Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 3, Issue 4, 2025

AN ENHANCED MACHINE LEARNING AND BLOCKCHAIN-BASED FRAMEWORK FOR SECURE AND DECENTRALIZED ARTIFICIAL INTELLIGENCE APPLICATIONS IN 6G NETWORKS USING ARTIFICIAL NEURAL NETWORKS (ANNS)

Nasir Ayub[*1], Salheen Bakhet[2], M Junaid Arshad[3], Muhammad Usman Saleem[4], Dr. Rimsha Anam[5], Muhammad Zubair Fuzail[6],

[*1]*Deputy Head of Engineering Calrom Limited, M1 6EG, United Kingdom Department of Computer Science, Faculty of Computer Science & IT Superior University Lahore, 54000, Pakistan*
[2]*Department of Computer Science, University of Engineering and Technology, Lahore*
[3]*Department of Computer Engineering, University of Engineering & Technology, Lahore*
[4]*Department of Computer Science, Government College Women University Sialkot*
[5]*Comsats University Lahore, 54000, Pakistan*
[6]*Assistant Professor/ HoD CS&IT Lahore College of Pharmaceutical Sciences*

[*1]nasir.ayyub@hotmail.com, [2]salheen@ieee.org, [3]junaidarshad@uet.edu.pk, [4]usman.saleem@gcwus.edu.pk, [5]rimshaanamcs@gmail.com, [6]mzubair1725@gmail.com

DOI: https://doi.org/10.5281/zenodo.15210227

Keywords
Blockchain; 6G Networks; wireless Network; security management; machine learning Deep neural Network, CNN, Healthcare, Prediction models

Article History
Received on 07 March 2025
Accepted on 07 April 2025
Published on 14 April 2025

Corresponding Author: *
Nasir Ayub

Abstract
Artificial Intelligence (AI) and especially Machine Learning (ML) can play a very important role in realizing and optimizing 6G Network applications. 6G mobile Network technology will establish new benchmarks necessary for achieving unreasonable performance targets that exceed what 5G Networks can deliver. The performance targets which 5G Networks cannot achieve make 6G mobile technology necessary. The current limitations of 5G Networking become evident when more Networks become operational. More widespread 5G Network deployments encourage the study of 6G Networks because of their increased installation rates. Studies in this investigation cover essential aspects of privacy security alongside them. Security issues related to 6G technology. Maintaining a real-time system requires wireless monitoring to be secure. Sensor Networks (WSNs). The security vulnerability known as denial of service represents a major threat to Networks. The DoS attacks that WSNs encounter pose serious risks because they harm their complete operational system. This research proposes a novel Blockchain and Machine Learning based infrastructure (KSI) hash chain for 6G technology that enables Network security optimization through this new proposed method. A machine learning model for the 6G Network security system is implemented during this research. The blockchain user datagram transport protocol integrates reinforcement management methods to operate security function. Subsequent operations for Network optimization are accomplished through artificial democracy. The outcomes of simulation tests used different Network parameters. The Network evaluation relies on measurements of throughput together with energy efficiency packet delivery ratio and end–to–end delay parameters. The system provides a capability to determine optimal node and

path selection which minimizes Network traffic. The proposed technique obtained 97% throughput, 95% energy efficiency, 96% accuracy, 50% send–to–end delay, and 94% packet delivery ratio.

INTRODUCTION

The changes in these Networks' topology will result in effects on their routing approaches along with delivery delay and multi-layer structure requirements coverage range and fault-tolerance capabilities. The implementation includes delay, multi-layer architecture, coverage, and Quality of Services (QoS) along with fault detection [1, 2]. This intervention seeks to resolve the specific purposes embedded devices need to serve. WSN management needs a fundamental assessment for creating new protocols that integrate WSNs properly [3]. Security represents the primary set of problems that WSNs currently face together with energy usage. Both security and energy utilization need immediate attention because each factor negatively influences the other. The overall security complexity drives up the power consumption of the nodes [4, 5]. Given the challenging Leadership of both security concerns and energy, requirements emerge as the main determinant for the operating environments of these sensors. Recent research in this field attempts to tackle the problems which arise from WSNs. All security protocols require immediate reevaluation to achieve optimal performance. The security procedures known as Triangle consist of three essential definitions which include Confidentiality Integration and Authentication [6]. The three security procedures of key exchange along with encryption enable secure communication data exchanges between devices. Traditional approaches implement these devices as per [7]. Due to elements including wireless medium, short transmission range, ad hoc deployment, hostile environments, and limits the main issue facing WSNs is security because of limited energy capabilities. WSNs operate with two separate ways of functioning. Two security methods exist for WSN sensor protection: prevention-based and detection-based. Prevention-based Security strategies exist as initial protective measures against attacks in Wireless Sensor Networks [8]. Cryptography is the Prevention-based strategies use Cryptography as its main element though processes require additional time alongside substantial resources and funds. Figure 1 displays the architecture of a traditional Self Organizing Map model. Autoencoders: learning circuits that copy inputs into outputs, aiming to have the least possible deviation. They have great results on both classification and regression problems. Autoencoders are stacked approaches and are trained unsupervised bottom.

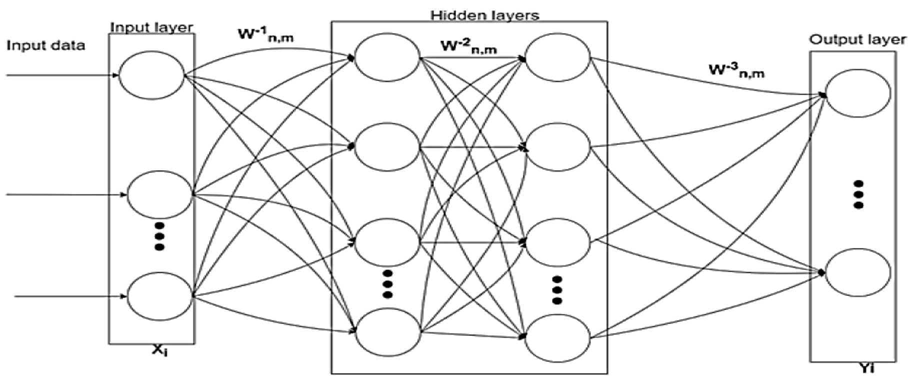

Figure 1: I/O Model for Decentralized 6G System

1.1 Machine Learning-based Wireless Network Security Management

The misuse/signature or anomaly detection methods in solutions are better suited for WSNs than other approaches. These detection approaches require fewer resources and duration to operate. The method explains how to gather abnormal Network activities.

Behavior from earlier [10, 11]. After detection, they evaluate incidents that their technique had previously identified. Defined. The signature-based detection technique maintains an understanding of attack behaviors that were predefined in its signature database. The definition of previous assaults makes this system unable to detect newly emerging threats [12]. The anomaly detection system proceeds with building reconnaissance models for ordinary Network events The detection methods build a typical Network model through analysis of normal environmental behavior patterns. The method uses differences between normal and abnormal Network occurrences to make its decisions [13, 14].

Anomalies constitute the data points that differ from regular occurrences. Anomaly detection identifies the anomalies The detection method functions through a set of pre-established typical occurrences and data. Therefore, this type of analysis of variance through this detection method helps find unidentified security attacks [15, 16]. Anomaly detection has a significant The system displays few false alerts but detects a large number of suspicious events. The IoT system, including The introduction of artificial intelligence to WSN, enables system improvement which overcomes previous limitations.

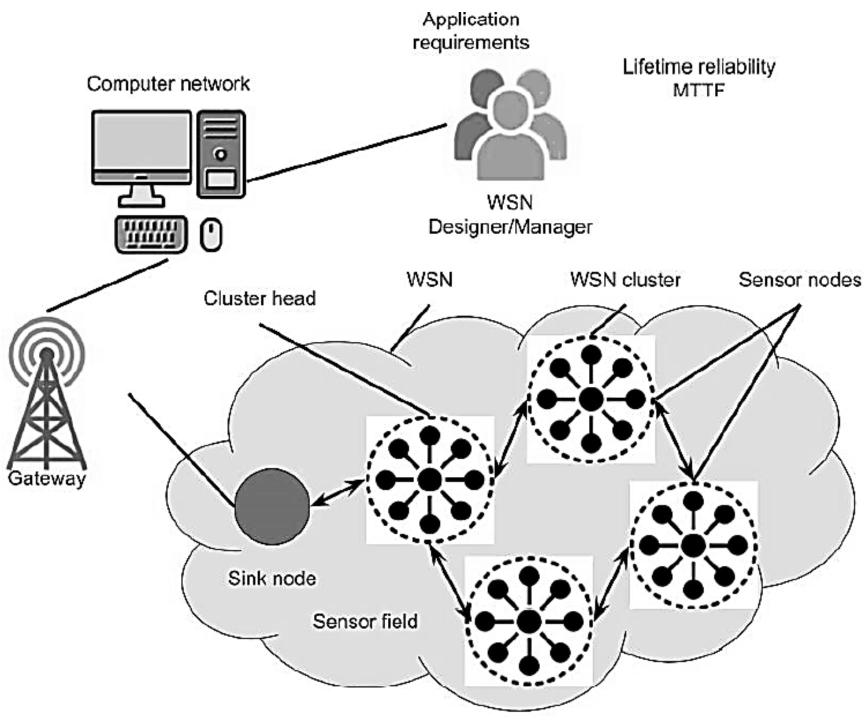

Figure 2: WNS based on CNN Sensor node [17]

Artificial intelligence technology shows rapid growth because developers create new algorithms regularly. Processing power improves significantly alongside the exponential growth of the data volume. Evolving algorithms represent the most common selection within this category. The research presents two algorithms called differential evolution (DE) along with genetic algorithms (GAs) which both model biological evolutionary occurrences [18, 19].

$$\rho_c = \frac{2a_{12}}{(\mu_1 - \mu_2)^2 + \sigma_1^2 + \sigma_2^2} \quad \text{Eq (1)}$$

$$R^2 = 1 - \frac{\sum_{i=1}^{n}\left(Y_i - \hat{Y}_i\right)^2}{\sum_{i=1}^{n}(Y_1 - \bar{Y})^2} \quad \text{Eq (2)}$$

The above Equations represents Evolutionary occurrences Such as pigeon-inspired optimization (PIO), grey wolf optimizer (GWO), particle swarm optimization (PSO), and cat swarm optimization The algorithms of cat swarm optimization (CSO) obtain their concepts from natural biological collective behaviors. Specific algorithms, such as the sine cosine algorithm (SCA), multi-verse optimizer (MVO), QUATRE, and others, The algorithms connect to mathematical principles together with physical theories.

$$R^2 = 1 - \frac{\sum_{i=1}^{n}\left(Y_1 - \hat{Y}_n\right)^2}{\sum_{i=1}^{n}(Y_1 - \bar{Y})^2} \quad \text{Eq (3)}$$

Owing to its exceptional Multiple challenging problems find efficient solutions through evolutionary algorithms because of their ability to adapt and be resilient [20].

2. Literature Review

Asserted application of optimization algorithms for multiple theoretical research problems and engineering technology requirements. It can also The method enables the optimization of multiple functions using abundant data under effective algorithmic procedures. Data and an effective algorithmic method [21]. Massive machine learning techniques have gained increasing adoption in WSNs throughout the past decade.

WSNs more and more intensively. In [22] a framework that serves as a solution for WSN security and authorization issues during Network access control. The system works to solve security-related problems and authorization issues within IoT Network access management systems. A newly proposed system manages IoT data sharing by delivering precise protection and authentication features with complete encryption standards. Networks. The article presents an original system to deliver a data-sharing protocol framework. A blockchain-oriented system provides access control to IoT devices. In addition, a detailed paper in [23, 24] presents research findings that analyze sustainable development with blockchain technology applications.

$$R^2 = 1 - \frac{\sum_{i=1}^{n}\left(Y_2 - \hat{Y}_n\right)^2}{\sum_{i=1}^{n}(Y_2 - \bar{Y})^2} \quad \text{Eq (4)}$$

A simplified introduction of machine learning techniques applicable to WSNs The system employs these methods to improve both information processing capabilities and Network performance results. [25] the team conducted a review of machine learning usages in wireless ad hoc Networks. Wireless ad hoc Networks. Three well-known machine learning algorithms—reinforcement All WSN communication layers received application from three machine learning frameworks including reinforcement learning and decision trees and neural Networks layers [26]. Certain investigations focus on demonstrating machine learning usage for particular WSN needs. There exist multiple research papers focusing on specific WSN challenges. The establishment of proper actions requires this system.

[27] created practical methods for outlier detection as an example of work demonstrated in this field. Algorithms for outlier detection exist using principles of machine learning among other approaches. Computational intelligence approaches currently resolve multiple problems that occur in WSNs.

The system requires solutions for routing, task scheduling, localization, optimal deployment, data fusion along data aggregation [28]. In this context, computational intelligence refers to a subfield of machine The field of computational intelligence uses biological inspiration to create algorithms which include evolutionary algorithms as well as fuzzy systems and neural Networks. Fuzzy systems, and neural Networks [29, 30]. An energy-efficient intrusion detection technique Maintenance operations are essential for the system which detects weak points in the Network's implementation area. The combination of Internet-of-Things devices with wireless sensors operates through 5G technology Networks [31].

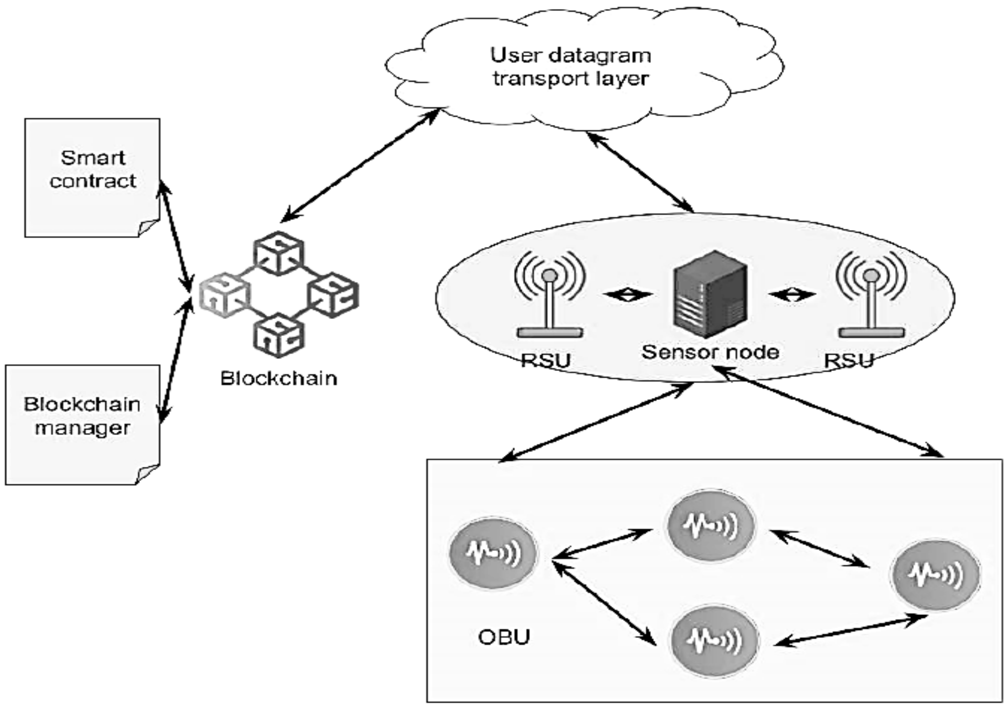

Figure 3: Blockchain-based User Datagram protocol in 6G data security [32]

2.1 Artificial and Convolutional Neural Networks

The Artificial Neural Network model involves computations and mathematics, which simulate the Network processes. Many of the recently achieved advancements are related to the artificial intelligence research area such as image and voice recognition, Network, and using ANNs [33]. These are responsible for image classification, and object detection tasks to help networks see, interpret and understand the visual world. CNNs have been extremely successful, with architectures like AlexNet getting a top-5 error rate of 15.3% on the ImageNet dataset. Research about mammalian visual cortex mechanisms formed the basis of Convolutional Neural Networks (CNNs). CNNs reproduce network functionality which enables neurons to analyze various spatial patterns in visual information [34, 35]. CNN architecture refers to an essential mathematical approach that enables weight sharing along with local processing and spatial pattern retention. The LeNet-5 model created by Kate and Shukla marked the first successful implementation of CNNs for handwritten number detection during the 1980s [36, 37]. Document recognition progressed a great deal after the model introduced gradient-based learning mechanisms. CNNs demonstrate exceptional performance in data arrangements with grid-like structures such as images that equal two-dimensional pixel grids. The study reviewed the foundation of neural Networks and their advanced structures alongside their primary medical diagnostic applications [38, 39]. As cyber threats become increasingly sophisticated, understanding the role of VPNs in mitigating these risks is critical. This paper explores the technological evolution of VPNs, examines their contemporary applications, and identifies potential advancements to address emerging security challenges [40].

$$min \sum_{s=1}^{N} \sum_{i=1}^{U} DP(U_{rq})_i - B_r$$

Eq (5)

$$DP\left(U_{rq}\right) = \frac{N \times \left(U_{rq_{max}} - U_{rq_{min}}\right)}{U_{rs_N}}$$

Eq (6)

The Internet of Things (IoT) has achieved great popularity and acceptance with the rapid growth of high-speed Networks and smart devices. In this respect, IoT represents a Network, in which "things" or devices are interconnected through a public or a private Network [41, 42]. These devices are equipped with tiny sensors and powerful hardware that collect and process data at unprecedented speed Researchers have explored various approaches to address these concerns, including the development of lightweight cryptographic algorithms to secure data transmission and storage in resource-constrained IoT devices. Additionally, efforts have been made to design secure frameworks and authentication protocols to mitigate the risks of IoT-related security breaches. Another key challenge in the IoT domain is the protection of user privacy [43, 44]. As IoT devices collect and transmit vast amounts of personal data, there is a growing concern about the potential misuse of this information, such as unauthorized surveillance, profiling, and targeted advertising [45]. While significant advancements have been made in cybersecurity technologies and legal frameworks, critical gaps remain. Many existing systems fail to address zero-day vulnerabilities and AI-driven cyberattacks, leaving organizations vulnerable [46]. Additionally, the legal frameworks intended to protect consumer data often lag behind technological advancements, creating regulatory gaps that attackers exploit. Ethical concerns, particularly regarding the misuse of surveillance technologies, further highlight the limitations of current approaches [47].

The proposed classifier contains i to represent random units of b-layer units and y to represent the total b-layer units.

$$S_i^{(b,t)} = \sum_{z=1}^{E} p_{iz}^{(b)} J_z^{(b-1,t)} + \sum_{i'}^{y} x_{ii'}^{(b)} J_{i'}^{(b,t-1)}$$

Eq (7)

$$J_i^{(b,t)} = \beta^{(b)}(S_i^{(b,t)})$$

Eq (8)

2.3 Machine Learning Algorithms

The ML algorithms that are required for these AI capabilities to function need integration in these humanoid networks. These algorithms help the network to digest data on how catheters are built and then control them to effectively work to accomplish outcomes based on them. Some common ML algorithms used in humanoid Network.

2.3.1 Supervised Learning, Unsupervised Learning and Reinforcement Learning

These are the algorithms that predict or classify new data according to train earlier classified data. Neural Networks and decision trees, object recognition and speech signal processing, respectively are widely used techniques. It helps to see the hidden pattern inside the data sets with no description. This can also work well in detecting novel occurrences or extracting useful data by engaging in some clustering or dimensional reduction [50]. This approach trains the network to make decisions by setting rewards for possible good choices (12). This also explores elastic behavioral sequences. The visual input helps humanoid networks categorize, and connect with their surroundings. These methods include: Convolutional Neural Networks (CNNs) which do image content classification and object detection (allowing networks to 'see' so that it can learn without any physical interaction [48].

3. Method & Materials

In realistic scenarios, the latency of inferring directly from participants is much lower communication than predicting in the cloud and then transferring to participants. The implementation of FL in mobile edge Networks accelerates content delivery and improves mobile service quality by reducing unnecessary system communication load. The model inference is completed locally without a cloud round-trip that avoids propagation delay caused by transferring data, and thus latency-sensitive applications can benefit from such a solution. Transmitting private data through a dedicated private circuit. $f = -Ex \sim pdata\ [\log pmodel(x)]$

$$\min_{w \in Rd} f(w) = K \sum k=1\ nk\ n\ Fk(w)$$

Eq (9)

Lipschitz Objective Function (LOF): $f(x)$ is β-Lipschitz continuous if there exists

$\beta \geq 0$ such that for all $x1, x2 \in Rd$

$|f(x1) - f(x2)| \leq \beta \| x1 - x2 \|$. Eq (10)

Smooth Objective Function (SOF): $f(x)$ is L-smooth if f (x) has L-Lipschitz continuous gradient, i.e., for all x1,x2 ∈ *Rd*,

$\|\nabla f(x1) - \nabla f(x2)\| \leq L\|x1 - x2\|$ Eq (11)

Strongly Convex Objective Function (SCOF): *f (x)* is μ- strongly convex if there exists μ≥ 0 such that for all x1,x2 ∈ *Rd*,*f (x1)* ≥ *f (x2)*+*(x1 −x2)T* ∇*f (x2)*+ *μ*

Coercive Function (CF): *f (x)* is coercive if lim ∥ x ∥ →∞ f (x) → ∞.

2 2

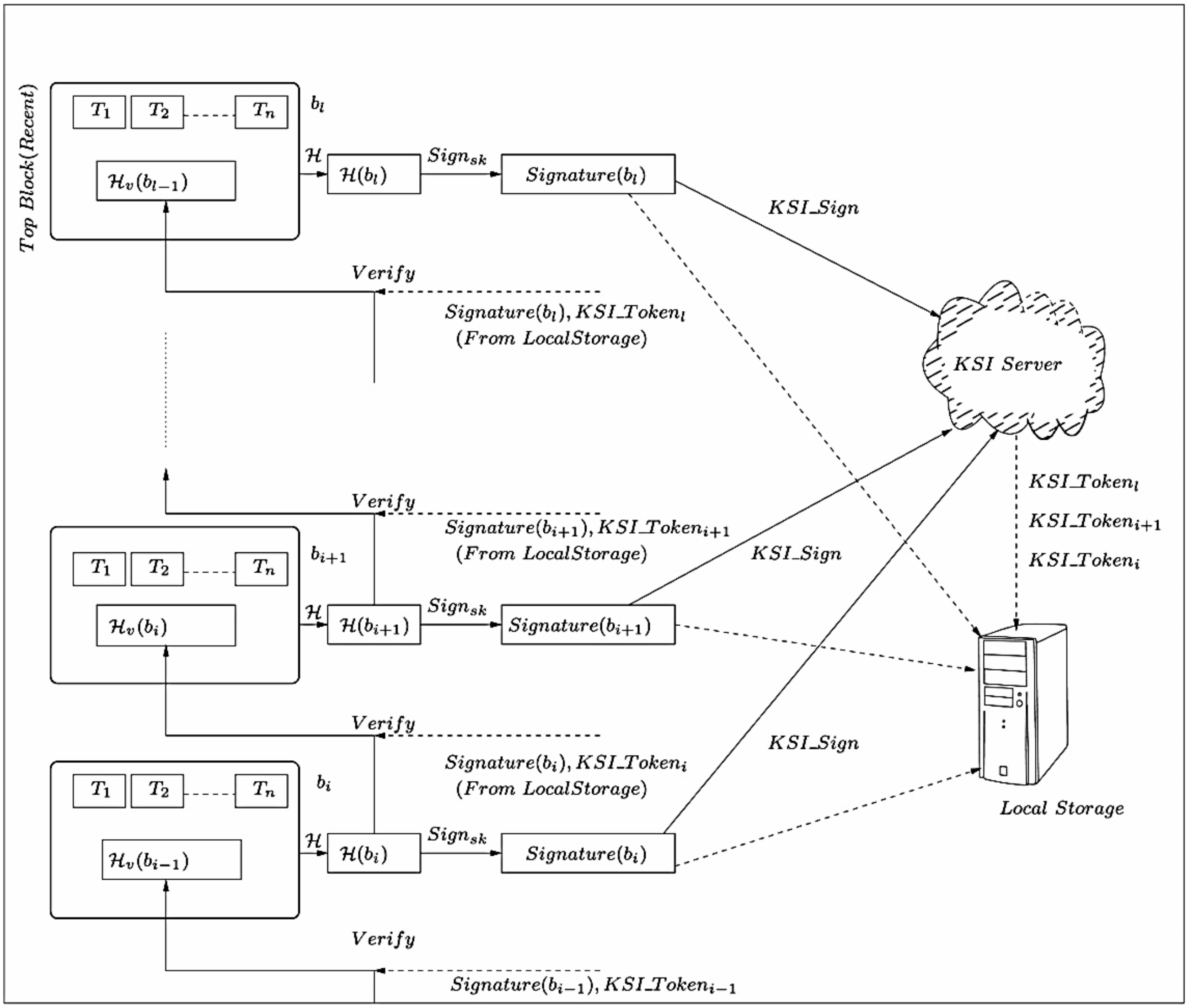

Figure 4: Proposed Framework for Machine Learning and Blockchain-based Decentralized 6G Network Using KSI Hash Chain

Bounded Variance (BV): The variance of each stochastic gradient ∇fi(x;ξ) is bounded if there exists σ∈ R, such that

$E\xi\| \nabla fi(x;\xi) - \nabla fi(x)\|^2 \leq \sigma^2$, Eq (12)

where *fi*(*t*) denotes the local objective function of the i-th client, x is the current model parameter and ξ is the data sampled in the current round of local training In the above assumptions, LOF, SOF, and LH describe the smoothness of the objective function. SCOF and COF characterize the convexity of objective functions. CF ensures that the objective function has a global minimum. BG, BV, and BGD capture the properties of gradients. These gaps underscore the need for a more integrated approach that addresses technological, legal, and ethical dimensions. The Proposed Technique works based on below Algorithm:

Algorithm 1: Algorithm for ML-based 6G Network

Step 1. Initialize the training models $\{k_1, k_2, \ldots k_m\}$, learning rate 'η', regularization 'λ', model parameters ΘA, ΘB, datasets $\{L_1, L_2, \ldots L_m\}$, space feature M_a and M_b;

Step 2. Minimize $k(i)$ parameter 'w' is

$$Min_w^k(i) = \sum_{j=1}^{M} k_i(w \mid L_i)$$

Step 3. The objective of the training is

$$Min \sum_i [\| \theta_A M_i^A + \theta_B M_i^B] - [N_i \| + \frac{\lambda}{2}(\|\theta_A\|^2 + \|\theta_B\|^2)]$$

Step 4. The encrypted loss is

$$L = \left[\!\left[\sum_i ((U_i^A + U_i^B - N_i))^2 + \frac{\lambda}{2}(\theta_A^2 + \theta_B^2) \right]\!\right]$$

Step 5. The gradients are

$$\left[\!\left[\frac{\delta L}{\delta \theta_A} \right]\!\right] = \sum_i d_i M_i^A + \lambda \theta_A \text{, and}$$

$$\left[\!\left[\frac{\delta L}{\delta \theta_B} \right]\!\right] = \sum_i d_i M_i^B + \lambda \theta_B$$

Step 6. The models are retrained

Step 7. Encrypts the data randomly

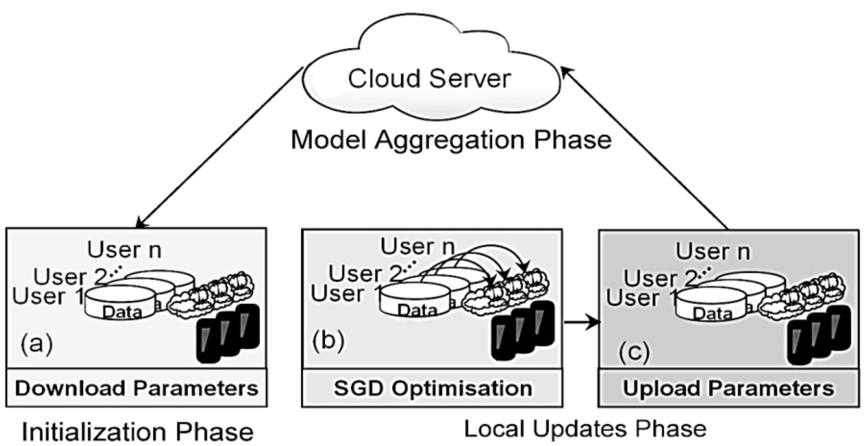

Figure 5: Generalize Framework for 6G Decentralized Servers

$$\sum_{i=\{1,..,n\}/k}^{n} \frac{c_i}{\tau_i} + \frac{c_k + \alpha_k}{\tau_k} \quad \textbf{Eq (13)}$$

While another task $\mathbf{t_2}$ With intrusions arrive at the earliest deadline before the end of the execution task. $\mathbf{t_1}$Then the length of the idle interval due to Network delay and threat is denoted as $\boldsymbol{\lambda_j}$ And max time duration for the idle period is represented as $\boldsymbol{\alpha_j}$ During longer data attacks that can be measured using Eq. (14).

$$\sum_{i=\{1,,,,n\}/(k,j)}^{n} \frac{c_i}{\tau_i} + \frac{c_k + \alpha_k}{\tau_k} + \frac{c_j + \alpha_j}{\tau_j} = 1$$ Eq (14)

$$\sum_{i=\{1,,,,n\}/(k,j)}^{n} \frac{c_0}{\tau_0} + \frac{c_0 + \alpha_0}{\tau_0} + \frac{c_0 + \alpha_0}{\tau_0}$$ Eq (15)

$$\sum_{i=\{1,,,,n\}/(k,j)}^{n} \frac{c_1}{\tau_1} + \frac{c_1 + \alpha_1}{\tau_1} + \frac{c_1 + \alpha_1}{\tau_1}$$ Eq (16)

$$\sum_{i=\{1,,,,n\}/(k,j)}^{n} \frac{c_3}{\tau_3} + \frac{c_3 + \alpha_3}{\tau_3} + \frac{c_3 + \alpha_3}{\tau_3}$$ Eq (17)

$$\sum_{i=\{1,,,,n\}/(k,j)}^{n} \frac{c_n}{\tau_n} + \frac{c_n + \alpha_n}{\tau_n} + \frac{c_n + \alpha_n}{\tau_n}$$ Eq (18)

3.1 Training and Validation of Proposed Scheme:

The dataset is split into training (80%) and testing (20%) sets and the model is trained using labeled sentiment data. Hyperparameter tuning is performed to optimize model accuracy.

$$B = \{B_1, B_2, \ldots, B_k, \ldots, B_l\}$$ Eq (19)

$$E_c = \frac{1}{K} \times \sum_{g=1}^{k} J_v^{b,t} - k_v$$ Eq (20)

$$B_{m,n}(q+1) = B_{m,n}(q) + X(0,1) \times (R_{s,n} - B_{m,n}(q))$$ Eq (21)

$$B_{m,n}(q+1) = \frac{B_{m,n}(q+1) - c_{m,n} \times f_{mn}(q) R_{s,n}}{1 - c_{m,n} \times f_{mn}(q)} \times [1 - X(0,1) - X(-1,1)] + X(0,1) \times R_{s,n} + X(-1,1) \times B_{fn}(q)$$ Eq (22)

The findings emphasize the importance of global collaboration, adaptive legal frameworks, and ethical considerations in creating a more secure digital environment. The structure of the paper includes an extended literature review, a discussion of key findings, and a conclusion outlining practical implications and future research directions. The increasing sophistication of cyber threats has rendered traditional defense mechanisms inadequate. Identify a critical issue in leveraging threat intelligence, noting that organizations struggle to process and act on the vast amounts of data required to prevent attacks. Emerging trends in cybersecurity highlight the growing importance of global collaboration and information sharing. Argue that a standardized international approach to cybersecurity is essential for addressing cross-border threats. Additionally, advancements in blockchain technology and decentralized systems offer promising solutions to some of the challenges in cybersecurity. Note that blockchain can enhance data integrity and reduce the risk of breaches, though attackers are already finding ways to exploit vulnerabilities in these systems.

$$B_{m,n}(q+1) = \frac{B_{m,n}(q+1)[1 - X(0,1) - X(-1,1)]}{1 - c_{m,n} \times f_{mn}(q)} - \frac{c_{m,n} \times f_{mn}(q) R_{s,n}[1 - X(0,1) - X(-1,1)]}{1 - c_{m,n} \times f_{mn}(q)}$$ Eq (23)

$$B_{m,n}(q+1) - \frac{B_{m,n}(q+1)[1 - X(0,1) - X(-1,1)]}{1 - c_{m,n} \times f_{mn}(q)} = X(0,1) \times R_{s,n} + X(-1,1) \times B_{fn}(q) - \frac{c_{m,n} \times f_{mn}(q) R_{s,n}[1 - X(0,1) - X(-1,1)]}{1 - c_{m,n} \times f_{mn}(q)}$$ Eq (24)

$$B_{m,n}(q+1)\left(1 - \frac{1 - X(0,1) - X(-1,1)}{1 - c_{m,n} \times f_{mn}(q)}\right) = X(0,1) \times R_{s,n}$$ Eq (25)

VPNs are indispensable tools in today's digital ecosystem, serving as safeguards for personal privacy, enterprise data security, and secure communication in remote work settings. They ensure confidentiality, integrity, and authentication, enabling secure transmission of sensitive information. Moreover, VPNs are instrumental in circumventing geo-restrictions and ensuring internet freedom, particularly in regions with stringent censorship laws.

$$P(c|x) = \frac{P(X|C).P(C)}{P(X)}$$ Eq (26)

P (C|X): The probability of which query belongs to the class C malicious.
P (X|C): This is the likelihood the data of X is given to class C.
P (C): This prior probability of the class C is a common class.
P (X): This is the total probability of the data X.

3.2 Data Poisoning Attack Methods

Data poisoning attacks can be divided into methods such as label flipping, target optimization, gradient optimization, and clean labeling based on technical implementation methods. Data poisoning by directly modifying the label information of the training data of the target category, while the characteristics of the data remain unchanged. Attackers can poison data by modifying data and data labels. Train a softmax classifier across ten honest clients, each holding a single-digit partition of the original ten-digit MNIST dataset. Attackers achieve data poisoning attack goals by manipulating data labels, such as deliberately labeling the number.

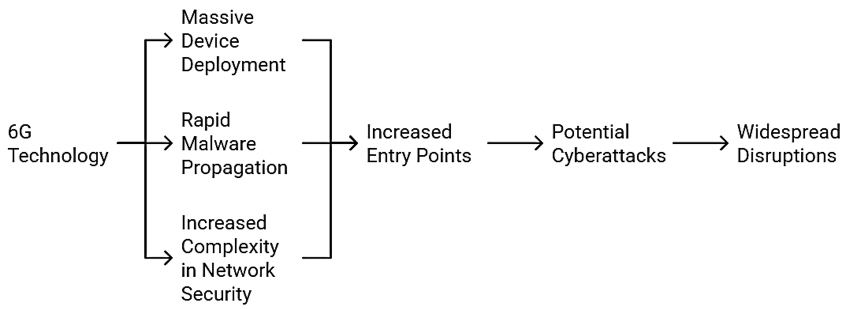

Figure 6: Data Poisoning and Security attacks in 6G

WireGuard was designed to be simpler, faster, and more secure than older protocols. Unlike its predecessors, WireGuard features a minimalistic codebase, making it easier to implement and audit for security flaws. WireGuard quickly gained attention due to its excellent performance and simplicity, making it a popular choice for both developers and users. It became a strong contender against established VPN protocols like OpenVPN and IKEv2, offering both speed and high-level encryption. Naive Bayes is the fast machine learning model which is based on Bayes' theorem. Which predicts the probability of a query belonging to a certain class like malicious or normal, by looking at the various features of data. It works well when features are independent of each other. This model is used for baseline because it works fast and is easy to implement. It works well with simple and structured data. A decision tree is a model that splits data based on maximum information gain. Pruning techniques were applied to reduce the overfitting.

$$h(m) = \sqrt{\frac{t(m)}{f}} + \frac{t(m)}{f},$$

Eq (27)

$$f(w) = \frac{count_w}{totalno.oftokens},$$

Eq (28)

t. This is a specific node in the decision tree.

k. The classes of malicious queries in the SQL injection detection.

p_i. The proportion of the elements belonging to class *I* in the node *T*.

$$Gini\ (t) = 1 - \sum_{i-1}^{k} p_i^2$$ Eq (29)

We optimized the support vector machine (SVM) with a Radial Basis function kernel for non-linear classification. Hyperparameters C regularization parameter and γ kernel coefficient were fine-tuned using the grid search strategy to achieve the optimal performance.

The SVM decision function:

$$f(x) = w^T x + b$$

Eq (30)

W is the weight of the vector.

X represents the feature of a vector as an input sample.

b is the bias term.

An ensemble model combining 1,000 decision trees with each tree trained on the bootstrapped samples. The feature important analysis was conducted to optimize the feature selection. A deep neural Network with hidden layers, each containing 256 neurons. The dropout and batch normalization were used to prevent overfitting and accelerate convergence.

$$\mathbf{f(x) = max(0, x)\ \ (ReLU)}$$

Eq (31)

3.3 Evaluation of Cyber-Physical Systems in the Internet of Things

The stacked ensemble combines ANN's nonlinear learning capacity and SVM's decision boundaries. The ANN outputs are fed into the SVM classifier to refine prediction. Hyperparameter tuning was performed for both components while the cryptography techniques, such as homomorphic encryption and secure multi-party computation (SMC), are widely used in the existing literature of privacy-preserving FL algorithms. In particular, each client encrypts the update before uploading it to the cloud server, where the cloud server decrypts these updates to obtain a new global model. However, these techniques are vulnerable to inference attacks, because each client has to share the gradients accessible to the adversaries. Applying cryptography techniques to the FL systems can also result in major computation overhead, due to the extra operations of encryption and decryption. By examining the memory for suspicious processes and DLLs used also the APIs used for call making the examiner can find important artifacts related to any malware. The main techniques used for the analysis of memory are memory injections and uncovering the persistence mechanism of any malware. As remote work becomes more common, VPNs are a lifeline for businesses, allowing employees to securely access company Networks from anywhere. VPNs create a safe connection over the internet, ensuring that remote workers can access crucial resources without compromising security. Whether employees are working from home or in different locations, VPNs ensure they can access company databases and applications securely, even on public Wi-Fi Networks. Modern attackers employ sophisticated techniques, such as advanced persistent threats and zero-day vulnerabilities, to compromise VPN connections. Future quantum computers could render current encryption algorithms obsolete, necessitating the development of quantum-resistant protocols. Balancing robust encryption with minimal latency remains a challenge, particularly for high-traffic environments. Considering this below are the two modes of Network Security Protocols (a) Transport mode.

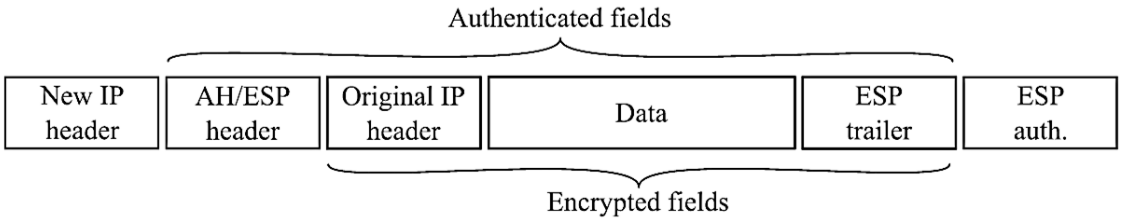

Figure 7: Network Security Protocols Transport mode in Decentralized in 5G and beyond

4. Evaluation Metrics:

The accuracy measures the proportion of the correctly classified instances both true positives and true negatives out of all instances.

The accuracy is defined as:

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN}$$

Eq (31)

TP: True positives which malicious queries are correctly classified as malicious.

TN: True Negative which benign queries correctly classified as benign.

FP: False positive which benign queries incorrectly classified as malicious.

FN: False Negatives which malicious queries incorrectly classified as benign.

The precision calculates how many predicted positive instances were positive.

$$Precision = \frac{TP}{TP+FP}$$

Eq (32)

Recall measures the model's ability to identify the actual positive instances.

$$Recall = \frac{TP}{TP+FN}$$

Eq (33)

The F1 Score is the harmonic mean of the Precision and Recall, Which provides a single metric to balance both.

$$F1 - Score = 2 \cdot \frac{Precision \cdot Recall}{Precision+Recall}$$

Eq (34)

The duration is required for the model to learn from the training dataset while the time taken to make the predictions on the testing dataset, is critical for real-time applications.

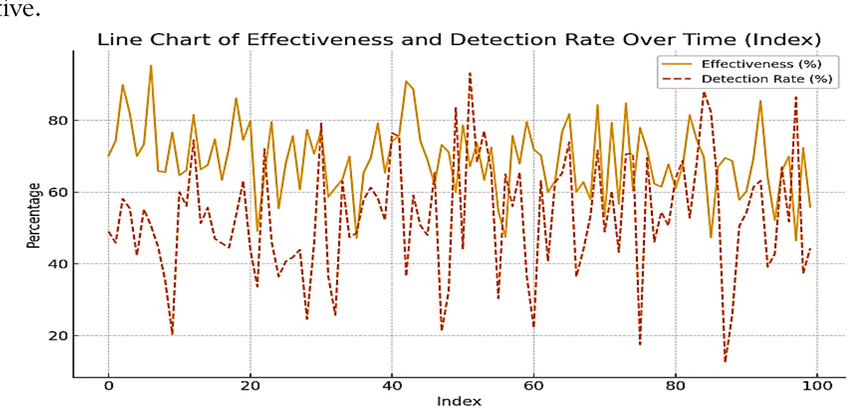

Figure 8: Line Chart of Effectiveness and Detection Rate over Time (Index)

Fig 8 outlines the fluctuations within the effectiveness and discovery rate rates over time, represented by the record on the x-axis. The solid yellow line tracks the effectiveness of security measures, whereas the dashed ruddy line speaks to the location rate.

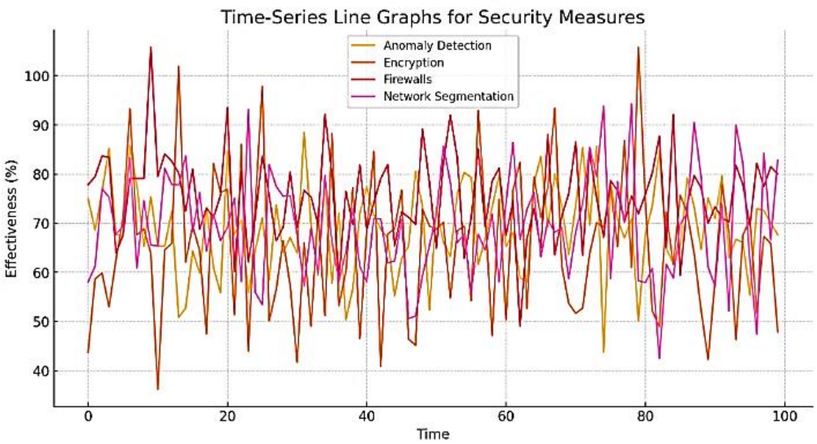

Figure 9: Time Series Line Graphs for Security Measures

In Fig 9, The time-series line graph outlines the adequacy of four different security measures—Anomaly Detection, Encryption, Firewalls, and 6G Network Segmentation—over an indicated period. Each line speaks to the execution of one of the security measures, with viability appearing on the y-axis and time on the x-axis.

$$\mathbf{T-Test: t = \frac{80.5-70.2}{\sqrt{\frac{12.3)^2}{n_1}+\frac{1.44^2}{n_2}}} = 2.56} \quad \text{Eq (35)}$$

$$\mathbf{Chi-Square: \chi^2 = 18.5} \quad \text{Eq (36)}$$

Regression: $\mathbf{Effectiveness = 24.67 + 0.76 \times Detection\ Rate}$ (15)

With $\mathbf{R^2 = 0.76}$ inferring, 76% of the discovery rate accounts for the change in viability.

5. Conclusion and Recommendations

The growing demand for secure and decentralized AI Application in cybersecurity has prompted this investigation of blockchain technology. The potential benefits and drawbacks of utilizing blockchain technology and decentralized AI in cybersecurity, as well as current solutions and practical use cases, have all been examined in this paper, and the analysis has revealed that the integration of blockchain technology and decentralized AI mechanisms holds enormous promise. This research has presented the design and development mechanism and framework enhanced 6G framework ML algorithms.. Machine learning algorithms, computer vision, NLP and advanced control systems are the pivotal methodologies increasing Networks performance. The system provides a capability to determine optimal node and path selection which minimizes Network traffic. The proposed technique obtained 97% throughput, 95% energy efficiency, 96% accuracy, 50% send–to–end delay, and 94% packet delivery ratio. But this kind of technology presents other challenges such as high computational complexity, ethical considerations and safety concerns before it can be exploited to its full potential. Addressing these issues further will depend on future studies and construction to force the field of human Network.

Funding Statement: The authors received no specific funding for this study.

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

References

Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., ... & Choo, K. K. R. (2022). Artificial intelligence in cyber security: research advances, challenges, and opportunities. Artificial Intelligence Review, 1-25.

Hussain, S., Sarwar, N., Ali, A., Khan, H., Din, I., Alqahtani, A. M., ... & Ali, A. (2025). An Enhanced Random Forest (ERF)-based Machine Learning Framework for Resampling, Prediction, and Classification of Mobile Applications using Textual Features. Engineering, Technology & Applied Science Research, 15(1), 19776-19781.

Li, J. H. (2018). Cyber security meets artificial intelligence: a survey. Frontiers of Information Technology & Electronic Engineering, 19(12), 1462-1474.

Gao, J., Wang, H., & Shen, H. (2020). Task failure prediction in cloud data centers using deep learning. IEEE Transactions on Sersvices Computing, 1111–1116. https:// doi.org/10.1109/BigData47090.2019.9006011 ...

Guo, X., Aviles, G., Liu, Y., Tian, R., Unger, B. A., Lin, Y. H. T., & Kampmann, M. (2020). Mitochondrial stress is relayed to the cytosol by an OMA1–DELE1–HRI pathway. Nature, 579(7799), 427–432.

Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. SN Computer Science, 2(3), 173.

Jindal, A., Aujla, G. S., & Kumar, N. (2019). SURVIVOR: A blockchain-based edge-as-a-service framework for secure energy trading in an SDN-enabled vehicle-to-grid environment. Computer Networks, 153, 36–48. Khoramshahi, M., & Billard, A. (2019). A dynamical system approach to task adaptation in physical human-network interaction. Autonomous Networks, 43(4), 927–946.

Nasimi, M., Habibi, M. A., & Schotten, H. D. (2020). arXiv preprint. Platoon–assisted vehicular cloud in VANET: vision and challenges. arXiv preprint arXiv:2008.10928. Neto, P., Sim˜ao, M., Mendes, N., & &Safeea, M. (2019).

Gesture-based human-network interaction for human assistance in manufacturing. The International Journal of Advanced Manufacturing Technology, 101(1), 119–135. Nguyen, N. T., Liu, B. H., Pham, V. T., & Huang, C. Y. (2016). Network under limited mobile devices: A new technique for mobile charging scheduling with multiple sinks. IEEE Systems Journal, 12(3), 2186–2196.

Preeth, S. S. L., Dhanalakshmi, R., & Shakeel, P. M. (2020). An intelligent approach for energy efficient trajectory design for mobile sink based IoT supported wireless sensor Networks. Peer-to-Peer Networking and Applications, 13(6), 2011–2022.

Priyan, M. K., & Devi, G. U. (2018). Energy-efficient node selection algorithm based on node performance index and random waypoint mobility model on the Internet of vehicles. Cluster Computing, 21(1), 213–227.

Ramprasad, L., & Amudha, G. (2014, February). Spammer detection and tagging based user generated video search system—A survey. In International Conference on Information Communication and Embedded Systems (ICICES2014) (pp. 1–5).

Chung, J., Gulcehre, C., Cho, K. & Bengio, Y. Empirical evaluation of gated recurrent neural Networks on sequence modeling. Preprint at arXiv: 1412. 3555 (2014).

Hossain, M. M. et al. Cardiovascular disease identification using a hybrid cnn-lstm model with explainable AI. Inf. Med. Unlocked 42, 101370 (2023).

Ahsan, M. M. et al. Enhancing monkeypox diagnosis and explanation through modified transfer learning, vision

Castiglioni, I. et al. Ai applications to medical images: From machine learning to deep learning. Physica Med. 83, 9–24 (2021).

H. Khan, I. Uddin, A. Ali, M. Husain, "An Optimal DPM Based Energy-Aware Task Scheduling for Performance Enhancement in Embedded MPSoC", Computers, Materials & Continua., vol. 74, no. 1, pp. 2097-2113, Sep. 2023

Khan, S., Ullah, I., Khan, H., Rahman, F. U., Rahman, M. U., Saleem, M. A., ... & Ullah, A. (2024). Green synthesis of AgNPs from leaves extract of Saliva Sclarea, their characterization, antibacterial activity, and catalytic reduction ability. Zeitschrift für Physikalische Chemie, 238(5), 931-947.

U. Hashmi, S. A. ZeeshanNajam, "Thermal-Aware Real-Time Task Schedulabilty test for Energy and Power System Optimization using Homogeneous Cache Hierarchy of Multi-core Systems", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 4, pp. 442-452, Mar. 2023

Y. A. Khan, F. Khan, H. Khan, S. Ahmed, M. Ahmad, "Design and Analysis of Maximum Power Point Tracking (MPPT) Controller for PV System", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 1, pp. 276-288, May. 2019

Ali, M., Khan, H., Rana, M. T. A., Ali, A., Baig, M. Z., Rehman, S. U., & Alsaawy, Y. (2024). A Machine Learning Approach to Reduce Latency in Edge Computing for IoT Devices. Engineering, Technology & Applied Science Research, 14(5), 16751-16756.

Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.

Khan, A. Ali, S. Alshmrany, "Enery-Efficient Scheduling Based on Task Migration Policy Using DPM for Homogeneous MPSoCs", Computers, Materials & Continua., vol. 74, no. 1, pp. 965-981, Apr. 2023

Abdullah, M., Khan, H., Shafqat, A., Daniyal, M., Bilal, M., & Anas, M. (2024). Internet of Things (IoT's) in Agriculture: Unexplored Opportunities in Cross–Platform. Spectrum of engineering sciences, 2(4), 57-84.

Y. A. Khan, M. Ibrahim, M. Ali, H. Khan, E. Mustafa, "Cost Benefit Based Analytical Study of Automatic Meter Reading (AMR) and Blind Meter Reading (BMR) used by PESCO (WAPDA)", In 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-7, Aug. 2020

Fakhar, M. H., Baig, M. Z., Ali, A., Rana, M. T. A., Khan, H., Afzal, W., ... & Albouq, S. (2024). A Deep Learning-based Architecture for Diabetes Detection, Prediction, and Classification. Engineering, Technology & Applied Science Research, 14(5), 17501-17506.

Y. A. Khan, "A high state of modular transistor on a 105 kW HVPS for X-rays tomography Applications", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 1-6, Jun. 2019

Khan, S. Ahmad, N. Saleem, M. U. Hashmi, Q. Bashir, "Scheduling Based Dynamic Power Management Technique for offline Optimization of Energy in Multi Core Processors", Int. J. Sci. Eng. Res., vol. 9, no. 12, pp. 6-10, Dec. 2018

H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, A. Saleem, "Performance Evaluation for Secure DES-Algorithm Based Authentication & Counter Measures for Internet Mobile Host Protocol", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 181-185, July. 2018

Y. A. Khan, "Enhancing Energy Efficiency in Temperature Controlled Dynamic Scheduling Technique for Multi Processing System on Chip", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 46-53, Jan. 2019

Khan, K. Janjua, A. Sikandar, M. W. Qazi, Z. Hameed, "An Efficient Scheduling based cloud computing technique using virtual Machine Resource Allocation for efficient resource utilization of Servers", In 2020 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-7, Apr. 2020

Rahman, M. U., Khan, S., Khan, H., Ali, A., & Sarwar, F. (2024). Computational chemistry unveiled: a critical analysis of theoretical coordination chemistry and nanostructured materials. Chemical Product and Process Modeling, 19(4), 473-515.

Naz, H. Khan, I. Ud Din, A. Ali, and M. Husain, "An Efficient Optimization System for Early Breast Cancer Diagnosis based on Internet of Medical Things and Deep Learning", Eng. Technol. Appl. Sci. Res., vol. 14, no. 4, pp. 15957–15962, Aug. 2024

Akmal, I., Khan, H., Khushnood, A., Zulfiqar, F., & Shahbaz, E. (2024). An Efficient Artificial Intelligence (AI) and Blockchain-Based Security Strategies for Enhancing the Protection of Low-Power loT Devices in 5G Networks. Spectrum of engineering siences, 2(3), 528-586.

H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Dec. 2018

Waleed, A. Ali, S. Tariq, G. Mustafa, H. Sarwar, S. Saif, I. Uddin, "An Efficient Artificial Intelligence (AI) and Internet of Things (IoT's) Based MEAN Stack Technology Applications", Bulletin of Business and Economics (BBE)., vol. 13, no. 2, pp. 200-206, July. 2024

Naveed, A., Khan, H., Imtiaz, Z., Hassan, W., & Fareed, U. (2024). Application and Ethical Aspects of Machine Learning Techniques in Networking: A Review. Spectrum of engineering sciences, 2(3), 455-501.

Shah, S. Ahmed, K. Saeed, M. Junaid, H. Khan, "Penetration testing active reconnaissance phase–optimized port scanning with nmap tool", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-6, Nov. 2019

Y. A. Khan, "A GSM based Resource Allocation technique to control Autonomous Networkic Glove for Spinal Cord Implant paralysed Patients using Flex Sensors", Sukkur IBA Journal of Emerging Technologies., vol. 3, no. 2, pp. 13-23, Feb. 2020

Hassan, H. Khan, I. Uddin, A. Sajid, "Optimal Emerging trends of Deep Learning Technique for Detection based on Convolutional Neural Network", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 264-273, Nov. 2023

Khan, A. Yasmeen, S. Jan, U. Hashmi, "Enhanced Resource Leveling Indynamic Power Management Techniqueof Improvement In Performance For Multi-Core Processors" ,Journal of Mechanics of Continua and Mathematical Sciences., vol. 6, no. 14, pp 956-972, Sep. 2019

Javed, M. A., Anjum, M., Ahmed, H. A., Ali, A., Shahzad, H. M., Khan, H., & Alshahrani, A. M. (2024). Leveraging Convolutional Neural Network (CNN)-based Auto Encoders for Enhanced Anomaly Detection in High-Dimensional Datasets. Engineering, Technology & Applied Science Research, 14(6), 17894-17899.

Khan, I. Ullah, M. U. Rahman, H. Khan, A. B. Shah, R. H. Althomali, M. M. Rahman, "Inorganic-polymer composite electrolytes: basics, fabrications, challenges and future perspectives", Reviews in Inorganic Chemistry., vol. 44, no. 3, pp. 1-2, Jan. 2024

Khan, H., Ali, A., & Alshmrany, S. (2023). Energy-Efficient Scheduling Based on Task Migration Policy Using DPM for Homogeneous MPSoCs. Computers, Materials & Continua, 75(1).

Y. A. Khan, U. Khalil, H. Khan, A. Uddin, S. Ahmed, "Power flow control by unified power flow controller",Engineering, Technology & Applied Science Research., vol. 9, no. 2, pp. 3900-3904, Feb. 2019

Abdullahi, M., Baashar, Y., Alhussian, H., Alwadain, A., Aziz, N., Capretz, L. F., & Abdulkadir, S. J. (2022). Detecting cybersecurity attacks in internet of things using artificial intelligence methods: A systematic literature review. Electronics, 11(2), 198.

Lin, K., Li, Y., Sun, J., Zhou, D., & Zhang, Q. (2020). Multi-sensor fusion for a body sensor Network in a medical human-network interaction scenario. Information Fusion, 57, 15–26. Manogaran, G., Baskar, S., Hsu, C. H., Kadry, S. N., Sundarasekar, R., Kumar, P. M., & Muthu, B. A. (2021).

FDM: Fuzzy-optimized Data Management Technique for Improving Big Data Analytics. IEEE Transactions on Fuzzy Systems, 29(1), 177–185. Manogaran, G., Shakeel, P. M., Priyan, R. V., Chilamkurti, N., & Srivastava, A. (2019). Ant colony optimization-induced route optimization for enhancing the driving range of electric vehicles. International Journal of Communication Systems, e3964. https://doi.org/10.1002/dac.3964.