorporate the secret data using a repeatable address configuration. The investigation shows that extracting the encoded data is a challenging task for an attacker. The data embedding procedure won't raise red flags since the miner gathers regular transactions to create a block rather than creating anomalous transactions, delivering an elevated level of protection.

Ruohan et al., [13] proposed a Cycle GAN for secure communication in IoT. The danger of data theft and leakage in the Internet of Things (IoT) is steadily rising due to its widespread use and data transfer via public communication channels. As a result, one of the main issues with information security nowadays is IoT security. One of the most important techniques for addressing the issues of covert communication and personal privacy exposure is steganography. This study adapts to the concealed interaction and privacy preservation of the Internet of Things by proposing a novel steganography method utilizing image-to-image translation by integrating steganography and steganalysis modules into Cycle GAN. To enhance the stego image's anti-detection capabilities, a steganalysis network is employed. Furthermore, the integrity of the produced illustration may be ensured by cycle consistency in Cycle GAN. The stego picture can partially withstand steganalysis by monitors thanks to the suggested method. The technique is modified to address IoT communication security issues and enable covert terminal-to-terminal communication. The limitations involve the possibility of picture quality degradation, the inability to conceal information completely, the dependence on electronic media for integration, and the vulnerability to complex steganalysis tools. Furthermore, resilience against detection might differ according to how advanced the monitoring systems are.

Alhaddad et al., [8] proposed an Audio Steganography for Securing 5G-Enabled Internet of Things. Numerous Internet of Things (IoT) applications are centred around Voice over IP (VoIP) and need to protect information collected by prospective listeners and attackers. Examples of these applications include self-driving cars, drone delivery, online commerce, IoT smart cities, e-healthcare, and robotic-assisted surgery. One well-known method that uses audio steganography to ensure security is the covert transmission of confidential data between the devices. An effective, dependable, and low-latency technique for securely sending sensitive data via wireless networks is audio steganography. The data rate of MPEG-1 Audio Layer 3 is within the permissible audio quality threshold. Its sound quality is unaffected by its low degree of noise distortion, making it an excellent carrier medium for watermarking and steganography. Every embedding technique's undetectability criteria is what gives it effectiveness. The accuracy of hidden data detection is inaccurate, even though several detection techniques exist that include steganography and watermarking. Whether variable bit rates or an unvarying sample rate for embedding facilitate identification has not yet been verified. As the compression rate rises or falls, the accuracy of finding buried details within MP3 files decreases. The increase in bit rate, sampling rate, or file track size is what's causing this dip or rise. Text message identification and embedding in MP3 files were done using training data. Several iterations were assessed. Decreased detection accuracy with different compression rates, possible deterioration of embedded information with shifting rates of bits or size of the file, and dependence on certain encoding settings are some of the constraints of audio steganography while protecting IoT via MP3 files. The efficacy of the procedure could fluctuate depending on the embedding technique used, and changing detection algorithms and compression standards might have an impact on detection accuracy.

Subramanian et al.,[14] recommended a deep convolutional autoencoder for image steganography. Using picture steganography, a secret image may be covertly hidden inside a cover image. Traditionally, the cover picture is statistically altered to incorporate the hidden binary bits once the secret data has been translated into binary bits. If the cover picture is overloaded, it might deform and reveal hidden information. As a result, the old approaches' ability to conceal information is restricted. This work proposes a deep convolutional autoencoder framework that is lightweight and straightforward, and that can be used to both extract the hidden secret picture from the stego image and embed it within a cover image. Effectiveness is measured using peak

signal-to-noise ratio, concealing capability, and concealment outcomes on the test set. The experimental findings show that compared to previous deep-learning picture steganography techniques, the suggested method performs better in terms of concealment, protection and resilience, and concealing capacity. Through the use of human auditory redundancy, audio steganography seeks to conceal a hidden message from prying ears by embedding it into cover sounds. Recent research, however, has demonstrated that by removing high-dimensional characteristics from stego audio for categorization, the audio steganography now in use may be readily revealed using deep learning-based steganalysis. The current GAN-based steganography techniques have mostly been researched for picture covers; less research has been done on audio covers. Furthermore, even with the limited number of GAN-based audio steganography techniques that have been put out, there is still an opportunity for enhancements in terms of undetectability and perceptive qualities. This proposal in this study is an audio steganography system that can be trained to automatically produce high-quality steganographic overlay audio enabling message embedding. The proposed architecture has three distinct components for training: a generator, a discriminator, and a trained deep learning-based steganalysis. The secret message is then embedded within the steganographic-covered audio using the conventional message embedding technique, LSBM, to create stego audio. This is then sent to the developed steganalysis for incorrectly identifying as cover audio. After these three parties have finished their adversarial training, a well-trained generator may be obtained, which can provide steganographic covering audio for later message embedding. Using a conventional steganography technique, the secret message is embedded within the steganographic covering audio to create the stego audio in the implementation of the suggested approach. According to experimental results, the suggested audio steganography might generate steganographic cover audio for message embedding that maintains essentially good perception integrity.

Khari et al.,[15] proposed Securing data in Internet of Things using cryptography and steganography technique. The domain of Internet of Things is one in which data is transferred instantaneously. Although protecting sensitive data is a difficult endeavor, security risks can be reduced by using steganography and cryptography approaches. When it comes to user verification and data protection, these methods are essential. The protocol for elliptic Galois cryptography is presented and analyzed in the proposed work. This protocol encrypts private information obtained from several medical sources using a cryptography approach. Subsequently, a low complexity picture is embedded with the encrypted data using the matrix XOR encoding the steganography approach. The suggested method additionally optimizes the picking of cover blocks inside the image using an algorithm known as Adaptive Firefly. A number of parameters are assessed and contrasted with the current methods in light of the findings. Ultimately, the information concealed inside the picture is extracted and subsequently decoded. The use of digital media during embedding, the possible loss of data integrity while encryption and embedding, the restricted ability to conceal data inside pictures, and the vulnerability to complex steganalysis and cryptanalysis tools are some of the constraints. Furthermore, considering the expertise of the offenders and the surveillance systems, resilience against discovery may differ. Zheng et al., [16] suggested a key as secret message for steganography. The proposal, Keys as Secret Messages (KASM), is a completely novel blockchain-based steganography plan that might be pre-calculated by both parties with certain confidential parameters pre-negotiated before covert communication. This will improve the effectiveness of the stegosystem upon blockchain and equilibrium the time utilized by Encode and Decode operations. They design the stegosystem with proven security under selected hidden text attack and implement key generation of codebook item by using random number generators and elliptic curve features. Through testing on the Bitcoin protocol and contrasting Keys as Secret Messages against Blockchain Covert Channel, they find that the suggested stegosystem may decode stegotexts in a very acceptable amount of time and can encode hidden texts quicker than Blockchain Covert Channel. Because Keys as Secret Messages encode and decode processes take equal amounts of time, they may be used in duplex communication scenarios. Senders' digital currency can be safeguarded since Keys as Secret Messages do not divulge the sender's private keys. Keys as Secret Messages has some limitations, including the use of pre-negotiated secret parameters that might lead to security flaws if hacked. Furthermore, even though Keys as Secret Messages provides quicker encoding and decoding than Blockchain Covert Channel, the computational demands associated with key derivation and codebook production may still influence its efficiency. Its dependence on generators of pseudorandom numbers and elliptic curves further adds intricacy and possible challenges to its execution.

The study of the literature offers insights into a range of steganography approaches, with a special emphasis on how they are applied in diverse areas, including picture and audio communications, blockchain, and the Internet of Things. Several novel approaches are shown, such as deep learning architectures-based picture and audio steganography methods and blockchain-based steganography methods like Stego-chain and Keys as Secret Messages. These techniques seek to improve data security and secrecy across a range of communication channels, from medical data transfer via IoT networks to blockchain transactions. The assessment also emphasizes how crucial it is to combine steganography and cryptography methods to reach better degrees of safeguarding information. But each method has its limits, even with steganography's improvements. For instance, although a key as a secret message provides quicker encoding and decoding, there may be weaknesses due to its dependence on pre-negotiated secret parameters. Similar difficulties may arise for audio

steganography techniques in ensuring undetectability and excellent perceptual quality, particularly in the presence of deep learning-based steganalysis. Overall, even if these methods seem to be promising in resolving security issues, more investigation is required to get past their shortcomings and guarantee effective safeguarding of sensitive data across a range of communication circumstances

3. Problem Statement

The security and effectiveness of current steganography techniques for Internet of Things communication are frequently compromised. The increasing security risks that IoT devices confront, such as data interception and manipulation, may not be sufficiently addressed by conventional methods. Moreover, the processing constraints of Internet of Things devices limit the viability of employing intricate steganographic techniques. Furthermore, it is still difficult to guarantee the confidentiality and integrity of data that is sent, especially in decentralized Internet of Things networks with little central supervision. Furthermore, the inability to withstand sophisticated assaults and the lack of an impenetrable record of data transfers highlight the necessity for enhanced safeguards[17]. The suggested initiative, DeepStegBlock, seeks to overcome these restrictions by utilizing blockchain technology and deep learning-enhanced steganography. By cleverly encrypting messages and seamlessly integrating them into audiovisual material, deep learning algorithms provide increased security while maintaining undetectable communication. Blockchain technology ensures the security and integrity of information by offering a secure record for documenting data transfers. Deep Steg Block provides a unique way to improve the security and confidentiality of information in IoT communication by merging these technologies, making sure that private data is covered from manipulation and unauthorized access.

4. Secure IoT Communication with Deep Steg Block

Using blockchain technology and deep learning-enhanced steganography, the Deep Steg Block technique incorporates crucial phases to allow secure communication in IoT devices. First, to find appropriate deep learning models as well as blockchain frameworks that can be efficiently utilized within the resource restrictions of IoT devices, a thorough examination of the needs and limitations of IoT devices is carried out. Message is encrypted using AES. Subsequently, convolutional neural networks—a deep learning technique—are used to intelligently insert encrypted messages throughout multimedia content, providing undetectable communication. Considering the restricted computing resources of IoT devices, these CNN models have been adjusted and tuned to perform well on them. Furthermore, the framework incorporates blockchain technology to provide an impenetrable ledger for documenting data transfers amongst IoT devices, guaranteeing data confidentiality and integrity. By automating and enforcing data-sharing rules, smart contracts improve communication security and dependability. Moreover, the suggested technique comprises thorough testing and assessment to determine DeepStegBlock's security and performance. This entails testing the viability of the suggested architecture in safely transferring sensitive data across IoT devices while maintaining data integrity and privacy in both simulated and real-world settings. Furthermore, possible weaknesses and restrictions are found and fixed by utilizing ongoing methodological improvement and optimization.

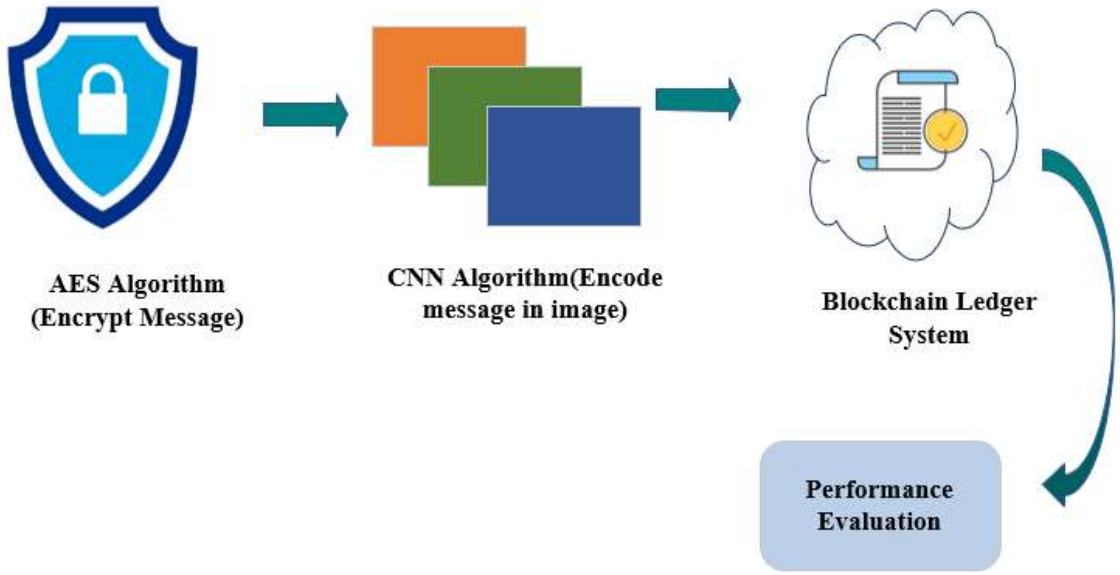

Fig 1: Proposed Architecture of Deep Steg Block

4.1 AES Algorithm for Encrypted Message

The Advanced Encryption Standard technique is used in the proposed Deep Steg Block architecture to encrypt messages before their embedding into multimedia content. Symmetric encryption technology AES is widely recognized for its strong security and effectiveness. Depending on the required level of security, determining an appropriate key size—typically 128, 192, or 256 bits—is the first step in the encryption process. The AES algorithm then divides the plain-text message, which might be any data to be delivered securely, into blocks of a defined size. Every block is subjected to a sequence of encryption rounds, during which the algorithm utilizes a key schedule to produce a distinct round key. The first-round key is XORed with the plaintext block during encryption. This is followed by a sequence of mixing, substitution, and permutation operations called Add Round Key, Mix Columns, Shift Rows, and Sub Bytes, respectively. The key size determines how many times these processes are done. The operations are repeated several times. Without the matching decryption key, the resultant ciphertext block is an altered version of the plaintext block that cannot be understood. Through the creation of ciphertext that is impervious to cryptanalysis, the AES encryption procedure guarantees the message's secrecy. To enable safe and undetectable interaction among IoT devices inside the blockchain-enabled framework, steganography techniques are used to embed the AES-encrypted message in multimedia content within the Deep Steg Block framework.

4.2 Convolutional Neural Network Enhanced Steganography

CNN processes the encrypted message in the suggested Deep Steg Block architecture before it is embedded into the image. To keep the encrypted message undetectable, it must first be formatted to work alongside the CNN input layer and then embedded into the image. The encrypted message initially goes through a procedure in the recommended Deep Steg Block architecture to make sure it is compatible with the CNN model [18], which is used to incorporate images. The encrypted message must be transformed into a format that can be integrated with CNN's input layer throughout this procedure. When ready, CNN embeds the encrypted message into the multimedia material using its embedding technique. The encrypted message must be transformed into a CNN model-compatible format before it can be included in multimedia content. To do this, the message is usually encoded into numerical or category values that the CNN can understand. To prepare AES-encrypted messages for embedding into CNNs in the Deep Steg Block architecture, the binary sequence of encrypted data must be transformed into a format that can be integrated with multimedia information. The AES encrypted message is first normalized (a binary sequence of bits) to make sure it is consistent and compatible with the embedding procedure. In order to comply with the CNN model's input specifications, the binary sequence's length must be modified in this normalization phase. The encrypted message is then normalized and structured into an embeddable structure. Depending on the needs and input size of the CNN model, this can comprise splitting the binary sequence across smaller blocks or frames. The message that has been encrypted is ready to be embedded into the image in each of its blocks or frames. To make incorporation with the CNN model easier, the preprocessing stage may also involve encoding the encrypted message. Fig 2 depicts the working of CNN in steganography.

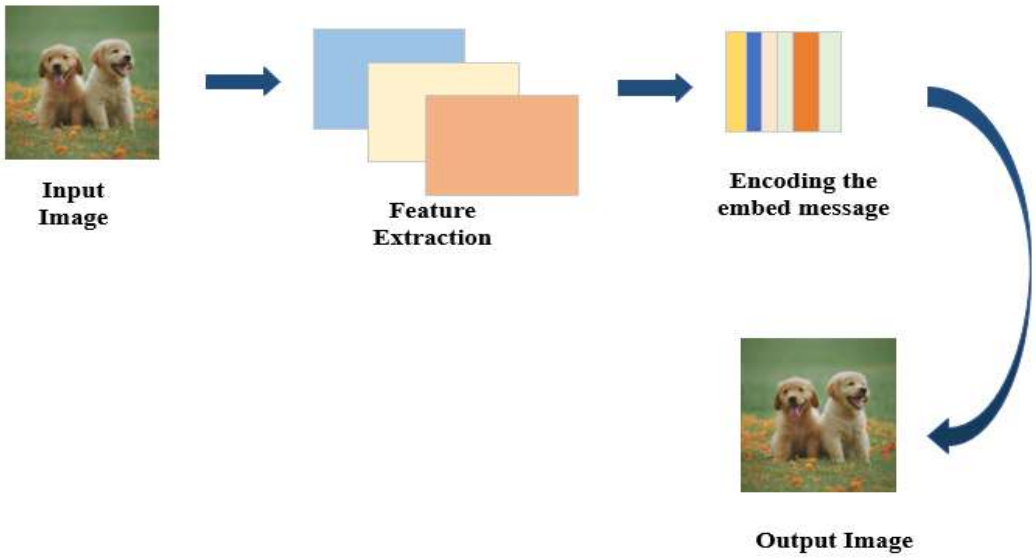

Fig 2: CNN Architecture for Steganography

By using this encoding, the message that is encrypted is ensured to be encoded in a way that the CNN model can process it efficiently when it is embedded. One popular method is to use methods like one-hot encoding as well as tokenization to translate the encrypted message's characters into numerical representations. For

instance, the secret message "HELLO" is subjected to one-hot encoding in the suggested Deep Steg Block structure, which turns each letter into a binary vector depending on a predetermined vocabulary. The complete encrypted message is represented by one input vector that is created by concatenating these binary vectors. A CNN processes this vector after which it embeds the message into audiovisual material while maintaining its original look. Ensuring safe communication across IoT networks, the embedded content conceals the encrypted message while remaining undetectable to human observers. The CNN model utilizes its embedding method to conceal the encrypted message inside the image after it has been created and encrypted. While maintaining the multimedia content's initial perception, CNN effectively embeds the encoded message using its layers and parameters. The embedding process can be represented mathematically as follows in eqn. (1). Let I represent the pre-processed image and M represent the encoded message vector. The embedding process can be formulated as:

$$E = CNN\_Embed(I, M) \quad (1)$$

Where, E is the embedded image produced by the CNN. The function CNN_Embed represents the embedding mechanism of the CNN, which integrates the encoded message vector M into the feature maps extracted from the image I. One of the most important steps in employing CNNs to analyse and comprehend multimedia information is feature extraction. Feature extraction is an important step in getting images, for embedding secure messages in the proposed Deep Steg Block architecture while maintaining its original look. The pre-processed image is input into the CNN's first layers during feature extraction. These layers, also called convolutional layers, are in charge of identifying and removing low-level characteristics from the input data. Basic visual patterns including borders, textures, colours, and forms are examples of these low-level elements. To create feature maps, the convolutional layers convolve the input data using several filters or kernels. Convolution procedures, which include element-wise multiplying the filter weights using the input data and then summarising the results, are how each filter finds certain patterns inside the input data. These convolutional layers let the pre-processed multimedia information to flow through filters that identify different low-level characteristics in the content. For instance, filters may recognize forms by recognizing contours or outlines, textures by capturing recurring patterns, and edges by emphasizing sudden changes in pixel intensity. Convolutional layers produce a collection of feature maps that show whether particular low-level characteristics are present in various areas of an image or not. As a more advanced depiction of the input data, these feature maps capture crucial visual attributes required for further processing stages, such as the encoding of encrypted messages. Feature extraction makes it possible for CNN to learn useful representations of the processed by extracting pertinent low-level characteristics. This makes it easier to incorporate encrypted messages while preserving the original look of the content. Ensuring the imperceptibility of the embedded messages to human observers is a crucial procedure that improves the security and secrecy of communication inside the Deep Steg Block framework.

After feature extraction, the next step in the Deep Steg Block framework is encoding integration, where the encoded message vector is seamlessly integrated into the feature maps extracted from the pre-processed image. This integration process involves modifying specific elements of the feature maps to encode the message information effectively. These modifications are carefully controlled to ensure that the embedded message remains imperceptible to human observers while preserving the visual quality and integrity of the multimedia content. Following encoding integration, the modified feature maps, now containing the embedded message information, are passed through deeper layers of the CNN for deep embedding. In this phase, the CNN further processes the feature maps to abstract and combine the embedded message with higher-level features extracted from the multimedia content. These deeper layers of the CNN are responsible for learning complex representations of the multimedia content, capturing intricate visual patterns, semantic information, and context. Deep embedding ensures that the embedded message stays concealed inside the audio visual material while retaining its original look by deeply integrating it with the structure of representation that CNN has learned. This procedure improves the security and secrecy of interactions within the DeepStegBlock architecture by utilizing the hierarchical structure of CNNs to embed the message's contents in a way that is difficult for outside observers to detect. The last instance of embedded image is created by CNN's output layer, and it now includes the encrypted message concealed within its characteristics. Human viewers cannot detect this embedded image since the CNN's adjustments have been meticulously crafted to ensure that they have the least possible visual impact.

4.3 Blockchain Ledger System for Secure IoT Communication

Blockchain technology, which is based on the Bitcoin cryptosystem, has become a significant technological innovation that can help manage, control, and protect the system without the need for outside intervention. Every node in the blockchain network has a copy of a block, and they are all connected in a mesh topology. A block is made up of the nonce, current hash, previous hash, and Merkle root in addition to the total amount of valid transactions. The node has the capacity for transmission to the network and establishes a transaction that integrates with a digital signature. The network then extracts and verifies the transactions. The details that

make up a blockchain's block structure are as follows, Current hash is the current block's hash value. Previous hashes are the hash of the most recent block that was added. Timestamp: The block's current generation time stamps. Nonce the computation-related number. Data are the block-specific information. Merkle root is a collection of valid transactions from a block, and the hash values of each transaction are computed to create a root hash that resembles a tree. The ledger of a blockchain is a distributed information system that is kept up to date by a group of computers working together. It employs encryption to make sure that every transaction is safe and cannot be changed in the past without the network's approval. The transactions, timestamp, and cryptographic hash of the preceding block are all included in each block that makes up the ledger. In the proposed DeepStegBlock framework, the process of blockchain transaction and transmission plays a crucial role in ensuring the secure and immutable transfer of multimedia content embedded with encrypted messages over the IoT network. Firstly, after the image is embedded with the encrypted message using steganography techniques and CNNs, a transaction is created. This transaction includes the embedded multimedia content along with additional metadata such as timestamps and encryption key. The timestamp indicates the exact time when the transaction occurs, providing a chronological record of data exchanges. The encryption key is also included to ensure that only authorized parties with the corresponding decryption key can access the embedded message.

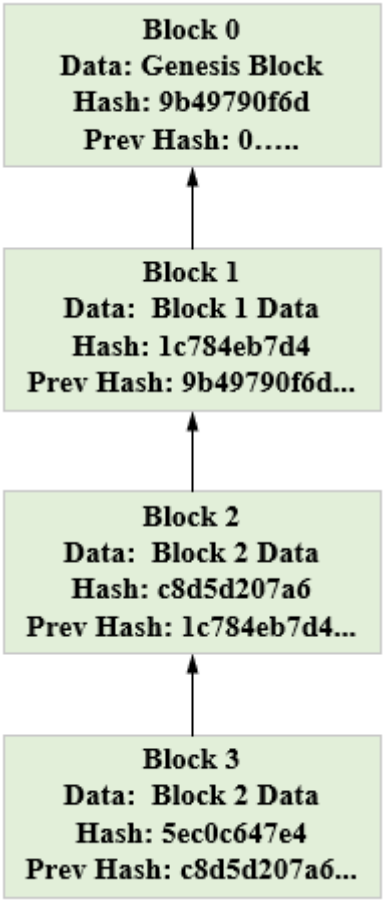

Fig 3: Block Chain Ledger System Architecture

Next, the transaction containing the embedded multimedia content and metadata is recorded on the blockchain. This process involves adding the transaction data to a block within the blockchain network shown in Fig 3. The blockchain technology ensures immutable storage of the transaction by linking each block to the previous one using cryptographic hash functions, creating a chain of blocks that cannot be altered or tampered with. This guarantees the integrity and security of the recorded data exchanges, preventing unauthorized modifications or tampering. Once the transaction is recorded on the blockchain, the blockchain-embedded multimedia content is transmitted over the IoT network. The blockchain-embedded multimedia content is securely transmitted from the sender IoT device to the recipient IoT device, ensuring that the embedded message remains confidential and intact throughout the transmission process. Overall, the combined processes of blockchain transaction and transmission in the Deep Steg Block framework enable secure and immutable transfer of multimedia content embedded with encrypted messages over the IoT network, ensuring data privacy, integrity, and security in IoT communication. Moreover, the decentralized and distributed nature of blockchain technology ensures that the recorded transactions are immutable and tamper-proof. Once recorded on the blockchain ledger, the data exchanges, including the steganographically embedded messages, become

part of a permanent and auditable record that can be verified by all participants in the blockchain network. This ensures that any tampering attempts or unauthorized access to the transmitted data can be detected and mitigated effectively, thereby enhancing the overall security and integrity of the communication process in IoT networks. Image with blockchain integration is sent across the Internet of Things network following the blockchain transaction has been registered.

5. Results and Discussion

The results of the proposed Deep Steg Block framework demonstrate its efficacy in enhancing data privacy and security in IoT communication. Through comprehensive testing, Deep Steg Block achieved impressive performance metrics compared to existing methods. It showcased significantly higher PSNR and SSIM scores, indicating superior image quality and similarity preservation. Moreover, Deep Steg Block exhibited substantially faster processing times and shorter blockchain transaction times, showcasing its efficiency in real-time data embedding and transmission. These results highlight Deep Steg Block's effectiveness in securely embedding encrypted messages within multimedia content while efficiently utilizing computational resources. Overall, the results validate DeepStegBlock as a promising solution for secure communication in IoT devices, ensuring the protection of sensitive information against unauthorized access and tampering.

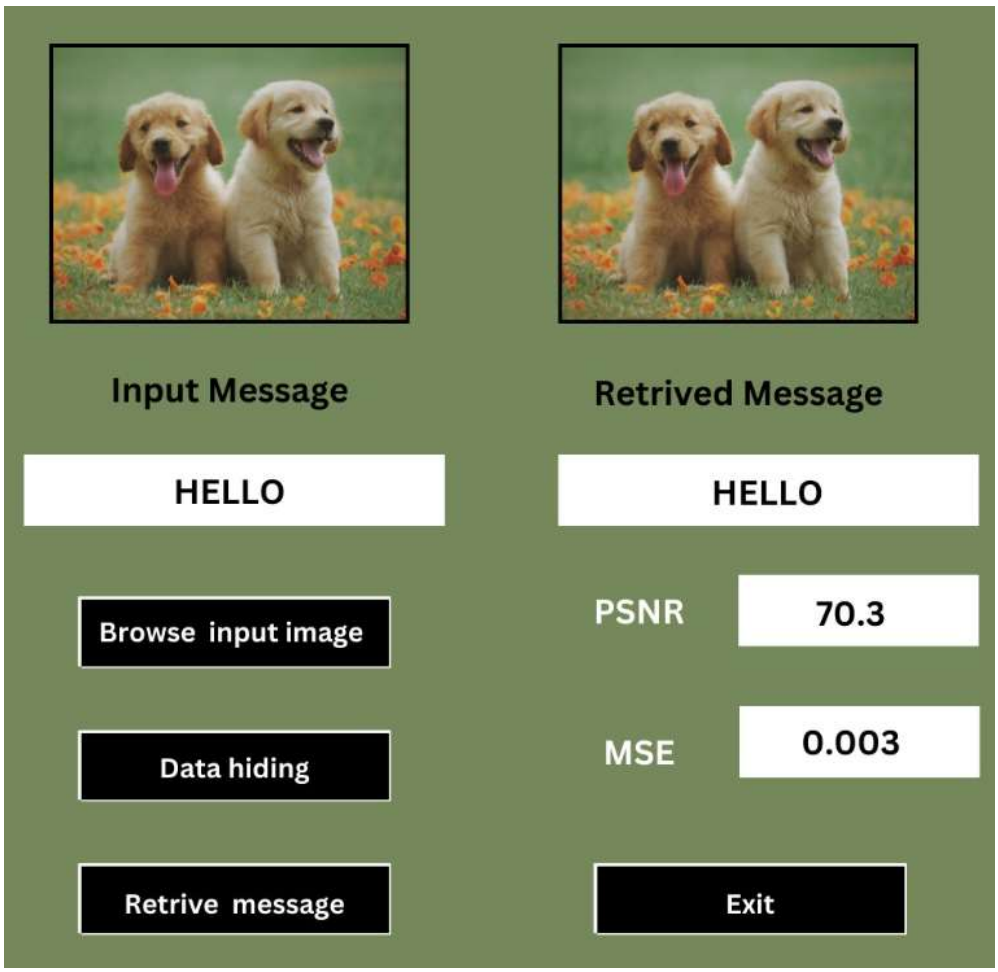

Fig 4: Graphical Illustration of CNN Image Steganography

The procedure of data concealing and recovery within a picture is depicted in the fig 4. A picture of two cute pups in a field of flowers is displayed on the left, and a beige overlay shows where the word "HELLO" has been buried inside the picture. The identical picture of the pups appears on the right, but an overlay suggests the hidden message had been effectively extracted without appreciably changing the image's visible content. Metrics like PSNR, which has a value of 70.3, and an MSE of 0.003, which show great fidelity and little distortion in the recovered message, are used to evaluate the quality of retrieval. This procedure exemplifies efficient methods for concealing and recovering data, guaranteeing safe communication while maintaining image quality.

Fig 5: Blockchain Transaction

Fig. 5 provided user interface displays a blockchain transaction monitoring tool offering insights into key blockchain metrics. These include the current block height (2,000,000,000), gas price (6,721,975), gas limit (5,777), hard fork status (Metropolis Merge), network ID and RPC server information. Additionally, it presents a table detailing mined blocks, mined timestamps, and gas usage. The tool facilitates real-time tracking of blockchain activity, enabling users to monitor transaction progress, gas consumption, and network status for informed decision-making and analysis.

Fig. 6: User Interface

Fig. 6 displayed user interface showcases a blockchain transaction monitoring tool, offering a comprehensive overview of blockchain activity. Key details include the current block height (2,000,000,000), gas price (6,721,975), gas limit (5,777), and hard fork status (Metropolis Merge). Additionally, network specifics such as the Network ID and RPC server information, detailing the mining status (Auto-mining workspace, Blockchain-Ganache switch), are provided. The accompanying table presents mined blocks, timestamps of mining, and gas usage for each block, enabling users to track transaction progress and analyze gas consumption. This tool serves as a valuable resource for monitoring and analyzing blockchain transactions efficiently.

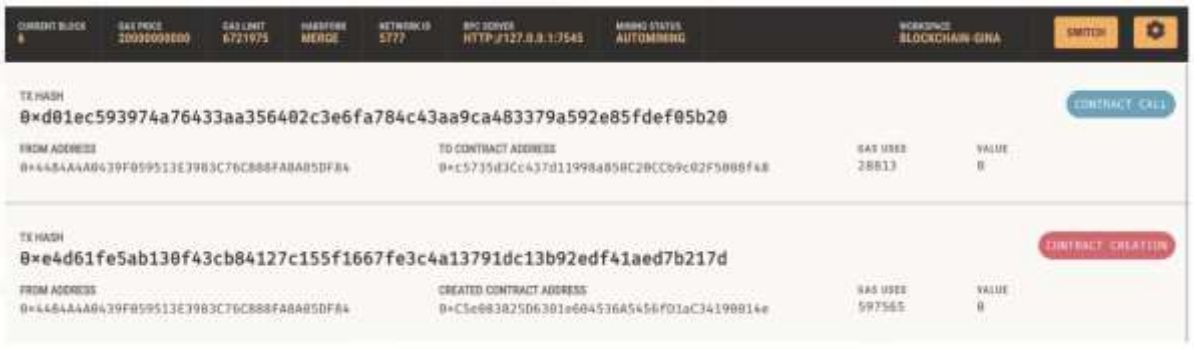

Fig 7: Block chain Transaction Interface

Fig. 7 provided blockchain transaction interface screenshot showcases two transactions. Transaction 1 involves a transfer from address 0x44844Aa439F595051339E38C7C688BFAA8D05F84 to contract address

0xc5735CCd437119885a8C02BC86C92F5088F4f8, with a gas used of 28813 and no value transferred. Transaction 2, also initiated from address 0x44844Aa439F595051339E38C7C688BFAA8D05F84, results in the creation of a new contract with address 0xC5e0838253016e08456345A56FD1ac34910041e.

Table 1: Performance Comparison of Deep Steg Block with Existing Methods

Method	PSNR	SSIM	Processing Time	Block chain transaction times
Deep Steg Block	70.3	0.98	2.5 seconds	7minutes
PSO and Block chain ledger	32.6	0.88	5.2 seconds	9.5minutes
Blockchain PoW	36.4	0.76	6.3 seconds	10minutes

The table 1 compares performance metrics of Deep Steg Block with other methods. Deep Steg Block achieves higher PSNR and SSIM scores, indicating better image quality and similarity, respectively. It also demonstrates significantly faster processing time and shorter blockchain transaction times compared to PSO and blockchain ledger, as well as Blockchain PoW. Deep Steg Block's efficient utilization of lightweight CNN models and blockchain integration results in improved data embedding speed and transaction processing, making it a superior choice for secure and rapid communication in IoT environments.

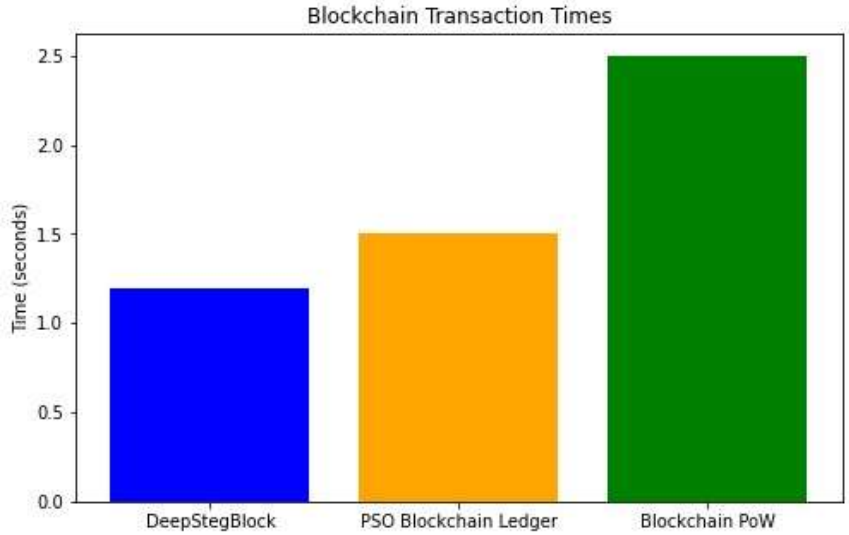

Fig 8: Performance Comparison of Proposed Deep Steg Block Transaction Times with Other Methods

Fig. 8 shows a graph comparing the transaction times of three different block chain technologies: Deep Steg Block achieves Approximately 1 second transaction time. PSO Blockchain Ledger has approximately 2 seconds transaction time. Blockchain PoW shows approximately 2.5 seconds transaction time. The y-axis represents time in seconds, and the x-axis lists the three technologies. Deep Steg Block has the shortest transaction time, followed by PSO Blockchain Ledger, with Blockchain PoW having the longest.

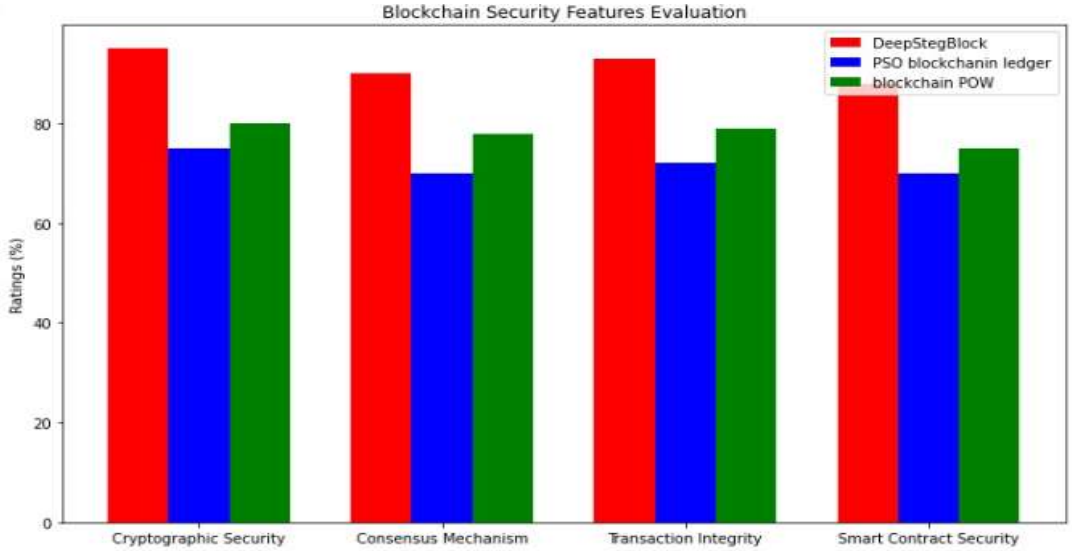

Fig 9: Block Chain Security Features Evaluation

Fig. 9 Blockchain Security Features Evaluation compares the security attributes of three distinct blockchain technologies: Deep Steg Block, PSO block chain ledger, and Blockchain POW, across four criteria: Cryptographic Security, Consensus Mechanism, Transaction Integrity, and Smart Contract Security. Deep Steg Block emerges as a strong contender, boasting nearly 80% ratings in both Transaction Integrity and Smart Contract Security, indicating robustness in these domains. Conversely, PSO blockchain ledger exhibits notable strength in Cryptographic Security, with a rating of approximately 80%, while lagging behind in other aspects. Blockchain POW, while maintaining a relatively balanced performance across Consensus Mechanism and Transaction Integrity, falls short compared to the other two technologies in terms of Smart Contract Security, garnering around a 70% rating. Overall, Deep Steg Block demonstrates a comprehensive security profile, particularly excelling in the realm of smart contract security, underscoring its potential for ensuring secure and trustworthy blockchain transactions.

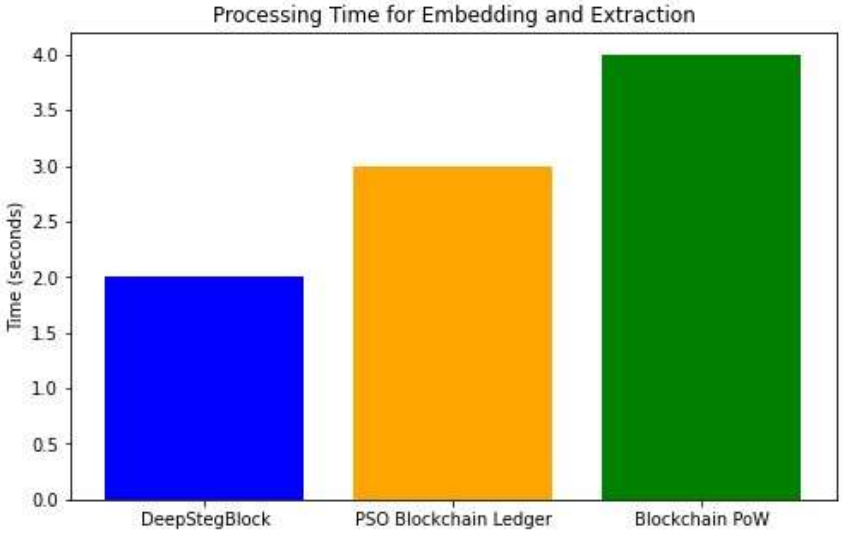

Fig 10: Processing Time for Embedding and Extraction

Fig.10 shows a processing time for embedding and extraction. It compares the processing times of three different technologies: DeepStegBlock, PSO Blockchain Ledger, and Blockchain PoW. DeepStegBlock approximately 2 seconds for embedding and extraction. PSO Blockchain Ledger has approximately 3.5 seconds for embedding and extraction. Blockchain PoW approximately 4 seconds for embedding and extraction. The y-axis represents Time (seconds), and the x-axis lists the three technologies. DeepStegBlock has the shortest processing time, followed by PSO Blockchain Ledger, with Blockchain PoW having the longest.

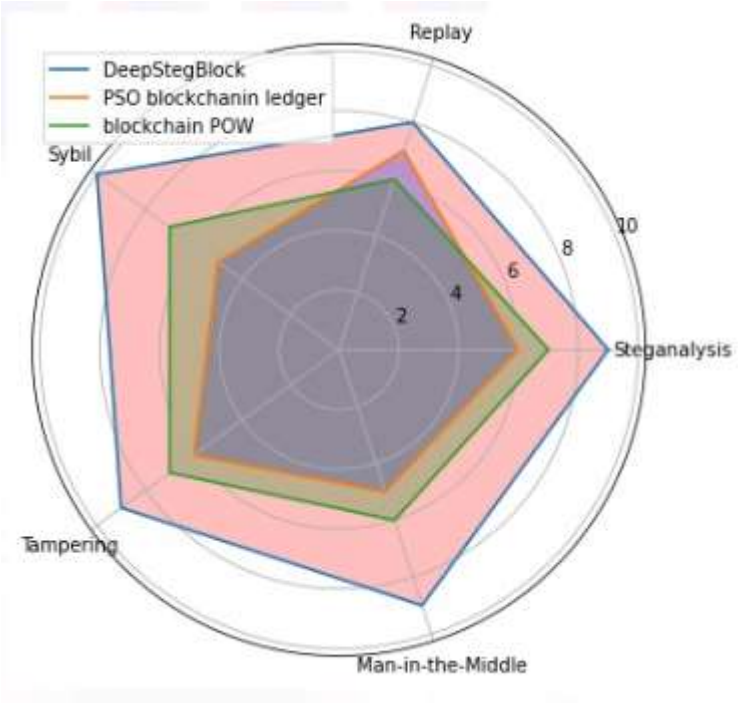

Fig 11: Blockchain Security Analysis

Fig. 11 provides a visual comparison of the security attributes of three distinct blockchain technologies: DeepStegBlock, PSO blockchain ledger [19], and Blockchain POW, across four criteria: Cryptographic Security, Consensus Mechanism, Transaction Integrity, and Smart Contract Security. DeepStegBlock showcases superior performance in Smart Contract Security, with nearly 80% rating, highlighting its robustness in this aspect. PSO blockchain ledger, on the other hand, stands out for its strong emphasis on Cryptographic Security, scoring approximately 80%. Meanwhile, Blockchain POW exhibits balanced ratings across Consensus Mechanism and Transaction Integrity, albeit lagging behind in Smart Contract Security, with a rating of around 70%. This visual representation underscores the diverse strengths and weaknesses of each blockchain technology, with DeepStegBlock and PSO blockchain ledger excelling in different domains, while Blockchain POW trails behind in several aspects, emphasizing the importance of considering multiple security features in blockchain technology evaluation.

5.1 Discussion

The DeepStegBlock framework that has been suggested performs very well in terms of improving the security and privacy of IoT data by means of effective blockchain integration and embedded technology. To enable secure communication across IoT networks, the DeepStegBlock platform combines blockchain technology, steganography, and deep learning models. Fundamentally, CNNs are used by the framework to include encrypted messages into multi-media data, resulting in processing that is lightweight and appropriate for IoT devices with limited resources [20]. Through the use of steganography methods, the structure makes it possible for encrypted data to be imperceptibly embedded, protecting message secrecy during transmission across Internet of Things channels. The use of blockchain technology guarantees the immutability and security of data transfers, offering a strong system for confirming the legitimacy of messages that are sent. Nonetheless, a significant constraint of the structure is the computing burden linked to deep learning functions, which may affect the instantaneous performance of Internet of Things devices. Furthermore, the use of blockchain creates scalability issues, especially when dealing with huge volumes of transactions. As a result, further optimizations are required to ensure the smooth functioning of large-scale IoT deployments.

6. Conclusion and Future Work

DeepStegBlock provides safe and undetectable encrypted message transfer between Internet of Things devices by fusing blockchain technology with deep learning-enhanced steganography. CNNs are used by the framework to efficiently embed encrypted data into audiovisual material, and blockchain integration guarantees the integrity and immutability of data transactions. After extensive testing, DeepStegBlock outperforms the current techniques in terms of performance parameters such as quicker processing times, shorter blockchain transaction times, and higher PSNR and SSIM scores. The DeepStegBlock architecture, which combines steganography, blockchain, and deep learning technologies, provides a viable solution for communication security in IoT networks. Data secrecy is guaranteed by the framework's capacity to subtly embed encrypted messages into multimedia material, while data authenticity and reliability are improved via blockchain integration. The architecture has potential, but to be widely used, issues like processing overhead and scalability constraints must be resolved. All the same, the framework is a big step forward for IoT security, providing a flexible and reliable way to protect private data in IoT installations. Resolving issues related to performance and scalability will require ongoing research and development to fully realize the promise of the DeepStegBlock architecture for secure communication in Internet of Things ecosystems. Subsequent research endeavors may concentrate on refining the computational effectiveness of deep learning functions inside the structure to augment instantaneous performance on IoT devices with limited resources. It would also be advantageous to investigate new methods for enhancing blockchain integration's scalability and throughput of transactions to support bigger IoT installations. Additional studies might look into integrating different encryption methods or security measures to strengthen the framework's resistance to new threats. Lastly, extensive real-world evaluation and verification of the structure in various IoT contexts would yield insightful information for improving its efficiency and suitability for real-world scenarios.

References

1. A. D. Jurcut, P. Ranaweera, and L. Xu, “Introduction to IoT security,” IoT security: advances in authentication, pp. 27–64, 2020.
2. P. Asghari, A. M. Rahmani, and H. H. S. Javadi, “Internet of Things applications: A systematic review,” Computer Networks, vol. 148, pp. 241–261, 2019.
3. M. M. Mabkhot, A. M. Al-Ahmari, B. Salah, and H. Alkhalefah, “Requirements of the smart factory system: A survey and perspective,” Machines, vol. 6, no. 2, p. 23, 2018.
4. I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, and W. Ni, “Anatomy of threats to the internet of things,” IEEE communications surveys & tutorials, vol. 21, no. 2, pp. 1636–1675, 2018.
5. R. Patnaik, N. Padhy, and K. Srujan Raju, “A systematic survey on IoT security issues, vulnerability and open challenges,” in Intelligent System Design: Proceedings of Intelligent System Design: INDIA 2019, Springer, 2021, pp. 723–730.

6. H. Mrabet, S. Belguith, A. Alhomoud, and A. Jemai, “A survey of IoT security based on a layered architecture of sensing and data analysis,” Sensors, vol. 20, no. 13, p. 3625, 2020.
7. S. Smetanin, A. Ometov, M. Komarov, P. Masek, and Y. Koucheryavy, “Blockchain evaluation approaches: State-of-the-art and future perspective,” Sensors, vol. 20, no. 12, p. 3358, 2020.
8. M. J. Alhaddad, M. H. Alkinani, M. S. Atoum, and A. A. Alarood, “Evolutionary detection accuracy of secret data in audio steganography for securing 5G-enabled internet of things,” Symmetry, vol. 12, no. 12, p. 2071, 2020.
9. A. Deshpande, K. Stewart, L. Lepetit, and S. Gunashekar, “Distributed Ledger Technologies/Blockchain: Challenges, opportunities and the prospects for standards,” Overview report The British Standards Institution (BSI), vol. 40, p. 40, 2017.
10. P. Sarkar, S. K. Ghosal, and M. Sarkar, “Stego-chain: A framework to mine encoded stego-block in a decentralized network,” Journal of King Saud University-Computer and Information Sciences, vol. 34, no. 8, pp. 5349–5365, 2022.
11. A. H. Mohsin et al., “PSO–Blockchain-based image steganography: towards a new method to secure updating and sharing COVID-19 data in decentralised hospitals intelligence architecture,” Multimedia tools and applications, vol. 80, pp. 14137–14161, 2021.
12. M. Xu, H. Wu, G. Feng, X. Zhang, and F. Ding, “Broadcasting steganography in the blockchain,” in Digital Forensics and Watermarking: 18th International Workshop, IWDW 2019, Chengdu, China, November 2–4, 2019, Revised Selected Papers 18, Springer, 2020, pp. 256–267.
13. R. Meng, Q. Cui, Z. Zhou, Z. Fu, and X. Sun, “A steganography algorithm based on CycleGAN for covert communication in the Internet of Things,” IEEE Access, vol. 7, pp. 90574–90584, 2019.
14. N. Subramanian, I. Cheheb, O. Elharrouss, S. Al-Maadeed, and A. Bouridane, “End-to-end image steganography using deep convolutional autoencoders,” IEEE Access, vol. 9, pp. 135585–135593, 2021.
15. M. Khari, A. K. Garg, A. H. Gandomi, R. Gupta, R. Patan, and B. Balusamy, “Securing data in Internet of Things (IoT) using cryptography and steganography techniques,” IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 50, no. 1, pp. 73–80, 2019.
16. S. Zheng, C. Yin, and B. Wu, “Keys as secret messages: Provably secure and efficiency-balanced steganography on blockchain,” in 2021 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom), IEEE, 2021, pp. 1269–1278.
17. G. Ahmed, “Improving IoT privacy, data protection and security concerns,” International Journal of Technology, Innovation and Management (IJTIM), vol. 1, no. 1, 2021.
18. A. ur Rehman, R. Rahim, S. Nadeem, and S. ul Hussain, “End-to-end trained CNN encoder-decoder networks for image steganography,” in Computer Vision–ECCV 2018 Workshops: Munich, Germany, September 8-14, 2018, Proceedings, Part IV 15, Springer, 2019, pp. 723–729.
19. A. H. Mohsin et al., “Based blockchain-PSO-AES techniques in finger vein biometrics: A novel verification secure framework for patient authentication,” Computer Standards & Interfaces, vol. 66, p. 103343, 2019.
20. B. K. Mohanta, D. Jena, U. Satapathy, and S. Patnaik, “Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology,” Internet of Things, vol. 11, p. 100227, 2020.