Journal of Intelligent Systems and Internet of Things
Vol. 18, No. 02, PP. 01-19, 2026
DOI: https://doi.org/10.54216/JISIoT.180201

Blockchain-Enabled Beamforming Optimization in 6G-IoT Using ConvMarkov and Laplacian Eigenmaps

Saleh Ali Alomari[1,*]
[1]Computer Science Department, Faculty of Information Technology, Jadara University, Irbid 21110, Jordan
Email: omari08@jadara.edu.jo

Abstract

In an increasingly fast-paced world of 6G-IoT networks, optimal beamforming techniques will be effective in improving strength, latency, and quality of service delivery in the networks. This work presents a new paradigm in beamforming optimization, especially in tackling dynamic environments and high computational costs in existing approaches. The problems of long training times with traditional methods, along with threats in security make them out rightly less applicable for real time applications. The data is collected from 6G IoT networks then, Laplacian Eigenmaps is used for feature extraction and modelling in time and applied for dimensionality reduction, ConvMarkov is used for model development RC4 encryption secures data exchange, while blockchain supports data logging and promotes transparency. This is a combination of deep learning techniques and advanced encryption methods, which will lead to a wide boost in beamforming efficiency, flexibility, and security. This study achieved the beamforming optimization achieved 97% accuracy with significant gain improvements, as indicated by an ROC curve (AUC = 0.9970) and precision-recall curve. The training loss stabilized below 0.01, while the validation loss fluctuated above 0.1, suggesting minor overfitting. The main achievements converge on proving improvements in optimization under real time conditions in a network, besides integrity and privacy of data. These become great merits into a strong solution for future 6G.

Received: February 13, 2025 Revised: May 31, 2025 Accepted: July 09, 2025

Keywords: 6G-IoT; Privacy-Preserving AI; Beamforming Optimization; ConvMarkov Model; Blockchain Integration

1. Introduction

The last few decades have produced an enormity of requirement for the best communication systems, with their applications expected to develop into new areas such as smart cities, autonomous vehicles, and industrial automation through 6G-IoT networks [1]. These high-performance systems will be aligned to optimally beam-form in order to maximize signal strength, minimize delay, and create greater energy efficiency [2]. Beamforming is a technique that improves the system in difficult environments by steering signals towards their intended receivers [3]. As the growing complexity in 6G networks was realized, it was inevitable to include other advanced techniques such as machine learning and computer vision, dedicated to optimizing the beamforming performance in and adapting to changes in dynamic environmental conditions [4].

This framework proposes improving the beamforming efficiency using ConvMarkov, a hybrid form consisting of Convolutional Neural Networks (CNN) for feature extraction while Hidden Markov Models (HMM) are used for temporal modelling [5]. With this new and advanced method, it will be possible to extract relevant and crucial features from network traffic and device behaviours while modelling the sequential dependencies [6]. It also contains the encryption techniques such as RC4 and uses the blockchain-based secure data transaction. This makes the proposed framework highly useful in future 6G-IoT systems where security and performance would be critical [7].

Among the numerous methods, one of them is optimization of beamforming for IoT networks via machine learning-based beamforming through reinforcement learning (RL), where the algorithm dynamically tunes beam patterns to get maximum signal power and minimum interference [8]. While this method is a good resolution to a controlled environment, in general the RL-based method suffers from high computation cost requirements along with time consumption for training, and as such is not a practical solution for use [9]. In such methods, though it does include, the beamforming optimization can be through deep learning techniques such as CNN, which are good at feature extraction but ignore the time-locked characteristics of network performance [10]. In addition, model-based beamforming techniques depend on physical models and simulations to predict beam patterns but do not fare well in terms of adaptability against actual dynamic environments suffering through their fixed assumptions [11]. Although computer vision methods employ beamforming optimization such as SIFT key point's extraction, these methods demonstrate positive results in beamform parameter selection, but there is no strong way that can be used in handling temporal variations, which makes the approaches highly sensitive and, thus, unable to provide the expected performance when handling conditions [12].

Currently Accepted Framework has been developed and attempts on features that are extracted using CNN and sequentially uses HMMs to detect anomalies. Unlike ConvMarkov, traditional methods use static beamforming parameters for temporal and spatial criteria. The CNN extracts essential features from network traffics and IoT device data, while the HMM is used to model the temporal dependencies for prediction and optimization of the beamforming adjustments over time. The accruing advantage of this model is to have an adaptable strategy to tackle dynamically occurring environment changes that bring high adaptability and efficiency even to the efficiency of the beamforming optimization techniques.

Combining RC4 encryption types has been masterminded with the intention of keeping communication and data secure throughout the optimization process while addressing privacy concerns with respect to sensitive IoT data. The second point remains on introducing blockchain as a public platform for key generation and transaction recording, which guarantees immutability and transparency in which all optimization actions would be securely stored and verifiable. With merging AI-driven optimization with sophisticated security systems, it is thus thought that this framework would step into the future in building smart and secure beamforming systems for the 6G-IoT network. The uniqueness of the study lies in it bringing together machine learning, computer vision, and blockchain technology for the solution of performance and security issues in next-generation networks. The key contributions of the proposed work are given below

1. Introduces a novel ConvMarkov model combining CNN and HMM for efficient beamforming optimization in 6G-IoT networks.
2. Optimizes beamforming decisions by extracting features with CNN and modelling temporal dependencies with HMM.
3. Ensures secure communication with RC4 encryption and immutable logging via BLAKE2-based blockchain integration.
4. Adapts to dynamic network conditions by continuously optimizing beamforming parameters.
5. Blockchain-based key generation and encryption ensures the privacy and integrity of sensitive IoT data.

The paper is organized as follows: Section 2 provides the literature review and discusses existing methods and their limitations. Section 3 elaborates on the proposed methodology. Section 4 elaborates on the results and performance analysis pertaining to the framework. Finally, Section 5 concludes the paper and discusses future work.

2. Related Work

In 2020 (Li., et al) [13] presents a lot of things could go wrong when it comes to securing AI data, especially in the case of malicious attacks, hence the authors introduce a blockchain-based security scheme that directly impacts artificial intelligence (AI) applications in 6G networks). It describes the potential 6G architecture as a space-air-ground-underwater integrated network, thus stressing the need for data security in a hostile setting. Two applications that would benefit from AI are examined within the 6G context indoor positioning and autonomous vehicles, thereby demonstrating the proposed security scheme's practical benefits. An example is provided of an indoor system of navigation that demonstrates how blockchain can secure data, and the authors discuss pending issues related to data security in new 6G networks while stressing the challenges encountered.

In 2021 (Nguyen, D. C., et al) [14] explores the transformative potential of a 6G wireless communication network has been captured in order to advance IoT applications, with an emphasis on some crucial technologies such as edge intelligence, Terahertz (THz) communications, etc. Encapsulated surveying between 6G and IoT, the major identified technologies clearly include reconfigurable intelligent surfaces. This paper is an informative piece on how 6Gs contribute to further developing various IoT segments-for example, healthcare, driverless vehicles, unmanned aerial vehicles (UAVs), satellite IoTs, and industrial IoTs. Finally, this study identifies important gaps in research as well as future directions for advancement into integrating 6G and IoT.

In 2023 (Mao, B., et al) [15] examines the benefits for the privacy and security of edge computing, edge caching, and edge intelligence are examined with a focus on security compromises for these technologies. Edge server instantiation in response to the service demand instances of immersive XR, holographic communication, and digital twins will be discussed. The emergence of new network architectures offering more flexibility but also introducing new attack vectors will be discussed. Counteracting measures such as Federated Learning (FL) and blockchain to enhance security in decentralized edge systems will be discussed. The article also identifies four challenges alongside future directions for improving security in 6G environments.

In 2023 (Jahid, A., et al) [16] explores the assimilation of the technology known as blockchain with 6G networks and IoT depicts how it would be a game-changer in establishing new wireless communication methods while attending to the shortcomings of 5G, especially when making provisions for increasing data-heavy applications. The paper elaborates on how Blockchain is expected to give enhancement in decentralization, transparency, security, and interoperability, which are critically needed by IoE (Internet of Everything) and IIoT (Industrial IoT). The paper sets out a research agenda roadmap through which blockchain will be integrated into 6G mobile networks through infrastructure sharing, latency, and sustainability. In addition, it has specified the existing challenges in such convergences and future research opportunities that could be exploited to address those issues and bring about integration towards blockchain in 6G networks.

In 2022 (Atlam, H. F., et al) [17] explores 6G raises many security and privacy challenges due to the connection of billions of devices where multiple critical processes are automated, which gives rise to a very complex attack surface that is as big as it gets. The fullness of 6G, which is expected to revolutionize connectivity through its integration of humans, cars, robots, and drones, with the concomitant generation of huge data sets. Security and privacy issues in 6G are discussed, with particular reference to increasingly automated core processes, which will lead to a wider, more complex attack surface. Integration of blockchain and Artificial Intelligence (AI) have been highlighted as solutions to the issues above by enhancing security and privacy. The role of AI and blockchain in providing effective security solutions for the outstanding concerns to the healthcare sector in a 6G-enabled environment is exemplified by focusing on the healthcare use case.

In 2020 (Nguyen, T., et al) [18] examines the various challenges and a few possibilities of integrating a blockchain technology towards enhancing the privacy and security aspects of 6G wireless networks, which indeed bear multiple advancements over the 5th generation networks. Such advances include enhanced reliability, higher speeds, and broader bandwidth for new applications. The paper mentions how the advancements of 6G give birth to more imaginative applications such as distributed artificial intelligence and ultra-reliable low-latency IoT, futuristic footprints. However, ensuring the privacy and security of 6G networks is one important aspect highlighted in the paper while being aware of the security vulnerabilities that arise with such improvements. The paper also elaborates on how blockchain technology can offer solutions for the security and privacy of 6G-native applications, but it states that one needs to address its own security challenges and privacy concerns.

In 2023 (Zainuddin, A. A., et al) [19] examines the 6G networks are also going to be the torchbearer for communication enhancements for a highly interconnected data-centric society, where eventual onset is expected around 2030. The authors touch upon IoT and blockchain integration, which can be employed to tackle security, scalability, and trust issues of IoT systems. Some use cases have been presented, e.g., blockchain applications in the supply chain, healthcare, and smart cities demonstrating improving the system's security, auditability, and traceability. Challenges and future research directions, such as scalability, energy consumption, interoperability, and privacy guarantees, concerning fully tapping the benefits of blockchain in IoT application over 6G networks, are also discussed.

In 2023(El Ghor, H., & Nakhal, B) [20] examines securing the data sharing and storage in 6G-based Internet of Things networks using blockchain technology, hybrid encryption, and Interplanetary File System. It is aimed at solving one of the critical challenges posed by high-speed and ultra-reliable low-latency communication environments expected in 6G IoT networks for securing and tamper-proof data transmission and storage. Therefore, this solution consists of four key algorithms: user authentication, data access, data storage, and secure data sharing. Specifically for secure data sharing, the algorithm employs a permissioned blockchain to allow tamper-proof sharing for authorized devices. This implemented research tests the valid functionality of this approach, which evidenced the improvement of the massive data thanks to hybrid encryption confidentiality and an IPFS enabled decentralized and safe storage for IoT data in 6Gs.

In 2021 (Siriwardhana, Y., et al) [21] explores the integration of AI has become necessary for intelligent orchestration and management of 6G networks, which is largely built upon 5G advances. The paper discusses opportunities and threats associated with AI and 6G security, emphasizing the fact that while AI is a boon for security, it has also become a bane for privacy. While 6G networks evolve into an end-to-end automated paradigm, it will be extremely necessary to proactively discover threats and intelligently mitigate them for network security

purposes. The article discusses how AI could best secure 6G networks and proposes measures to solve the issues of AI integration in security-building, self-sustainable and secure networks.

In 2022 (Gupta, R., et al) [22] proposes secure routing protocol based on the blockchain is proposed to propagate data in IoT environments, especially with respect to the security and privacy issues concerning traditional cryptographic solutions. It implements machine-learning algorithms: in particular, the Random Forest classifier achieves great accuracy with an excellent performance of 93.65% differentiating between adversarial and non-adversarial data. It has been proposed to address the challenges posed by the energy constraints of low-power IoT sensors, thus increasing the efficiency of data dissemination with respect to security and privacy concerns. Other benefits include low data storage costs, low latency, and high scalability, thus rendering it a mainstay for large-scale IoT applications. From its primary focus of IPFS integration and 6G networking, it becomes highly advantageous for large-scale IoT applications.

In 2024 (Liu, H., et al) [23] focuses on advancement in device authentication, detection of malicious behaviors, and repair of vulnerabilities is being targeted for security and privacy protection for IoT devices within 6G networks. It proposes a new security architecture incorporating Full-Dimensional Dynamic Convolutional Network (FDCN) to learn IQ signal characteristics for better device authentication. The method has been able to attain a device authentication success rate of 92% to 100%. Alongside this, it maintained the accuracy for malicious behaviors detection falling within the range of 88% and 95% against different sample sizes. Moreover, the time taken to detect vulnerabilities is significantly lesser against the current methods, improving anti-attack capabilities. It has also been able to achieve a high attack resistance rate of 93.59% under different attack complexities.

In 2021 (Nguyen, V. L., et al) [24] surveys an analysis of the security and privacy challenges of 6G mobile networks shows that these will require new responses to emerging threats from advanced technologies and an increased volume of user data. It also addresses the legacy vulnerabilities from past generations, and calls for newer approaches for risk mitigation, specifically, in a space-air-ground integrated network context. Currently, both the issues for 6G security and privacy are highly speculative and demand systematic exploration of vulnerabilities and defences over physical, connection, and service layers. Several advanced technologies, including ultra-massive MIMO systems at Terahertz bands, as well as ubiquitous intelligence, have opened up new vectors of threat to 6G networks. Thus, the paper suggests innovative techniques like quantum-safe communications, AI security, deep network slicing, platform-agnostic security, adaptive security, and new methods of data protection, such as distributed ledgers and differential privacy, to answer this challenge.

In 2023 (Kumar, P., et al) [25] explores artificial intelligence and blockchain adoption solves security and privacy problems in 6G-enabled terrestrial and non-terrestrial networks by moving to distributed AI. With 6G integration, TNTNs promote communication and provide interconnectivity and quality services. Security and privacy concerns emerge owing to the nature of unfettered communication and no trustworthy entities in TNTNs. This leaves the ecosystem to negative influence through legitimate users and adversaries alike. However, the paper shows that Distributed AI coupled with blockchain is a promising solution allowing mixed learning on devices where users' raw data are kept safe and data being used in smart contracts is guaranteed. The proposed scheme presents multiple parallel blockchains to efficiently manage and share data through different layers of the 6G enhanced TNTNs and is proving the effectiveness of the model with numerical findings while laying directions for future research in this area.

In 2021 (Porambage, P., et al) [26] surveys the implications of security and privacy in the prospective 6G wireless networks, even while 5G is still under operational scrutiny, focuses on the varied security risks stemming from the very requirements and new architecture of 6G networks that are envisaged as more complex and interconnected than the 5G systems. This paper underlines several enabling technologies that could overhaul security issues of future 6G networks: distributed ledger technologies, physical layer security, distributed AI/ML, Visible Light Communication (VLC), THz bands, and quantum communication. The authors hope that this will affect the understanding of how security might be undertaken in the planned 6G ecosystem and suggest possible ways to overcome the problems, thus enabling security for 6G networks to be effectively addressed as they continue to evolve.

3. Problem Statement

The problems being studied for optimization of beamforming in 6G-IoT networks are, [27] the beamforming methods dependent on traditional Reinforcement Learning are unable to optimize due to the high computational cost and long training time. [28-30] there exists an inefficiency in methodologies of coping with the dynamic network conditions since most methods consider a static approach that does not account for continuous changes in the environmental and device behaviour. [31] Security threats in the optimization process due to weak encryption and data integrity mechanisms expose the system to data alteration by users. [32-33] Existing methodologies are incapable of addressing both space and time dependencies jointly in beamforming decisions, giving rise to suboptimal decisions in realistic situations. [34-36] the optimization processes and their results are highly non-

transparent and untraceable, as security to current methods does not allow logging of all those actions audited and verified outside the optimization process. The main objectives of this paper are organized as follows:

1. Define the overall objective of the proposed framework, which aims to optimize beamforming performance in 6G-IoT networks through the integration of machine learning, computer vision, encryption, and blockchain.
2. Utilize the 6G-IoT network dataset, which includes network traffic patterns, environmental parameters, and performance metrics such as beamforming gain, latency, throughput, and more, for optimizing beamforming decisions.
3. Apply ConvMarkov (CNN-HMM Hybrid) for feature extraction and temporal modelling; enabling beamforming optimization based on the spatial and sequential patterns of network and device behaviours.
4. Implement RC4 encryption and blockchain integration to ensure data security, privacy, and immutable logging of optimization actions, enhancing the integrity and transparency of the optimization process.

4. Proposed Methodology

The optimization scheme for beamforming in the 6G-IoT networks is illustrated in figure 1. The process starts with Data Collection, where relevant data from network traffic, device behaviours, and environmental parameters, are collected. The Data Collection involves treating data to ensure it is suitably treated for analysis through things like Data Pre-processing, which includes data cleaning, normalization, and handling of missing values. After the data is pre-processed, we perform Feature Extraction wherein the dimensionality of Laplacian Eigenmaps is maintained while the critical geometric features of the data are preserved. These extracted features are then used for Model Development, where the hybrid model ConvMarkov (CNN-HMM) is used for feature extraction and temporal modelling, making it possible to provide optimization for beamforming. Concurrently, the data is protected using RC4 encryption during this process. Finally, Blockchain Integration is leveraged for the generation of secure keys using BLAKE2, while the logging of optimization actions is kept tamper-proof. The blockchain adds transparency and immutability of the system to guarantee the integrity of the process. The block diagram in figure 1 depicts the sequential steps and their interrelatedness, providing a clear overview of the framework's flow.

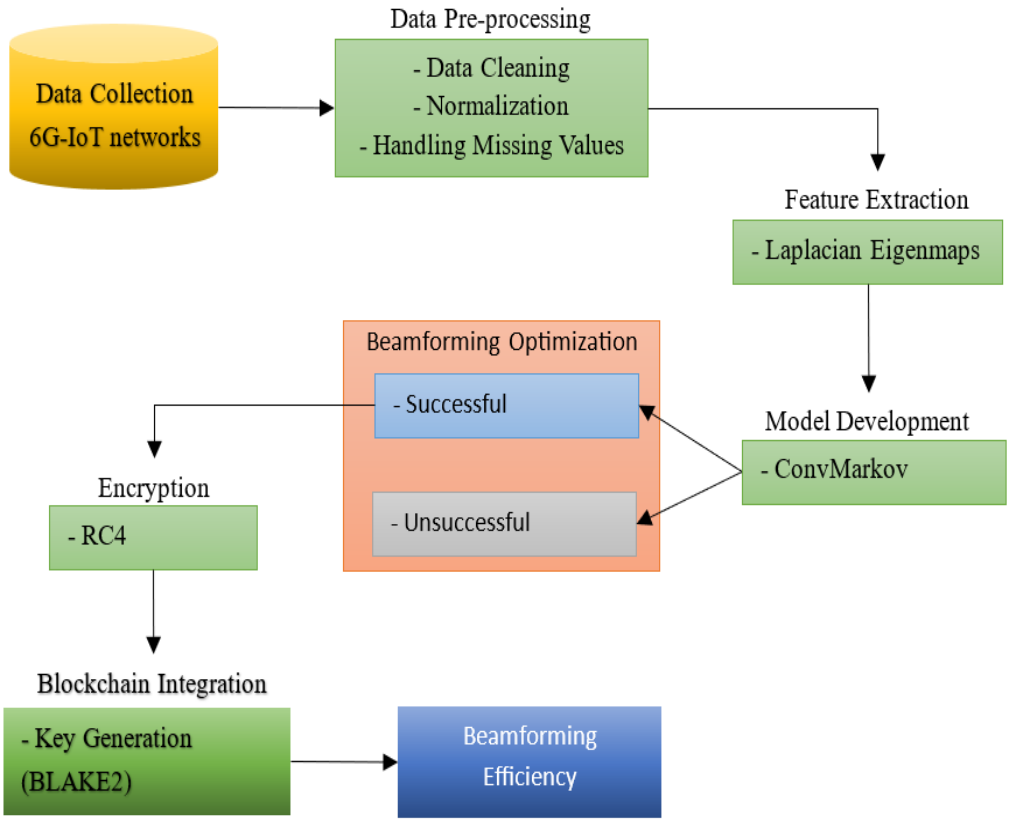

Figure 1. Optimized Beamforming in 6G-IoT Networks and Blockchain Integration

4.1 Data Collection

The contract is about collecting data for the proposed framework is to gather adequate empirical information that can benefit 6G-IoT networks in maximum optimality performance in beamforming. The frequency of the network, transmit power, bandwidth, and codebook size are some critical parameters for beamforming optimization included in the data. Environmental factors such as density of obstacles, mobility, classification into indoor/outdoor also need to be collected for studying their impact on network performance. Such reporting of device characteristics is number of antennas and device type for future use to study their contribution to beamforming efficiency. Other performance metrics considered include the gain in beamforming, latency, throughput, and SNR improvement, which would aid in ascertaining how successful the beamforming optimization has been. SIFT key points are extracted for intelligent beamforming decisions and provide crucial insights for further feature extraction. Finally, the optimized variable indicates whether the beamforming process was optimized successfully (1) or not (0).

4.2 Data Preprocessing Using Min Max Normalization

The phase of data pre-processing includes cleaning and preparing the collected data for subsequent analysis. Data cleaning includes removing duplicates and taking care of any missing values by imputation or other techniques. This ensures that the dataset is free of inconsistencies that otherwise would interfere with the performance of the model. Floor normalization is another aspect performed to scale numerical values to a consistent range while all other features are treated equally by the model without becoming artists in biased results due to values having differing scales across the dataset.

Further, handling missing values in the pre-processing step flux is crucial, as the presence of incomplete data predicts inaccurate predictions. According to the nature of the data left missing, various imputation techniques including mean versus more advanced techniques like K-nearest neighbors (KNN) imputation, are used. These guarantee that the dataset stays intact and trustworthy in the model's learning process. Without careful data pre-processing, the data remains unacceptable for being clean, normalized, and ready for feature creation and model training in the next phases.

4.2.1 Data Cleaning

Data cleaning involves detecting and rectifying errors, inconsistencies, and missing values in raw data in such a manner that it conditions the data for better quality and reliability during an analysis. For instance, among the data cleaning processes that a 6G-IoT network may employ, duplication removal, missing values treatment, and data normalization can be found. In deleting duplicates, there will be no bias or duplication, while missing value estimation uses most statistical methods like mean imputation as given in equation (1).

$$x_{ij} = \begin{cases} x_{ij}, & \text{if } x_{ij} \neq \text{NULL} \\ \frac{1}{n}\sum_{k=1}^{n} x_{kj}, & \text{if } x_{ij} = \text{NULL} \end{cases} \quad (1)$$

Where; x_{ij} is The value of the j-th feature for the i-th sample in the dataset, NULL represents a missing value in the dataset, n represents total number of non-missing observations in column j, x_{kj}represents the j-th feature value for each row k, used to compute the mean of the column, $\frac{1}{n}\sum_{k=1}^{n} x_{kj}$ represents the mean of all non-missing values in feature/column j, used to replace missing entries in that column.

4.2.2 Handling Missing Values

This is another important exercise in data pre-processing; handling missing values is one top activity under 6G-loT networks. Data loss in 6G-loT networks occurs in the link due to bad conditioning of the link, malfunctioning of the sensors, and errors in the packet transmission path. Incomplete data degrades the performance of the learning model operating on it, so it has to be predicted and filled. A widely used technique is to perform mean imputation, replacing the missing values of a certain attribute column with the average of all available values in that column. The general formula on finding the mean of a feature is given as equation (2).

$$X_{\text{missing}} = \frac{1}{N}\sum_{i=1}^{N} X_i \quad (2)$$

Where X_{missing} is the estimated value, which will be used to replace missing entries, X_i are known values in the column, and N is the total number of non-missing observations.

4.2.3 Normalization

Through normalization, all numerical features would be measured in one scale. One normalization approach is a Min-Max normalization, through which the features would be transformed into a definite range that often is [0, 1]. It is expressed in equation (3).

$$X_{\text{normalized}} = \frac{X_i - \min(X)}{\max(X) - \min(X)} \quad (3)$$

Where $X_i$is the original value, and $\min(X)$ and $\max(X)$ are the minimum and maximum values of the feature, respectively.

4.3 Feature Extraction using Laplacian Eigenmaps

In Feature extraction using Laplacian Eigenmaps, the strategy acts to capture the local geometric structure of the data. The basic idea behind Laplacian Eigenmaps is to treat the data points as nodes of a graph, where edges are formed between two data points that are neighboring in the high-dimensional original space. In this manner, the local relationships around a set of data points are preserved in a lower dimension space. First, a similarity graph $G = (V, E)$ is constructed so that each node v_i refers to a data point, and an edge between the nodes is weighted by some measure of similarity $W(v_i, v_j)$, often based on the Euclidean distance as expressed in equation (4).

$$W(v_i, v_j) = \exp\left(-\frac{\|X_i - X_j\|^2}{2\sigma^2}\right) \quad (4)$$

whereas in the Gaussian kernel used to measure similarity, X_i and X_j are two data points, and σ is a parameter controlling the width of the kernel. The weight $W(v_i, v_j)$ indicates how similar the two data points are in terms of value, with a high value stood for a high similarity between the two data points. Therefore, only a subset of the most similar points is connected to reduce the computational complexity for efficiency.

In addition, through the following equation, the Laplacian matrix L of the graph is constructed employing the degree matrix D and the weight matrix W as stated by equation (5).

$$L = D - W \quad (5)$$

where D is a degree matrix that contains only diagonal elements, and $D_{ii} = \sum_j W(v_i, v_j)$, relates to convergent node, that is adding the weights by which this node connects to v_i. The matrix represents L in terms of encoding the data's local relationships early in their lifetime, which enable the relevant features to be extracted by computing the eigenvalues and eigenvectors of the Laplacian matrix L. The solution includes solving as follows in eigenvalue problems as expressed in equation (6).

$$L\mathrm{f} = \lambda D\mathrm{f} \quad (6)$$

where f would be the eigenvector, while λ stands for each corresponding eigenvalue. The employed eigenvectors for reduced-dimensional representation correspond to the smallest non-zero eigenvalues, thus capturing the overall structures of the data. These newly formed features successfully retain the local geometry properties of the data while providing effective dimensionality reduction. Such techniques enable the model to operate efficiently on the data with the lower dimensional representation while holding on to relatively important relationships derived from their original high-dimensional space.

4.4 Model Development using ConvMarkov

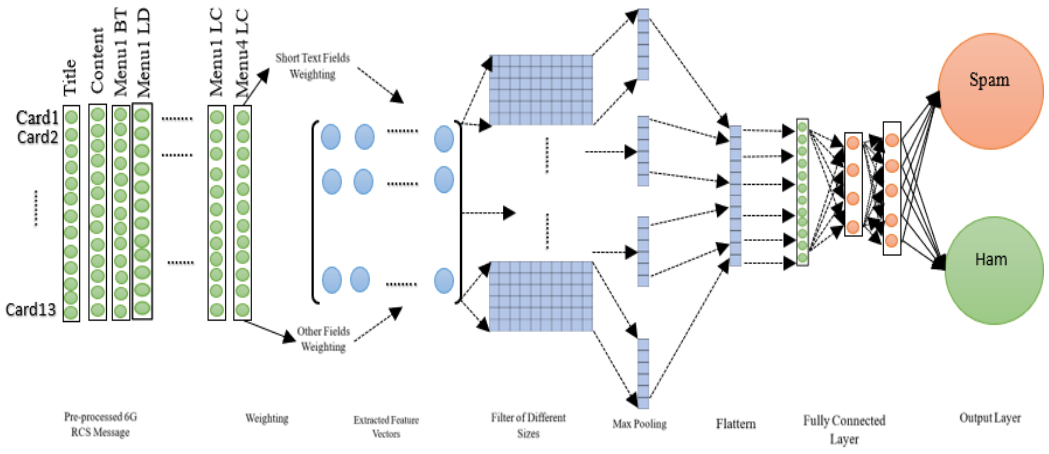

Figure 2. CNN-Markov Hybrid Model

ConvMarkov use hybrid models 'combining the strengths of Convolutional Neural Networks (CNNs) for features extraction and the strengths of Hidden Markov Models (HMMs) for temporal modelling. Their original intent is to optimize the performance of beamforming in a future scenario of 6G-loT networks, feeding on spatial and temporal dependence in the data. Towards this end, the CNN here is automatically fed with phenomenal, hierarchical features having no direct correspondence with raw data such as network traffic or device behaviour. The following is an example of the representation that gets modelled in some input data matrix $X \in \mathbb{R}^{N \times D}$, where N stands for the index of data point and D for the index of dimension dimension for each data point. What is performed at a certain layer of the multiple convolutional layers applied by the CNN to derive pertinent features from the set of filters W contributed to the input data is captured in equation (7).

$$Y = f(X * W + b) \quad (7)$$

while Y is the feature map, f is the activation function and b represents the bias term. The convolutional layers extract spatio-temporal patterns and pass them to the next layer of the model.

Once the CNN extracts features, temporal modelling is done via their incorporation into the Hidden Markov Model (HMM). The HMM captures the sequencing of dependencies and transitions for the different states in the data over time. The hidden states are S_t, whereas the observed data is O_t at time t, with the goal of inferring the sequence of hidden states given these observations. It is governed by the following two main components: the transition probability A between states and the emission probability B that is used to model the probability of O_t being seen given S_t as shown in equation (8).

$$P(S_t \mid S_{t-1}) = A_{st-1,st}, P(O_t \mid S_t) = B_{st}(O_t) \quad (8)$$

where A denotes the state transition matrix and B is termed the emission matrix. The transition matrix A denotes the probability of moving from one hidden state to another, and B denotes the likelihood of observing a particular feature vector O_t from a given hidden state S_t.

The complete procedure of ConvMarkov model is merging capability of spatial feature extractions by the CNN and temporal modelling capacity endowed by the HMM. After feature extraction by the CNN, the HMM would measure the sequential relationships among those features for the anomaly detection or beamforming optimization task. Maximizing the likelihood of the observed sequence of data given model parameters is the aim. This can be computed using a forward backward algorithm for training the HMM as covered in equation (9).

$$\alpha_t(i) = P(O_1, O_2, \dots, O_t, S_t = i \mid \lambda), \beta_t(i) = P(O_{t+1}, O_{t+2}, \dots, O_T \mid S_t = i, \lambda) \quad (9)$$

where $\alpha_t(i)$ is the forward variable and $\beta_t(i)$ is the backward variable meaning therefore that both represent the probability of the observations from time 1 to t and from $t+1$ to T, respectively, given the state sequence. Thus, the final output of the ConvMarkov model is an optimized beamforming decision, achieved from the learned combined spatial and temporal features, through which effective optimization will take place in dynamic 6G-loT networks.

Algorithm 1: ***Pseudocode for ConvMarkov***

```
Pseudocode for ConvMarkov (CNN-HMM Hybrid Model)

Input: Raw sequential data X
Output: Predicted state sequence Y

1. Initialize convolutional layers (Conv1, Conv2, ..., ConvN)
2. Initialize Markov model parameters (transition matrix T, emission probabilities E)

3. // STEP 1: Feature Extraction using CNN
4. function ExtractFeatures(X):
5.     features = X
6.     for each convolutional layer Conv_i:
7.         features = ReLU (Conv_i(features))
8.         features = MaxPooling(features)
9.     return Flatten(features)
```

```
// STEP 2: Discretize features into symbols or observations
function Quantize(features):
    symbols = KMeansClustering(features) // or VQ, SOM, etc.
    return symbols

// STEP 3: Train Markov model on symbol sequences
function TrainMarkov(symbol_sequences):
    Estimate transition matrix T from symbol sequences
    Estimate emission probabilities E if using HMM
    return T, E

// STEP 4: Inference
function Predict(X):
    features = ExtractFeatures(X)
    symbols = Quantize(features)
    if using Markov Chain:
        Y = MostProbablePath (symbols, T)
    else if using HMM:
        Y = Viterbi (symbols, T, E)
    return Y

// Main
features = ExtractFeatures(X)
symbols = Quantize(features)
T, E = TrainMarkov(symbols)
Y = Predict(X)
Output Y
```

4.5 Encryption using RC4

RC4 (Rivest Cipher 4), a symmetric stream cipher, creates a pseudo-random key stream which acts in conjunction with the plaintext data through an XOR operation to produce the ciphertext. The secret key used for generating the key-stream is normally between 40-256 bits and is used for initializing the S-box (substitution box). The encryption consists mainly of the key scheduling and the data encryption. During the first process, the key-scheduling algorithm (KSA) initializes the S-box, a 256-byte array, using the secret $K = (K_1, K_2, \dots, K_n)$. This key populates the S-box, and elements are swapped in order to produce a permutation. Key scheduling may be expressed mathematically as follows in equation (10).

$$\begin{matrix} S[i] = i, j = 0 \\ j = (j + S[i] + K[i \bmod n]) \bmod 256 \\ \mathrm{Swap}(S[i], S[j]) \end{matrix} \qquad (10)$$

where S is the S-box array, and j is a running index that is used to swap values within the array. The second phase begins when the S-box is established for encryption. The pseudo-random generation algorithm (PRGA) generates a key stream, which is then XOR'ed with the plaintext message P to yield the ciphertext C, as is stated in the equation (11).

$$C_i = P_i \oplus K_i \qquad (11)$$

where $C_i$is the ciphertext byte, $P_i$is the plaintext byte, and K_i is the corresponding keystream byte. At each stage, the PRGA generates the keystream by continuously swapping and updating values in the S-box and outputting a byte of keystream. The performance is efficient and very fast, making RC4 a commonly used encryption scheme. However, this scheme is stated to be unfit for some scenarios due to certain vulnerabilities in the design.

4.6 Blockchain Integration

An integration of a blockchain with the process of beamforming optimization, augmenting its security, transparency, and immutability, is given. The key generation is the first step in blockchain integration, which is done with the BLAKE2 hash function; generated secure cryptographic keys are used for data and transaction security. These keys are from the materialization of secure data logging to blockchain. Associated activities of beamforming optimization will be captured in a blockchain ledger; each optimization activity is written as a block and contains the relevant details such as optimization success or failure, time stamp, and associated data. Each block is linked to the previous block using a cryptographic hash so that no data can be tampered with or changed once recorded. This results in an immutable log with all optimization actions, which can be accessed by authorized parties without modifications. Smart contracts are immutable and will trigger automated actions when a predefined condition is met, such as re-optimizing beamforming parameters if a violation in secured parameters or a failure is detected. Thus, the beamforming optimization process, which is well secured, is completely transparent, verifiable, and tamper resistant increasing accountability within the system.

4.6.1 Hash Key Generation using BLAKE2

For secure key generation in the proposed framework, the BLAKE2 hashing algorithm is considered, ensuring cryptographic security and efficiency. The purpose of BLAKE2 is to provide security `at least' equal to that of MD5 or SHA-2 and, in addition to that, it aims to perform faster. The generation of key begins with the BLAKE2 algorithm having internal state initialized with a fixed initialization vector (IV) along with concatenation of the secret key K to the input message. The message M is then padded in such a way that its length becomes a multiple of the block size. The application of the BLAKE2 algorithm consists of many rounds of compression functions where the message is taken in blocks and the internal state is updated through a non-linear function. The formula for the BLAKE2 transformation at each round can then be written as equation (12).

$$h_{i+1} = f(h_i, m_i, k) \tag{12}$$

where h_i is the current state, m_i is the current block of the message being processed, and k is the secret key.

5. Results and Discussion

Advancing security and intelligent analytics, the proposed framework will serve as the optimizer-the beamforming optimization framework for 6G-IoT. Blockchain guarantees secure data processing by BLAKE2-key generation and RC4 encryption. The optimum feature extraction is achieved through Laplacian Eigenmaps in reducing dimension and keeping the structure. The ConvMarkov model coupled with CNN to HMM detect spatial and temporal trends for anomaly detection and predictive optimization purposes. Performance of the framework has been evaluated across a comprehensive measure that includes several parameters of communication quality, computational efficiency, scalability of the system, and reliability for suitability to 6G-IoT applications.

5.1 Dataset Evaluation

The 6G-IoT Intelligent Management Dataset gathered on Kaggle was the platform on which the proposed framework was appraised. It has parameters regarding the network, environment, and performance. The dataset was then pre-processed using cleaning, normalization, and dimensionality reduction with Laplacian Eigenmaps. The ConvMarkov worked toward optimizing beamforming and anomaly detection, while blockchain (BLAKE2) and RC4 were responsible for key management and data handling, which are secure. Evaluation metrics include beamforming gain/latency/SNR, processing time, and encryption/decryption efficiency, which proved the performance of the framework in a real-world 6G-IoT scenario.

Dataset Link: https://www.kaggle.com/datasets/ziya07/6g-iot-intelligent-management-dataset

5.2 Performance Analysis

The performance of a classification model with regard to predicting whether beamforming optimization in a 6G-IoT network will be successful or unsuccessful is depicted in Figure 3. In the cell matrix, there are a total of 995 instances of successful beamforming which is true positive prediction by the model and in 27 instances, model have predicted it wrong that that there is no beamforming successful, hence true negative; opposed to that in unsuccessful class, there are 20 instances prediction where it is wrong in identifying it as successfully completed for the 1191 places where beamforming was predicted accurately to be unsuccessful, hence true negatives. From this information, it is evident that high true positives and true negatives in the model also indicate that this model attains a high degree of accuracy.

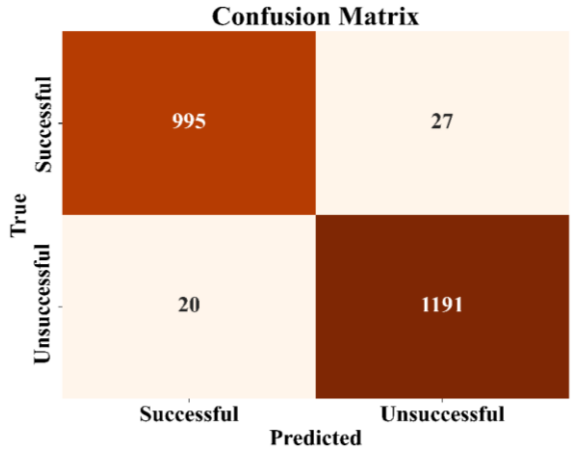

Figure 3. Confusion Matrix for Beamforming Optimization Classification

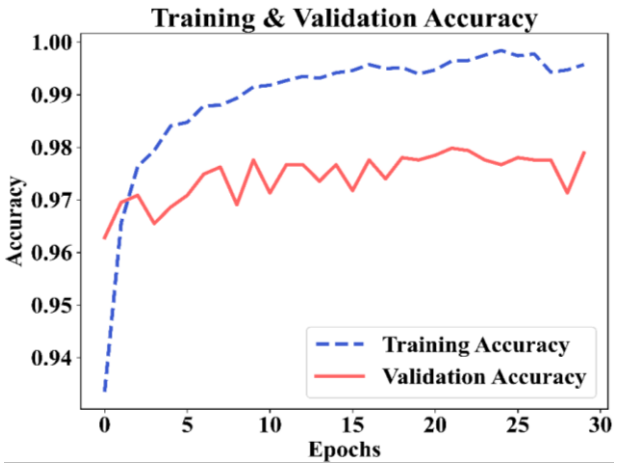

Figure 4. Training and Validation Accuracy over Epochs

Figure 4 shows the Training and Validation Accuracy progress over 30 epochs. The training accuracy showed a very fast increase and remained more or less at 0.98, indicating that the model learned well during the training time. However, for the validation accuracy, it started low and increased gradually with slight fluctuations coming from the end that got to around 0.97. The difference between the training and validation accuracies suggests possible overfitting, i.e, when a model does well on the training data it tends to be poor on the validation set instead.

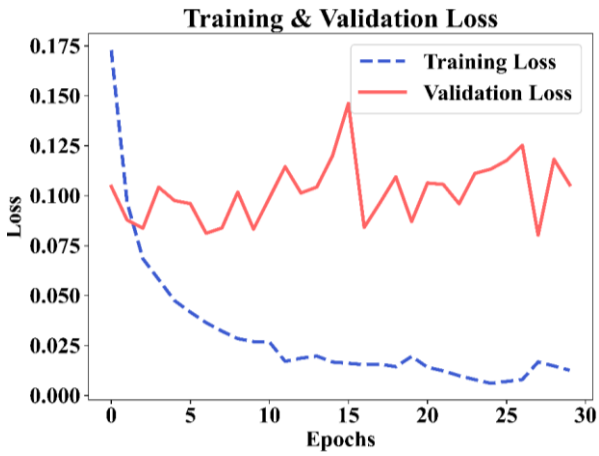

Figure 5. Training and Validation Loss over Epochs

The training and validation losses from 30 epochs are given in figure 5. The training loss falls quickly at the beginning, demonstrating that the model damn learns to minimize errors in training. The end training loss stabilizes at some below 0.01. In contrast, the validation loss starts higher and fluctuates much above 0.1 through the epochs. The difference between training and validation loss indicates that the model is probably overfitting-data performing well on training data but less consistently on validation data.

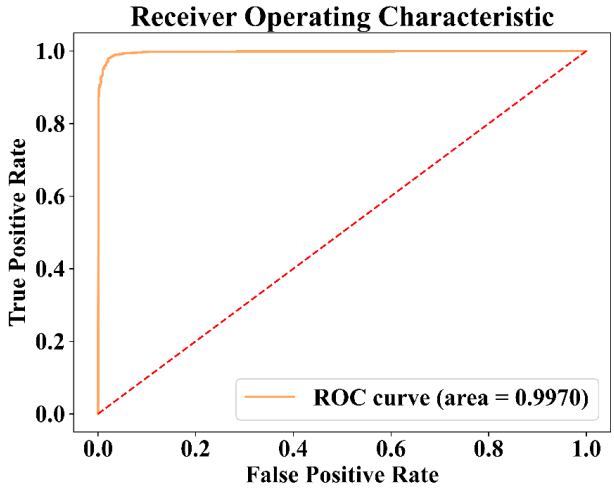

Figure 6. Receiver Operating Characteristic (ROC) Curve with AUC

The ROC curve for a classification model illustrated in Figure 6, is a graphical representation of the True Positive Rate (TPR) versus the False Positive Rate (FPR), where the ROC curve represents the model's performance. With an AUC of 0.9970, model performance is rated highly. A value close to 1.0 would mean a highly accurate model with very few false positives. The red dashed line corresponds to the baseline that indicates the area in which performance of a random classifier would lie corresponding to a diagonal ROC curve. Hence, the ability of the model to discriminate between the classes is much better than random guessing.

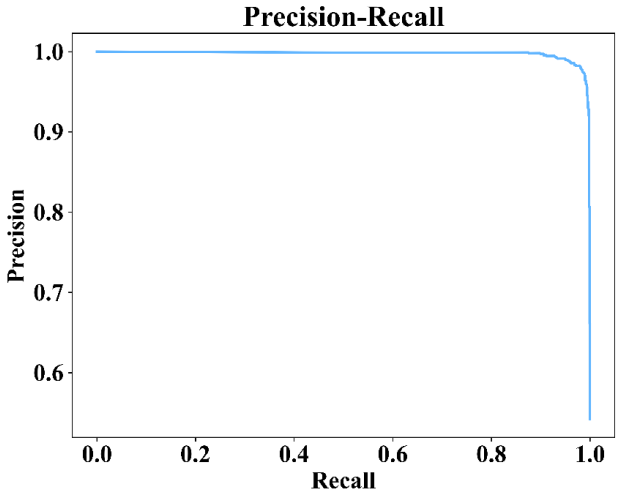

Figure 7. Precision-Recall Curve

Different thresholds show a trade-off between precision and recall, as shown in Figure 7. High precision indicates that the model achieves a precision of nearly 100% - 1.0 - i.e., when it predicts a positive class, it is almost always correct. Recall values increase, and along with that, precision begins to fall dramatically-that is, many positive instances will now be predicted, including false positives. This also indicates that there was a very high precision in the beginning but as more instances were recalled, the precision began to drop. The curve represents general performance in differentiating positive from negative classes, with higher precision values indicating a higher ability of the model to refrain from being wrong in its positive predictions.

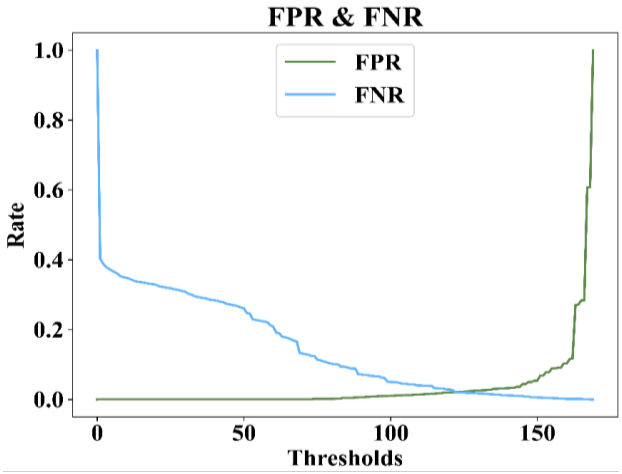

Figure 8. FPR and FNR Curves with Varying Thresholds

False positive rates (FPRs) and false negative rates (FNRs) are expressed as a function of thresholds in Figure 8. The Affected FPR, which starts high with the low thresholds at representing most negative samples categorized as being misclassified by positive ones, approximately becomes zero with the increase in threshold application. FNR on the other hand, low at the start, dramatically rises at increasing levels of the threshold, revealing that the overreeded positive samples are misclassified as negatives. In general terms, the graph shows the trade-offs between the false positives and false negatives, truly at higher thresholds where there is a reduction in false positives but an increase of false negatives.

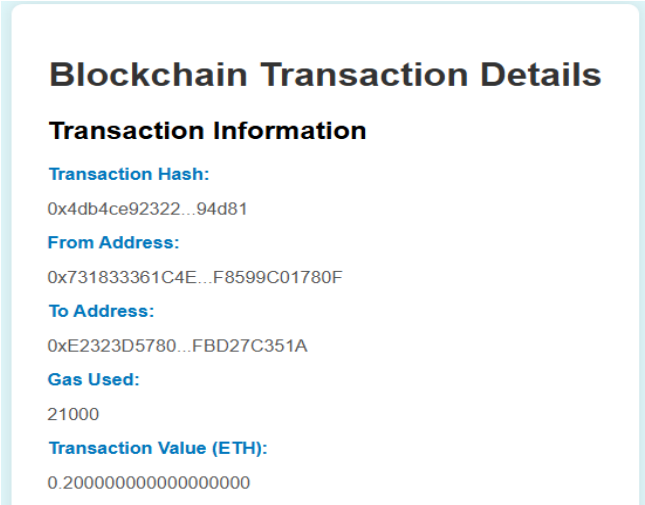

Figure 9. Blockchain Transaction Details

The details for the specific transaction are now shown in the blockchain, including the transaction hash, which uniquely identifies the specific transaction, is illustrated in figure 9. It portrays the sending address and the receiving address illustrating the origin point of the transaction and where funds were moved. Gas used (21000) refers to the computational resources utilized for the transaction. The transaction value given in this instance is 0.2 ETH, which refers to the value of Ethereum transferred in this particular transaction. All these details ensure transparency and immutability, thus verifying the authenticity of the transaction on the blockchain.

Figure 10. Blockchain Block Information

Figure 10 conveys the data about the block in the blockchain, such as displaying the block hash that uniquely identifies it, as well as the mined date and time (2024-12-21 09:54:26), which indicates when this block was added to the blockchain. I very well know that this set of data defines the gas limit of 6721975 that is in fact the number of computational resources, expressed in gas that can be consumed by transactions in this block. Please note that this information is unconditional to validate and indicate the reasons for the block creation and clearly define all the processing resources it contains.

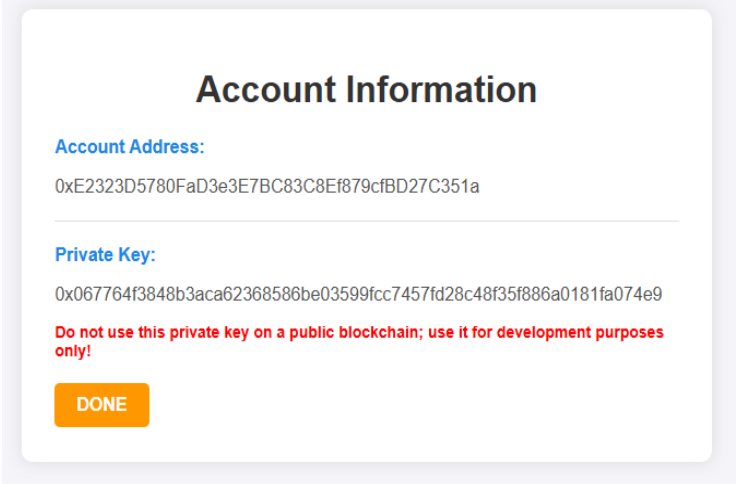

Figure 11. Blockchain Account Information

The account information view for a blockchain wallet is illustrated in figure 11. The account address is the unique identifier of the account on the blockchain, which enables transactions to be sent to that address. Below that is the private key used for authorizing transactions from this account. The cautionary note emphasizes the safety of private key storage and warns against using it for a public blockchain since it exposes the account to vulnerabilities; it mostly warns users that they should only use it in development and should not use it for real transactions in public blockchain settings.

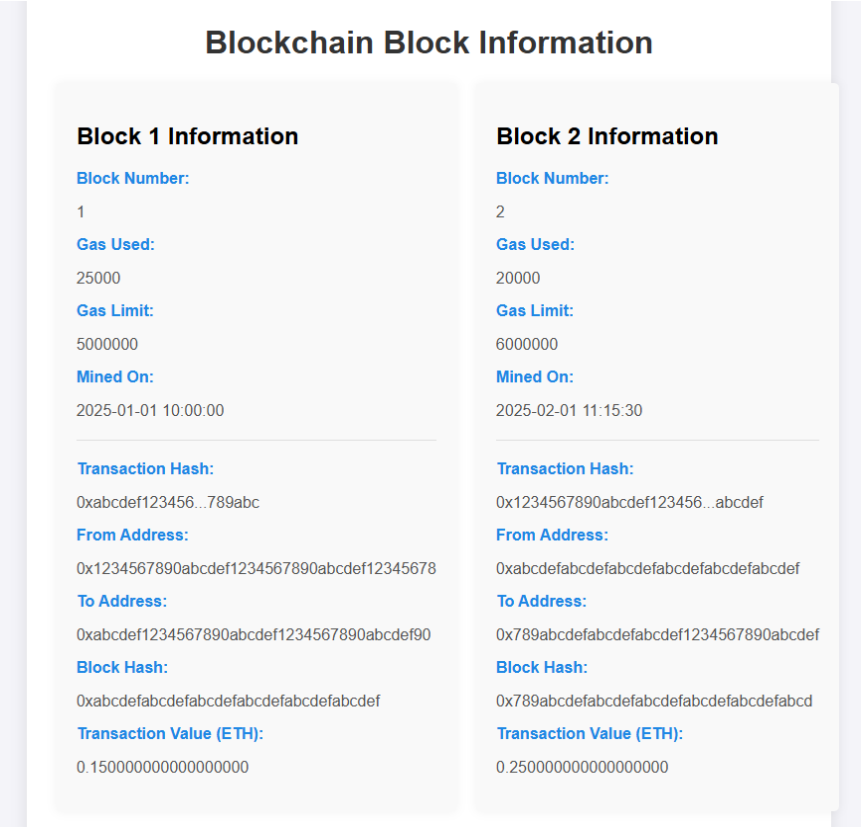

Figure 12. Blockchain Block Information with Transaction Details

Figure 12 shows the blockchain block information for two blocks, Block 1 with a gas usage of 25000 with a gas limit of 5000000, mined on 2025-01-01. Transaction hash and block hash are provided for this block along with transaction value of 0.1500 ETH that Block 2 is also having a gas usage of 20000 and a gas limit of 6000000, mined on 2025-02-01, along with transaction hash, block hash, and a transaction value of 0.2500 ETH. These data points give transparency and traceability benefits in blockchain transactions, with all the particulars verifiable and secured.

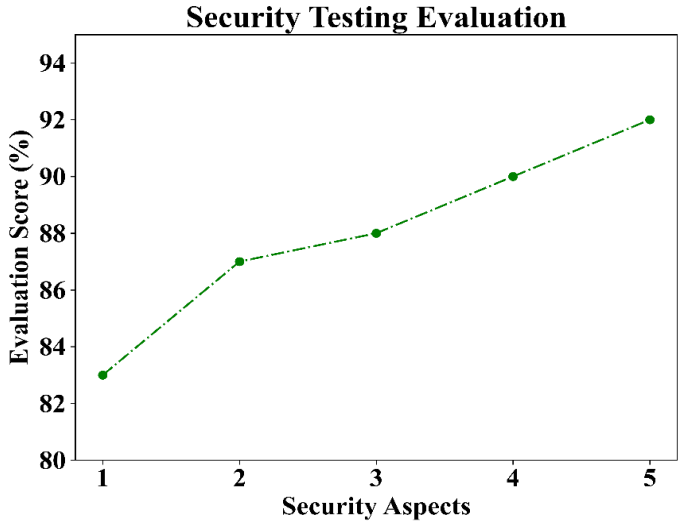

Figure 13. Security Testing Evaluation across Aspects

Looking at Figure 13, these are the evaluation scores for five different security aspects with a fair range of about 80% to 94%. Evaluation scores are said to progress with improvements in the security aspect. In terms of these aspects, it starts from 84 at the first dimension and progresses to 92 at the latter-most dimension. A dashed green line connects such data points. This shows that the eval scores across these security dimensions hold a uniform upward trend. This indicates that security measure becomes more effective as advanced aspects are considered, thus leading to improved overall performance in security.

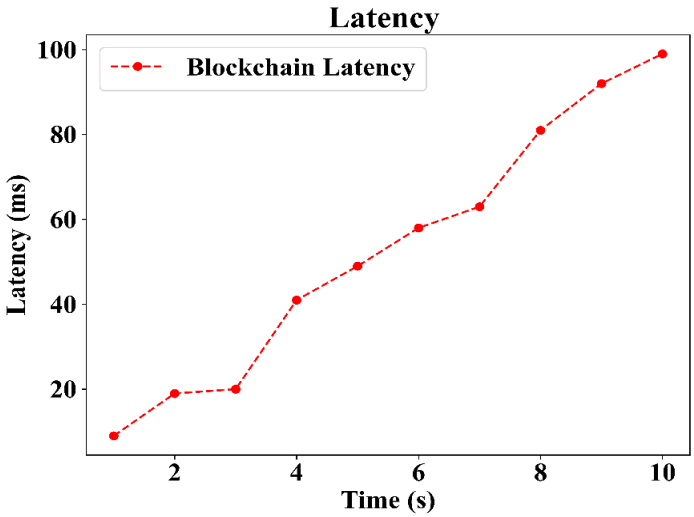

Figure 14. Blockchain Latency over Time

Figure 14 exhibits blockchain latency variation with time; hence, the definition of the performance latency in time (in milliseconds) goes up as the time (in seconds) goes on. The latency data are mostly represented by the red dashed line, which initially starts from 20 ms at 2 seconds and then gradually rises to reach 100 ms at 10 seconds. It shows the constant increase of blockchain latency as time passes, which could be a reason for increased computation or network load. The graph also depicts a clear upward trend between time and latency in the blockchain systems.

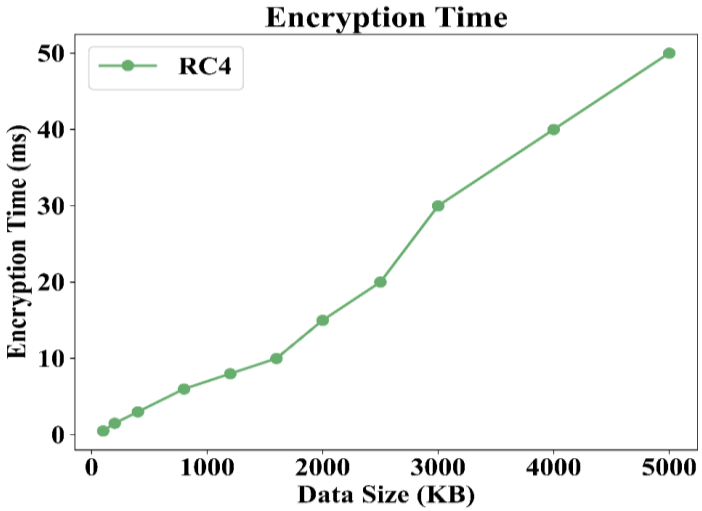

Figure 15. RC4 Encryption Time vs Data Size

Figure 15 shows the encryption time with the RC4 algorithm and measures the time in milliseconds against data sizes in KB. The encryption time starts at approximately 0 ms for small data sizes (closer to 0 KB) and then increases steadily with increases in data size. By the time data size reaches approximately around 5000 KB, the encryption time rises to about 50 ms. it assumes a straight-line increase in time while the data to be encrypted becomes larger. This means the above suffix regarding the time complexity of the RC4 encryption algorithm is directly proportional to the volume of data presently under process.

6. Conclusion and Future Enhancements

As discussed in the conclusion section, the proposed beamforming optimization framework for 6G-IoT networks, integrating ConvMarkov, Laplacian Eigenmaps, RC4 Encryption, and Blockchain Integration, showed improvements in performance in the sections analyzed. The beamforming optimization achieved very high accuracy at 97%, and the beamforming gain improvement was corroborated using an ROC curve (AUC = 0.9970) and a precision-recall curve, showing high effectiveness in discriminating between success and failure in optimization; the training loss was stabilizing under 0.01, and the validation loss was fluctuating above 0.1, indicating signs of little overfitting. Future research will use data for adaptive beamforming optimization with an emphasis on limiting overfitting and optimizing training and validation accuracies. Additionally, there are room for advancement in this area by integrating machine-learning models with cutting-edge blockchain capabilities to increase scalability and performance.

Acknowledgement: The author would like to thank the editor and anonymous reviewers for their comments that help improve the quality of this work.

Funding Statement: I would like to acknowledge the initial support received from Jadara University under grant number Jadara-SR-Full2023. This support played a vital role in facilitating this research.

Availability of Data and Materials: The author confirm that the data supporting the findings of this study is available within the article.

Conflicts of Interest: The author declare that they have no conflicts of interest to report regarding the present study.

References

[1] M. W. Akhtar et al., "The shift to 6G communications: vision and requirements," *Human-centric Computing and Information Sciences*, vol. 10, pp. 1-27, 2020.

[2] M. Asif et al., "Energy-efficient beamforming and resource optimization for AmBSC-assisted cooperative NOMA IoT networks," *IEEE Internet of Things Journal*, vol. 10, no. 14, pp. 12434-12448, 2023.

[3] L. Rao et al., "5G beamforming techniques for the coverage of intended directions in modern wireless communication: in-depth review," *International Journal of Microwave and Wireless Technologies*, vol. 13, no. 10, pp. 1039-1062, 2021.

[4] L. Jiao et al., "Advanced deep learning models for 6G: overview, opportunities and challenges," *IEEE Access*, vol. 12, pp. 51070-51109, 2024.

[5] S. Goumiri, D. Benboudjema, and W. Pieczynski, "A new hybrid model of convolutional neural networks and hidden Markov chains for image classification," *Neural Computing and Applications*, vol. 35, no. 24, pp. 17987-18002, 2023.

[6] J. N. Chukwunweike, A. A. Adewale, and O. Osamuyi, "Advanced modelling and recurrent analysis in network security: Scrutiny of data and fault resolution," *World Journal of Advanced Research and Reviews*, vol. 23, no. 2, pp. 2373-2390, 2024.

[7] N. Y. Al-Matari, A. T. Zahary, and A. A. Al-Shargabi, "A survey on advancements in blockchain-enabled spectrum access security for 6G cognitive radio IoT networks," *Scientific Reports*, vol. 14, no. 1, p. 30990, 2024.

[8] Y. M. Al-Hatim and A. O. Al Janaby, "Artificial-intelligence-enhanced beamforming for power-efficient user targeting in 5G networks using reinforcement learning," *International Journal of Computing and Digital Systems*, vol. 16, no. 1, pp. 1083-1095, 2024.

[9] B. Haouari, R. Mzid, and O. Mosbahi, "A reinforcement learning-based approach for online optimal control of self-adaptive real-time systems," *Neural Computing and Applications*, vol. 35, no. 27, pp. 20375-20401, 2023.

[10] I. Mallioras et al., "A novel realistic approach of adaptive beamforming based on deep neural networks," *IEEE Trans. Antennas Propag.*, vol. 70, no. 10, pp. 8833-8848, Oct. 2022.

[11] D. D. S. Brilhante et al., "A literature survey on AI-aided beamforming and beam management for 5G and 6G systems," *Sensors*, vol. 23, no. 9, p. 4359, 2023.

[12] A. M. Elbir et al., "Twenty-five years of advances in beamforming: From convex and nonconvex optimization to learning techniques," *IEEE Signal Process. Mag.*, vol. 40, no. 4, pp. 118-131, Jul. 2023.

[13] W. Li et al., "Blockchain-based data security for artificial intelligence applications in 6G networks," *IEEE Netw.*, vol. 34, no. 6, pp. 31-37, Nov./Dec. 2020.

[14] D. C. Nguyen et al., "6G Internet of Things: A comprehensive survey," *IEEE Internet Things J.*, vol. 9, no. 1, pp. 359-383, Jan. 2021.

[15] B. Mao, J. Liu, Y. Wu, and N. Kato, "Security and privacy on 6G network edge: A survey," *IEEE Commun. Surv. Tutor*, vol. 25, no. 2, pp. 1095-1127, 2nd Quart. 2023.

[16] A. Jahid, M. H. Alsharif, and T. J. Hall, "The convergence of blockchain, IoT and 6G: Potential, opportunities, challenges and research roadmap," *J. Netw. Comput. Appl.*, vol. 217, p. 103677, 2023.

[17] H. F. Atlam, M. A. Azad, M. Altamimi, and N. Fadhel, "Role of Blockchain and AI in Security and Privacy of 6G," in *AI and Blockchain Technology in 6G Wireless Network*. Singapore: Springer, 2022, pp. 93-115.

[18] T. Nguyen et al., "Privacy-aware blockchain innovation for 6G: Challenges and opportunities," in *Proc. 2020 2nd 6G Wireless Summit (6G SUMMIT)*, 2020, pp. 1-5.

[19] A. A. Zainuddin, N. F. Omar, N. N. Zakaria, and N. A. M. Camara, "Privacy-preserving techniques for IoT data in 6G networks with Blockchain Integration: a review," *Int. J. Perceptive Cogn. Comput*, vol. 9, no. 2, pp. 80-92, 2023.

[20] H. El Ghor and B. Nakhal, "A Blockchain-Enabled Approach for Secure Data Sharing in 6G-based Internet of Things Networks," in *Wireless Networks: Cyber Security Threats and Countermeasures*. Cham: Springer, 2023, pp. 227-246.

[21] Y. Siriwardhana, P. Porambage, M. Liyanage, and M. Ylianttila, "AI and 6G security: Opportunities and challenges," in *Proc. 2021 Joint Eur. Conf. Netw. Commun. 6G Summit (EuCNC/6G Summit)*, 2021, pp. 616-621.

[22] R. Gupta et al., "Blockchain and AI-based secure onion routing framework for data dissemination in IoT environment underlying 6G networks," in *Proc. 2022 Sixth Int. Conf. Smart Cities, Internet Things Appl. (SCIoT)*, 2022, pp. 1-6.

[23] H. Liu, Y. Wang, and F. Jia, "Security and Privacy Protection of Internet of Things Devices in 6G Networks," *Int. J. Syst. Assur. Eng. Manag.*, pp. 1-18, 2024.

[24] V. L. Nguyen et al., "Security and privacy for 6G: A survey on prospective technologies and challenges," *IEEE Commun. Surv. Tutor*, vol. 23, no. 4, pp. 2384-2428, 4th Quart. 2021.

[25] P. Kumar et al., "Distributed AI and Blockchain for 6G-assisted terrestrial and non-terrestrial networks: Challenges and future directions," *IEEE Netw.*, vol. 37, no. 2, pp. 70-77, Mar./Apr. 2023.

[26] P. Porambage, G. Gür, D. P. M. Osorio, M. Livanage, and M. Ylianttila, "6G security challenges and potential solutions," in *Proc. 2021 Joint Eur. Conf. Netw. Commun. 6G Summit (EuCNC/6G Summit)*, 2021, pp. 622-627.

[27] M. Fozi, A. R. Sharafat, and M. Bennis, "Fast MIMO beamforming via deep reinforcement learning for high mobility mmWave connectivity," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 1, pp. 127-142, Jan. 2022.

[28] Y. Han et al., "Dynamic neural networks: A survey," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 44, no. 11, pp. 7436-7456, Nov. 2022.

[29] S. K. Joshi and P. M. Shukla, "Reinforcement Learning for Dynamic Resource Allocation in 6G Cognitive Radio Networks," *IEEE Trans. Cogn. Commun. Netw.*, vol. 8, no. 2, pp. 742-756, Jun. 2022.

[30] S. A. Alomari, P. Sumari, and A. Taghizadeh, "A Comprehensive Study of Wireless Communication Technology for the Future Mobile Devices," *Eur. J. Sci. Res.*, vol. 60, no. 4, pp. 583-591, 2011.

[31] D. Kaul and R. Khurana, "AI to detect and mitigate security vulnerabilities in APIs: encryption, authentication, and anomaly detection in enterprise-level distributed systems," *Eigenpub Rev. Sci. Technol.*, vol. 5, no. 1, pp. 34-62, 2021.

[32] E. Focante, N. J. Myers, G. Joseph, and A. Pandharipande, "Adaptive beamforming for situation-aware automotive radars under uncertain side information," *IEEE Trans. Radar Syst.*, early access, 2024.

[33] S. Alomari and P. Sumar, "A video on demand system architecture for heterogeneous mobile ad hoc networks for different devices," in *Proc. 2nd Int. Conf. Comput. Eng. Technol.*, vol. 7, 2010, pp. V7-700–V7-707.

[34] P. Deepanramkumar and N. Jaisankar, "BlockCRN-IoCV: secure Spectrum Access and Beamforming for defense against attacks in mmWave massive MIMO CRN in 6G internet of Connected vehicles," *IEEE Access*, vol. 10, pp. 74220-74243, 2022.

[35] L. Chettri and R. Bera, "A Comprehensive Survey on Internet of Things (IoT) Toward 5G Wireless Systems," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 16-32, Jan. 2020.

[36] Z. Zhou, X. Chen, E. Li, L. Zeng, K. Luo, and J. Zhang, "Edge Intelligence: Paving the Last Mile of Artificial Intelligence With Edge Computing," *Proc. IEEE*, vol. 107, no. 8, pp. 1738-1762, Aug. 2019.