Ingénierie des Systèmes d'Information
Vol. 30, No. 5, May, 2025, pp. 1259-1269
Journal homepage: http://iieta.org/journals/isi

A Firefly-Based Optimization Algorithm for Secure 5G-IoT Cyber-Physical Systems

Smitha Parappurathu Bahulayan*, Periyasamy Kavipriya

Department of Electronics and Communication Engineering, Sathyabama Institute of Science and Technology, Chennai 600119, India

Corresponding Author Email: smithapb09@gmail.com

https://doi.org/10.18280/isi.300513

Received: 17 February 2025
Revised: 15 April 2025
Accepted: 23 April 2025
Available online: 31 May 2025

Keywords: *cyber-physical systems, IoT security, bio-inspired optimization algorithms, intrusion detection system, resource allocation, anomaly detection, latency reduction, secure data transmission*

ABSTRACT

The interaction between cyber-physical systems (CPS) and 5G-enabled Internet of Things (IoT) networks introduce critical challenges related to security, resource efficiency, and simulated data threat detection. Existing security mechanisms struggle to adapt to the dynamic and heterogeneous nature of these network infrastructures. To address these challenges, this study proposes a Firefly Optimization Algorithm (FOA) inspired by swarm-based firefly intelligence to enhance security, resource allocation, and energy efficiency in CPS-IoT networks. The proposed approach integrates an enhanced attraction-based motion mechanism and an adaptive mutation strategy to dynamically adjust security parameters, optimizing intrusion detection, anomaly mitigation, and encryption complexity. Empirical evaluations demonstrate that FOA outperforms existing methods in terms of detection accuracy, latency reduction, and computational efficiency, ensuring a robust and adaptive security framework for next-generation CPS systems. This research contributes to the development of intelligent, adaptive, and sustainable security solutions for 5G-enabled IoT ecosystems.

1. INTRODUCTION

Cyber-physical systems (CPS) are widely used for automating tasks enabling even basic hardware to function as smart devices. These devices typically have low power consumption, limited storage capacity, and minimal computational capability. The evolution of electronic systems has led to a new generation that integrates physical structures with computational methods. A computational method consists of a set of instructions that execute various operations on a physical system [1]. It includes network-connected computers that monitor and control different physical processes within a device. This automation reduces human intervention, minimizing errors and enhancing system efficiency. Examples of CPS applications include smart automobiles, smart homes, and intelligent devices. In the context of CPS, the Internet of Things (IoT) is driving advancements across multiple industries, contributing to the development of smart cities and intelligent residences [2].

CPS has become feasible due to internet connectivity and advancements in communication technologies, impacting industries ranging from manufacturing to research and development. While earlier generations of electrical devices featured automated processes, modern CPS systems are more dynamic, goal-oriented, and internet-connected, allowing for continuous interaction with devices from any location [3]. In a smart home system, automated air conditioning units can sense external temperatures and adjust accordingly. These systems can detect human presence, monitor environmental conditions, and analyse data to optimize room temperature settings for user comfort. As a result, CPS enhances decision-making capabilities in simulated data, making the system more adaptive and intelligent [4]. Figure 1 illustrates the components of CPS, detailing their implementation across various applications. The CPS architecture consists of three primary components: Things (Devices and Sensors); Applications & Data Analysis; and Manufacturing & Infrastructure. These components define the structural and functional aspects of CPS, enabling efficient automation and intelligent control across multiple domains [5].

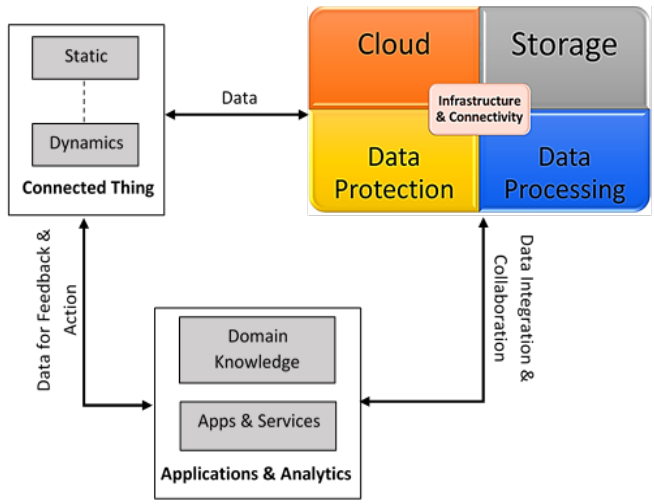

Figure 1. Components of CPS

Connected objects or artifacts collect information about their environment. Depending on their nature, these objects may operate in either static or dynamic contexts. Static objects do not change their behavior in response to environmental variations; strictly follow predefined instructions. Dynamic objects are designed to adapt to simulated data conditions allowing them to modify their operations accordingly [6]. The two fundamental requirements for these objects are the ability to collect data and transmit it to CPS applications for further processing. Beyond providing processing power and data storage, CPS component enables the integration of various smart processing methods such as databases, cloud storage, and other similar technologies [7]. Analytical and software applications leverage CPS-generated data to support informed decision-making, while also offering users enhanced features, functionalities, and capabilities. One of the most advanced connectivity solutions in this domain is 5G, which aims to achieve ultra-low latency, high reliability, flexibility, and security. In terms of manufacturing efficiency, production system adaptability, and reconfiguration, 5G is expected to drive smart manufacturing facilities and other industrial settings [8].

A key challenge in this transformation is the need for deep integration of Operational Technology (OT) and Information Technology (IT). This makes the transition to Industry 4.0 (I4.0) for a specific business, region, or factory a complex, multidisciplinary task. Numerous frameworks and approaches have been proposed to support transition, primarily by developing roadmaps based on technological readiness and digitization levels [9]. The primary goal of these frameworks is to assist industrial manufacturing companies in assessing their digital maturity levels and guiding their digitalization strategies through structured evaluation stages at each phase of the process. These models emphasize that reliable wireless communication is the key enabler of system interconnectivity ensuring seamless integration of all manufacturing resources [10]. This facilitates the implementation of both OT and advanced IT solutions such as mobile autonomous robots, matrix manufacturing, big data, and Artificial Intelligence (AI). While some frameworks consider communication-specific features, particularly in relation to industrial application requirements, they often lack detailed insights into how specific wireless communication methods perform in particular industrial environments. Wi-Fi remains the dominant connectivity choice in manufacturing settings; the wireless landscape consists of multiple technologies with diverse characteristics, requiring careful selection based on industry-specific demands [11].

Wi-Fi operates on unlicensed frequency bands, where the electromagnetic spectrum is shared with other networks. As a result, its efficiency and reliability can vary significantly depending on the specific environment and application scenario. Under such conditions, high dependability and Quality-of-Service (QoS) requirements may not always be met, as network access for transmissions requires contention-based competition [12]. With the initial commercial 5G networks now deployed for industrial applications is crucial to ensure that the full potential of 5G is properly evaluated and leveraged within manufacturing environments. 5G promises higher reliability and improved efficiency; however, there is a noticeable lack of comprehensive use case analyses, performance evaluations, and recommendations regarding the integration of wireless technologies into various I4.0 processes and broader digital transformation initiatives. To enhance the security of IoT networks against cyberattacks, the development of Intrusion Detection Systems (IDS) as an additional line of defense is essential. Machine learning (ML)-based Intrusion Detection Systems have been widely studied to protect IoT devices from unauthorized access [13]. Several research efforts have explored intrusion detection techniques for security systems, Wireless Sensor Networks (WSNs), ad hoc networks, and cloud-based IoT environments. The unique characteristics of IoT ecosystems present challenges for existing intrusion detection methods make insufficient or inefficient in safeguarding connected devices. Some of these challenges include limited bandwidth, energy constraints, diverse device types, and the pervasive nature of IoT networks [14]. ML has gained prominence for its ability to detect security threats in IoT networks effectively. Existing network monitoring techniques are often unsuitable for WSNs due to their restricted computational and transmission capabilities. ML models for traffic analysis are being extensively researched for WSN-based IDS [15]. As WSNs continue to expand in size and user base generate high-dimensional traffic data making it difficult for existing ML models to perform feature extraction and maintain detection accuracy. These limitations may fail to address the specific security requirements of WSN environments. By leveraging ML-based approaches, computational overhead can be reduced, and a better understanding of traffic anomalies can be achieved ultimately improving IDS accuracy compared to existing methods [16].

1.1 Problem statement

The integration of CPS with 5G-enabled IoT networks has enabled simulated data exchange and low-latency communication across domains such as smart cities, healthcare, and industrial automation. The large-scale deployment of heterogeneous and resource-constrained devices increases exposure to cyber threats, rendering existing static security measures ineffective. Key challenges include secure data transmission, simulated data threat detection, and lack of adaptive security frameworks. To ensure confidentiality, integrity, and availability in these critical infrastructures, there is a pressing need for intelligent, scalable, and energy-efficient security architectures that combine encryption, access control, and AI-driven detection techniques.

1.2 Motivation

CPS plays a vital role in mission-critical applications, where security failures can lead to severe consequences. The convergence of CPS and 5G-IoT enables benefits like massive MTC, URLLC, and advanced data processing but also opens avenues for advanced persistent threats and unauthorized access. The dynamic nature of these systems demands adaptive solutions beyond existing security models. Innovations such as blockchain-based authentication, AI-powered anomaly detection, and quantum-resistant encryption are essential to safeguard sensitive data and maintain trust. Developing such a robust framework is crucial to ensuring reliable, secure, and uninterrupted operation of next-generation intelligent environments.

2. RELATED WORKS

The deployment of small cells is pivotal for enabling ultra-dense 5G networks, particularly in intelligent medical applications that demand high data rates (e.g., remote surgeries ranging from 137 Mbps to 1.6 Gbps) [17]. Small cells femtocells, picocells, and microcells are low-power nodes with coverage areas from a few meters to a few kilometers. Femtocells, suitable for hospitals or homes, enhance signal quality and availability. Picocells extend network coverage in confined areas, while microcells support up to 2,000 users across a 2 km radius [18]. Compared to macrocells (20-mile coverage), small cells offer improved spectral efficiency and localized service shown in Figure 2.

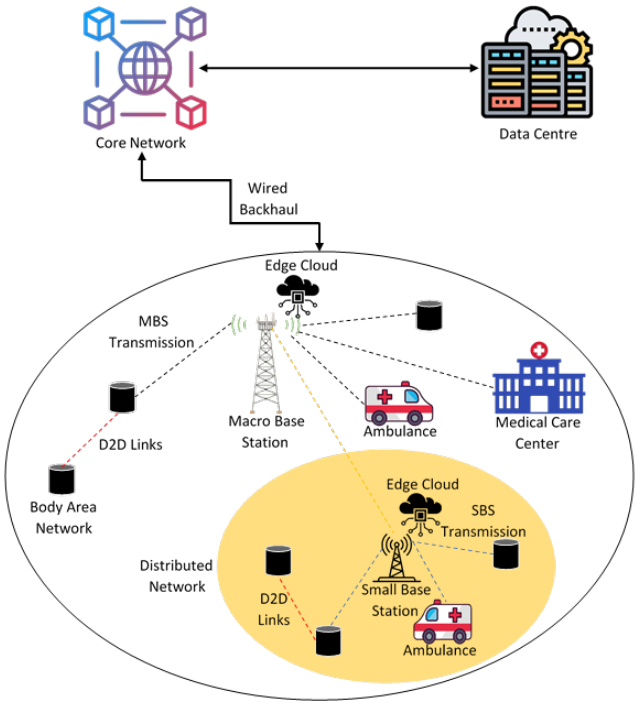

Figure 2. 5G based smart healthcare architecture

A dual-layer architecture where macrocell base stations manage control signaling at lower frequencies and small cells handle high-speed data at higher frequencies enables efficient and flexible 5G coverage. This separation between the user and control planes allows User Equipment (UE) to maintain simultaneous connectivity to both layers, facilitating high-throughput and mobility [19, 20]. CPS and Industry 4.0 environments face complex operational risks that require multi-level risk assessment strategies. Robust security frameworks integrating encrypted communications have been proposed for critical infrastructures and smart cities [21]. Studies suggest adapting transmission characteristics, such as beam-shaping and block length, to optimize covert communication efficiency while minimizing risk exposure. With increasing automation and remote surveillance, there is a growing demand for reliable authentication protocols to ensure system integrity [22].

Energy consumption remains a critical limitation in IoT, given the battery-constrained nature of many devices. Several works emphasize the importance of energy-efficient protocols, including optimized routing and node placement [23]. Cross-layer optimization and power-aware routing strategies have been proposed to minimize energy use while maintaining reliable communication. Lightweight encryption and low-power authentication mechanisms have been introduced to enhance security without significantly increasing computational overhead [24]. Security in 5G-enabled IoT and CPS networks has garnered significant attention. Traditional approaches use Intrusion Detection Systems, cryptographic algorithms, and authentication mechanisms. To improve trust and decentralization, blockchain-based identity verification and distributed trust management platforms have been proposed [25].

Advanced methods such as federated learning and AI-based anomaly detection preserve privacy while enabling simulated data threat response. Deep reinforcement learning (DRL) algorithms have shown promise in adapting to evolving cyber threats. Meanwhile, SDN and Zero Trust Architectures (ZTA) are gaining traction for enabling network segmentation and precise access control [26, 27]. Emerging concerns about quantum threats have led to the exploration of Post-Quantum Cryptography (PQC), ultra-lightweight encryption, and homomorphic encryption to secure resource-constrained devices [28]. Despite progress, scalability, latency, and hardware limitations remain challenges, underlining the need for integrated, low-latency, and energy-aware security frameworks in future CPS deployments.

3. MATERIALS AND METHODS

3.1 Problem formulation for secure CPS in 5G-enabled IoT networks

CPS in 5G-enabled IoT networks face significant security threats due to their distributed nature, heterogeneous devices, and simulated data communication requirements. Existing security mechanisms struggle with high latency, scalability, and dynamic attack surfaces. The problem can be mathematically formulated as follows:

Network model: Let N denote the number of lot devices in the CPS network, where each device $D_x(x = 1,2, \dots, N)$ connected via a SG-enabled infrastructure. The communication between devices and edge servers follows:

$$C_{x,y}(t) = B.log_2(1 + SNR_{x,y}(t)) \quad (1)$$

where, $C_{x,y}(t)$ is the channel capacity between device x and server y at time t.B is the channel bandwidth. $SNR_{x,y}(t)$ is the Signal-to-Noise Ratio (SNR) between device x and server y.

Attack model: Security threats in CPS can be classified into confidentiality, integrity, and availability attacks. The probability of a successful attack P_{attack} can be expressed as:

$$P_{\text{attack}} = 1 - (1 - P_{intrusion})(1 - P_{data\_tamper})(1 - P_{DDoS}) \quad (2)$$

where, $P_{intrusion}$ represents the probability of unauthorized access. P_{data_tamper} represents the probability of malicious data modification. P_{DDoS} represents the probability of a Distributed Denial-of-Service (DDoS) attack.

Security Optimization Objective: The security mechanism must optimize detection rate D_r minimize false positives FP, and maintain a low energy consumption E. The objective function is formulated as:

$$\max_S [\alpha D_r - \beta FP - \gamma E] \quad (3)$$

where, S is the security mechanism. α, β, γ are weighting factors for accuracy, false positives, and energy consumption, respectively.

Secure Data Transmission: To ensure secure data transmission, encryption is applied using an optimized cryptographic function E_{sec}:

$$E_{sec} = H(M) \oplus K \tag{4}$$

where, *H(M)* is the cryptographic hash of message *M*. *K* is the secret key. $\oplus$ represents the XOR operation.

Resource Allocation for Secure CPS: The resource allocation problem for ensuring security while minimizing latency L is formulated as:

$$\min_{R} \sum_{x=1}^{N} (W_x . L_x + \lambda S_x) \tag{5}$$

where, W_x is the weight factor for latency-sensitive devices; L_x is the latency for device x, λ is the security weight factor; S_x represents the security level of device x.

This formulation provides a foundation for designing robust security mechanisms in 5G-enabled CPS by optimizing detection accuracy, resource utilization, and secure communication while mitigating security risks effectively.

3.2 Dataset description

A variety of variables that record network traffic in simulated data, device behavior, and security-related factors make up the dataset for Secure CPS in 5G-enabled IoT Networking shown in Table 1. It contains device-specific information like Device ID and Device Type provide activity accountability and temporal information (Timestamp) to monitor occurrences. Analysis of interaction effectiveness and the detection of possible cyber threats are aided by network-related characteristics such as network activity, protocol size, procedure, delay, nervousness, and loss of packets. CPU Usage, Memory Usage, and Battery Level offer valuable information on how much computing power IoT devices are used for identifying anomalous activity brought on by hardware malfunctions or cyberattacks. The dataset includes an assault Type to categorize different safety hazards and an Anomaly Flag to indicate if a recorded occurrence is typical or indicative of an assault.

This dataset can be used to train machine learning models for IDS allowing simulated data threat analysis and anomaly detection in 5G-enabled IoT networks shown in Table 2.

Table 1. Dataset description

Attribute	Description	Data Type
Timestamp	Time of data capture in the IoT network	DateTime
Device ID	Unique identifier for IoT/CPS device	String
Device Type	Type of IoT device (e.g., sensor, actuator, gateway)	Categorical
Network Traffic	The volume of data transferred (in MB/s)	Float
Packet Size	Size of transmitted packets (in bytes)	Integer
Protocol	Communication protocol used	Categorical
Latency (ms)	End-to-end network delay in milliseconds	Float
Jitter (ms)	Variation in packet delay	Float
Packet Loss (%)	Percentage of lost packets in transmission	Float
CPU Usage (%)	Device computational load	Float
Memory Usage (%)	RAM utilization of the device	Float
Battery Level (%)	The power status of IoT device	Float
Anomaly Flag	A label indicating normal (0) or attack (1)	Binary
Attack Type	Type of cyberattack (if applicable)	Categorical

Table 2. Sample data

Timestamp	Device ID	Network Traffic (kbps)	Packet Size (bytes)	Protocol	Latency (ms)	Jitter (ms)	Packet Loss (%)	CPU Usage (%)	Memory Usage (%)	Battery Level (%)	Anomaly Flag	Attack Type
2025-02-10 12:01:23	ID_001	1200	512	TCP	15	2.3	0.1%	35	60	90	0	Normal
2025-02-10 12:02:10	ID_002	2500	1024	UDP	30	5.5	1.2%	65	75	80	1	DDoS
2025-02-10 12:03:45	ID_003	800	256	TCP	10	1.0	0.0%	20	50	95	0	Normal
2025-02-10 12:04:20	ID_004	1800	768	TCP	25	4.2	0.5%	50	65	85	1	MITM
2025-02-10 12:05:05	ID_005	600	128	UDP	12	2.0	0.2%	15	40	99	0	Normal

3.3 System design

Proposed method is intended to handle the difficulties brought about by the growing intricacy and interdependence of CPS, where existing safety precautions would not be sufficient to handle dynamic and changing security threats. The strategy leverages the FOA to optimize several security factors such as allocation of resources, intrusion prevention, and information encryption across IoT devices in a 5G setting shown in Figure 3. This FOA proposed method convergence rate and resilience to local minima is well-known for its ability to identify optimum solutions in intricate search environments. For large-scale IoT systems wherein safety must be flexible and sensitive to current information patterns and methods of attack, this enhancement is essential. To identify the best configuration for managing resources, internet access, and

secure transmission of information, the program continuously modifies the system's settings by mimicking the flashing actions of Firefly. Proposed method can strengthen the adaptability of 5G-enabled CPS against new cyber threats by allowing the network to dynamically detect vulnerabilities improve safety measures, and guarantee safe communication between the physical and cyber elements of IoT networks.

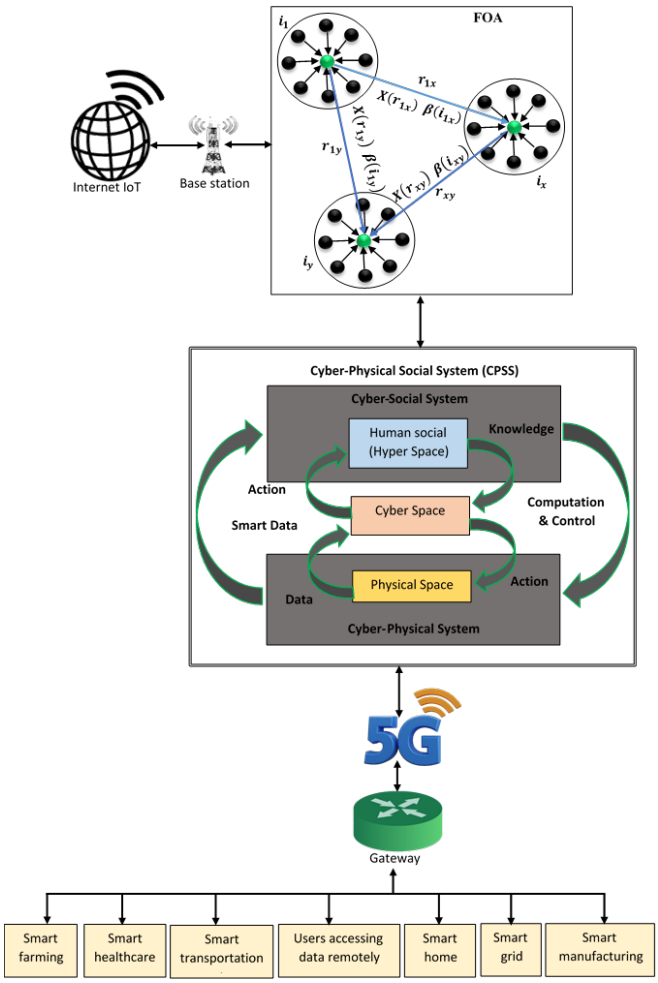

Figure 3. Proposed architecture

3.4 Pre-processing in secure 5G-enabled IoT communication systems

Pre-processing is an essential step in data analysis, particularly in complex communication systems like secure 5G-enabled IoT networks. In this context, pre-processing ensures that the raw data collected from IoT devices is clean, relevant, and formatted in a way that can be effectively used for security-related tasks such as intrusion detection, resource allocation, and encryption. Pre-processing typically involves several steps, including data cleaning, normalization, feature extraction, and dimensionality reduction.

Data cleaning: It involves handling missing, noisy, or inconsistent data. This is crucial in ensuring that any further analysis or optimization does not rely on incomplete or corrupted data. In 5G IoT systems, missing values in the collected sensor data can be filled using techniques like interpolation or imputation.

Data cleaning (imputation): Let i_x represent the raw data vector, and i_x^{cleaned} the cleaned data after handling missing values:

$$i_x^{\text{cleaned}} = \begin{cases} i_x & \text{if } i_x \text{ is available} \\ \frac{\sum_{y=1}^{n} i_y}{n} & \text{if } i_x \text{ is missing, replace with average value of the dataset} \end{cases} \quad (6)$$

where, n is the number of available data points in the dataset.

Normalization: In 5G IoT networks, loT device data such as signal strength, bandwidth usage, and power consumption may have varying scales.

$$i_{norm} = \frac{i_x - \min(i)}{\max(i) - \min(i)} \quad (7)$$

where, i_x is the raw value of the feature, min(i) and max(i) are the minimum and maximum values of the feature in the dataset.

Feature extraction: In secure 5G IoT communication, features related to network traffic, packet size, and transmission power might be relevant for intrusion detection or resource allocation. Principal Component Analysis (PCA) is used to extract the most important features by reducing the dimensionality of the data while retaining most of the variance. PCA transforms the data into principal components by solving the eigenvalue problem:

$$I_{new} = IW \quad (8)$$

where, I is the original dataset; W is the matrix of eigenvectors (principal components); I_{new} is the transformed data with reduced dimensions.

Dimensionality reduction: In secure 5G IoT systems, dimensionality reduction can help in improving the efficiency of security algorithms, particularly for simulated data IDS and resource allocation.

$$C = \sum_{x,y} \left(P_{xy} log \frac{P_{xy}}{q_{xy}} \right) \quad (9)$$

where, P_{xy} is the probability distribution of pairs of points in the high-dimensional space. q_{xy} is the probability distribution of pairs of points in the low-dimensional space (after dimensionality reduction), C is the Kullback-Leibler divergence, which is minimized to reduce dimensionality.

Data transformation: Data transformation techniques, such as Fourier Transform or Wavelet Transform, are sometimes applied to communication signals to convert data from time-domain to frequency-domain. This helps in detecting anomalies or irregular patterns, especially in network traffic data. The DFT of a signal i(t) can be expressed as:

$$I(f) = \sum_{n=0}^{N-1} i(n) e^{-y2\pi f n/N} \quad (10)$$

where, $I(f)$ is the frequency-domain representation of the signal, $i(n)$ is the signal in the time domain; Secure SG IoT data for analysis and optimization. By applying data cleaning, normalization, feature extraction, dimensionality reduction, and transformation techniques, the raw data can be transformed into a more useful format, leading to enhanced performance of security algorithms such as intrusion detection, resource allocation, and encryption.

Cybersecurity professionals constantly face new attacks that

exploit software vulnerabilities. Building collective resilience against IoT privacy and security concerns requires effective information sharing to fully realize the potential of IoT. This study highlights key issues and vulnerabilities in sectors such as healthcare and transportation, emphasizing the need for robust IoT cybersecurity implementation strategies in smart cities shown in Figure 4.

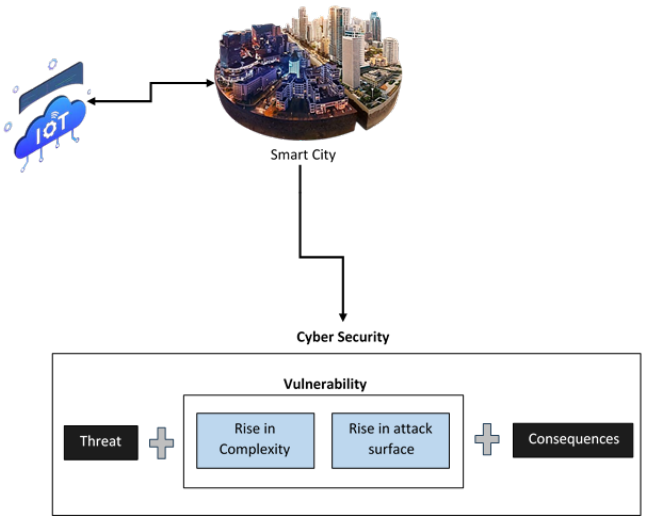

Figure 4. Smart cities infrastructure risk parameters

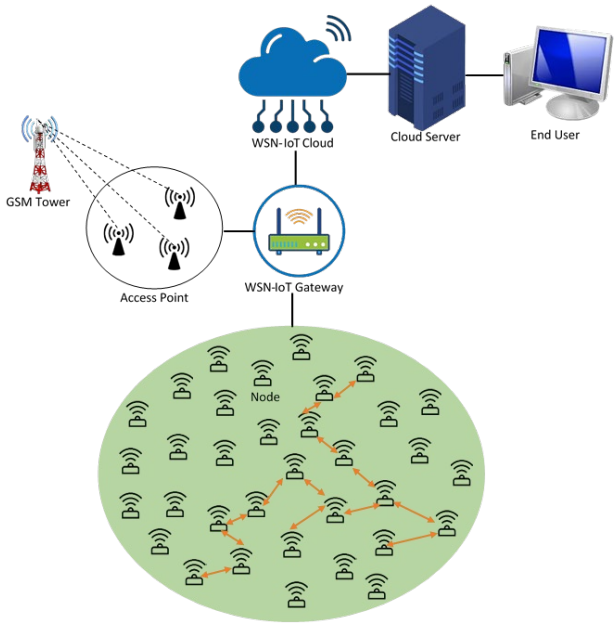

Figure 5. Network model of FOA with WSN-IoT

The proposed FOA iteratively applies to guide fireflies within the search space toward better solutions. Regardless of the type of optimization problem, the algorithm effectively balances attraction toward brighter solutions with random search enabling fireflies to explore the search space efficiently and converge toward optimal or near-optimal conditions. This combination of exploration and attraction allows FOA to solve complex optimization problems and identify effective solutions across various real-world applications. Figure 5 illustrates the FOA network framework using WSN-IoT. The Firefly Algorithm assessor performs several tasks, including constructing feature subsets from fireflies' binary solutions, training neural network models to detect intrusions in the WSN-IoT framework using these subsets, evaluating performance metrics such as precision or AUC to measure model efficiency assigning fitness values based on these metrics to guide optimization and iteratively adjusting firefly movement. This analysis process steers the algorithm toward feature subsets that enhance IDS accuracy and improve WSN-IoT security.

Position update (movement of fireflies): Each firefly moves towards a brighter firefly (one with a better objective value). The movement is influenced by two factors: Attraction to brighter fireflies (better solutions) and Random motion.

The position of the xth firefly is updated using the Eq. (11).

$$i_x(t+1) = i_x(t) + \beta . e^{-\gamma r^2} . \left(i_y(t) - i_x(t)\right) + \alpha . \epsilon_x(t) \quad (11)$$

where, $i_x(t)$ is the position of the xth firefly at time t; $i_y(t)$ is the position of the yth firefly (a brighter firefly). β is the attractiveness of firefly x towards firefly y is typically a function of the brightness and distance. γ is the absorption coefficient (controls how quickly the light intensity diminishes with distance). r is the distance between fireflies x and y, given by $r = \left|\left|i_x - i_y\right|\right|$. α is the randomization parameter (used to introduce randomness in the movement). ϵ_x(t) is a random vector, typically drawn from a uniform distribution, to provide randomness to the movement.

Brightness calculation (objective function): The brightness of a firefly is determined by the value of the objective function $f(i_x)$ and the firefly with a lower (or higher, depending on the problem) objective function value is considered brighter. In the case of optimization problems, the brightness X_x of the xth firefly is defined as:

$$X_x = f(i_x) \quad (12)$$

where, $f(i_x)$ is the objective function or fitness value of the xth firefly.

Attractiveness function: The attractiveness of a firefly is inversely related to the distance between two fireflies. This relationship is commonly modelled using an exponential function:

$$\beta(r) = \beta_0 e^{-\gamma r^2} \quad (13)$$

where, β_0 is the attractiveness at the origin (when r = 0), γ is the absorption coefficient controls the rate of decrease of attractiveness with distance. r is the distance between the two fireflies.

Distance between fireflies: The distance between two fireflies in the search space is typically calculated using the Euclidean distance:

$$r = \left\|i_x - i_y\right\| = \sqrt{\sum_{k=1}^{d} \left(i_{x,k} - i_{y,k}\right)^2} \quad (14)$$

where, i_x and i_y are the positions of two fireflies x and y. d is the dimension of the problem (number of variables). $i_{x,k}$ and $i_{y,k}$ are the k-th coordinates of fireflies x and y.

Randomization: The random movement of fireflies adds diversity to the population and helps in avoiding premature

convergence. The randomization is modeled as:

$$i_x(t+1) = i_x(t) + \alpha.\epsilon_x(t) \quad (15)$$

where, a is the randomization parameter and $\epsilon_x(t)$ is a random vector, typically uniformly distributed in the range [-1, 1].

FOA is a population-based optimization technique inspired by nature can be used for solving complex optimization problems. The algorithm's behaviour is governed by attraction towards brighter fireflies and random movements.

Figure 6 illustrates how multimedia information from sensor node N1 is sent to sensor node N5 which is chosen using the FOA method (i.e., the proposed FRO method chooses "N5" as the resource-optimized sensor node out of sensor nodes N2, N3, and N5). Until the mixed-media information arrives successfully at the target node "N12" this procedure is continued. As can be seen in Figure 6, the resource-optimized route paths N1, N5, F8, and N12 have been chosen. As a result, proposed FOA approach attain greater throughput. The FOA for secure CPS in 5G-enabled IoT networks algorithm is as follows.

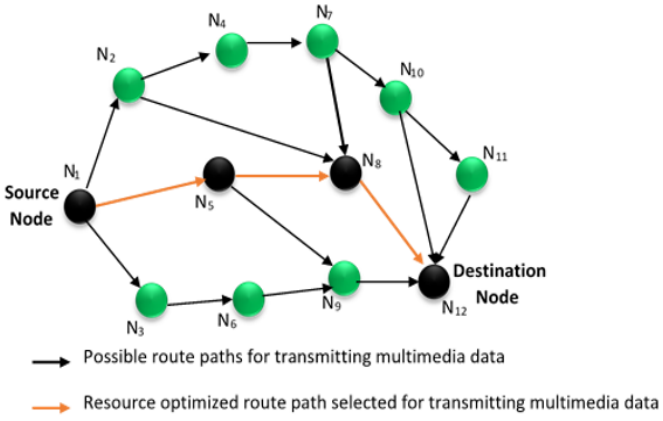

Figure 6. Resource optimized route path using FOA algorithm

In 5G-enabled IoT systems, the FOA is intended to enhance the safety, detection of intrusions, and optimization of resources of CPS. By adding adaptive mobility, dynamic light level updates, and an improved mutation process to avoid local optima capture, it outperforms the existing Firefly Algorithm (FA). Notations used in proposed algorithm is shown in Table 3.

Table 3. Notations

Symbol	Description
N	Number of fireflies (candidate security configurations)
I_x	Position of firefly x representing a solution
X_x	Light intensity (fitness value) of firefly x
β_0	Initial attractiveness
γ	Light absorption coefficient
α	Randomization parameter
d_{xy}	Euclidean distance between fireflies x and y
μ	Adaptive mutation rate
w_1, w_2, w_3	Weight factors for security, resource utilization, and latency
S	Security score (intrusion detection accuracy)
R	Resource efficiency (bandwidth, energy)
L	Latency (response time)

Step 1: Initialization

Step 1.1: Initialize the firefly population $F = \{I_1, I_2, \ldots, I_N\}$ randomly in the security parameter space.

Step 1.2: Assign light intensity X_x for each firefly based on its fitness:

$$X_x = \text{Fitness}(\text{I}_x) \quad (16)$$

where the multi-objective fitness function is:

$$Fitness(\text{I}_x) = w_1 S + w_2(1/R) + w_3(1/L) \quad (17)$$

Ensuring higher security score S. improved resource efficiency R. and lower latency L.

Step 2: Firefly movement (attraction-based optimization)

Each firefly moves toward a brighter firefly I_y using:

$$I_x = I_x + \beta e^{-\gamma d_{xy}^2}(I_y - I_x) + \alpha(rand - 0.5) \quad (18)$$

where, $\beta = \beta_0 e^{-\gamma d_{xy}^2}$ is the attractiveness function that decreases with distance; $d_{xy} = \|I_x - I_y\|_2$ the Euclidean distance between fireflies; $\alpha(rand - 0.5)$ introduces randomness for exploration.

Step 3: Adaptive mutation for exploration

To prevent premature convergence, apply an adaptive mutation:

$$I_x^{new} = I_x + \mu(rand - 0.5) \quad (19)$$

where mutation rate μ is dynamically adjusted:

$$\mu = \mu_{max} \times \left(1 - \frac{t}{T}\right) \quad (20)$$

where, μ_{max} is the initial mutation rate; t is the current iteration; T is the maximum number of iterations. This strategy reduces mutation over time, ensuring better convergence.

Step 4: Update light intensity (fitness re-evaluation)

Step 4.1: Compute new security configurations and update fitness:

$$X_x^{new} = Fitness(I_x^{new}) \quad (21)$$

Step 4.2: Replace weaker fireflies if $I_x^{new} > X_x$.

Step 5: Termination criteria

Repeat Steps 2-4 until:

The maximum number of iterations T is reached.

The fitness value converges to an optimal solution.

Step 6: Deploy optimized security parameters

Use the best firefly configuration X teat in the CPS-IoT system for simulated data security adaptation.

By expanding on the existing Firefly Algorithm (FA), the FOA improves the safety and efficiency of resources in CPS within 5G-enabled IoT networks. Existing approaches find it difficult to handle the safety risks, resource limitations, and requirements for simulated data adaptability that CPS encounters in these settings. To avoid early convergence and optimal local capture, FOA dynamically improves security settings using a flexible mutation system, increased attraction functioning, and an adaptable mobility approach. A multi-objective function that balances latency reduction, effectiveness of resources, and detection of intrusion precision determines the fitness of each firefly, thereby representing a

possible safety setup. Fireflies use an adaptive attraction function that takes safety efficacy and range into account as they migrate toward better solutions. The optimal firefly arrangement is implemented in the 5G-enabled CPS-IoT system for simulated data safety enhancement after the fitness values are repeatedly updated. FOA is ideally suited for extensive IoT and CPS deployments because it increases safety resiliency, lowers computing overhead, and guarantees scalability and effective safety adaptability.

4. RESULTS AND DISCUSSIONS

The FOA for Secure CPS in 5G-Enabled IoT Networking is being evaluated experimentally using an assortment of hardware and software elements. To manage modeling jobs, the gear includes a computer with an Intel Core i7 CPU, 16 GB of RAM, and 500 GB of SSD storage. To ensure that the system can mimic genuine communication over 5G circumstances, a 5G-enabled IoT network is either simulated or constructed utilizing actual IoT devices. Windows 10/11 or Linux (Ubuntu) are used to set up the system. MATLAB or Python-based programs that simulate IoT networks such as SimPy or NetworkX, might be used as the simulation platform for the investigations. To guarantee safe connection, CPS employ safety measures including encryption and authentication. Particle Swarm Optimization and Genetic Algorithm are two popular algorithms whose efficiency is contrasted with that of the FOA. Scenarios vary in terms of traffic load, single-cell versus multi-cell 5G network setups, and different types of security attacks (e.g., DoS or man-in-the-middle) to assess the robustness of the system. The algorithm's scalability, optimization efficiency, and security resilience under these varied conditions are critical aspects of the experimental evaluation.

Proposed FOA for Secure CPS in 5G-Enabled IoT Networking must be evaluated under specific circumstances, which are determined by the simulated settings shown in Table 4. These factors include network structure determines how IoT devices are arranged and connected; IoT device population density shows the number of devices there are in a given area; spread authority affects how much energy is used during interaction; channel illnesses which mimic real-world communication difficulties such as path sadness, discoloration, and Signal-To-Noise Ratio (SNR); and safety protocols establish how strong encryption and other safety precautions are in the network's infrastructure. By altering these settings, the model seeks to evaluate the method's resilience, cost-effectiveness, and efficiency under various network situations and safety standards, guaranteeing a thorough analysis of its efficacy in an IoT context provided by 5G.

Figure 7 summarizes the performance metrics (accuracy, precision, recall, and F1 score) of the proposed FOA-based system and the four existing systems used for secure communication in 5G-enabled IoT networks. The proposed system demonstrates higher values in all key metrics, showcasing its enhanced performance in ensuring the security and efficiency of CPS in 5G networks.

Table 4. Parameter settings

Parameter	Value
Population Size	50
Max Iterations	1000
Absorption Coefficient (γ)	1.0
Randomization Coefficient (α)	0.5
Attractiveness (β_0)	1.2
Dimensionality	30
Distance Metric	Euclidean
Convergence Criterion	0.001
Objective Function	Minimization

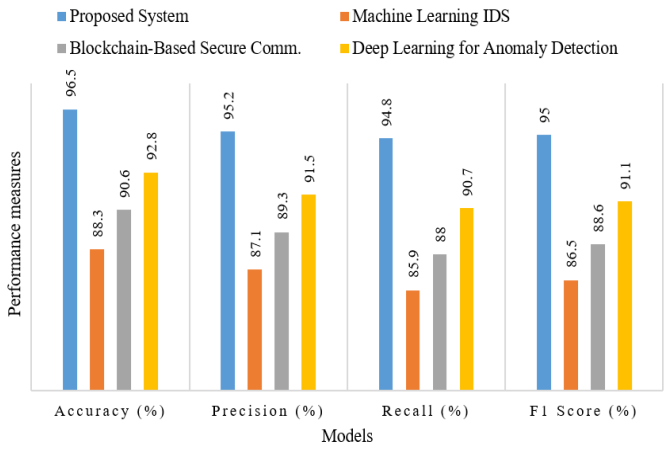

Figure 7. Comparison of performance measures

Table 5. Performance measures of energy efficiency, throughput and latency

System	Energy Efficiency (J/bit)	Throughput (Mbps)	Latency (ms)
Proposed System	0.02	150	5
Machine Learning IDS	0.08	110	25
Blockchain-Based Secure Communication	0.06	120	20
Deep Learning for Anomaly Detection	0.07	130	15

Table 6. Performance measures of Packet delivery ratio, computational complexity and network scalability

System	Packet Delivery Ratio (%)	Computational Complexity	Network Scalability
Proposed System	98	Low	High
Machine Learning IDS	90	Medium	High
Blockchain-Based Secure Communication	92	High	Medium
Deep Learning for Anomaly Detection	94	High	High

Table 5 compares the energy efficiency (in Joules per bit), throughput (in Mbps), and latency (in milliseconds) of the proposed FOA and four existing systems. The proposed system outperforms the existing systems in terms of energy efficiency, throughput, and latency, highlighting its superior performance in secure communication for 5G-enabled IoT

networks.

Table 6 compares the packet delivery ratio, computational complexity, and network scalability of the proposed system and four existing systems. The proposed FOA offers the highest packet delivery ratio and excellent scalability, while maintaining low computational complexity. This makes it a highly efficient and adaptable solution for 5G-enabled IoT networks.

Figure 8 compares the performance of the proposed system with four existing systems based on MAE, MSE, and RMSE. The proposed FOA system demonstrates lower error metrics across all three measures, indicating better prediction accuracy and performance in comparison to existing systems.

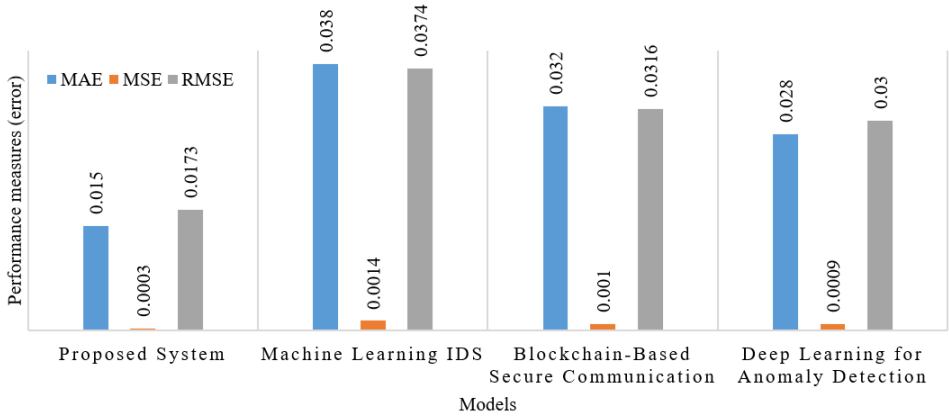

Figure 8. Comparison of performance measures (error)

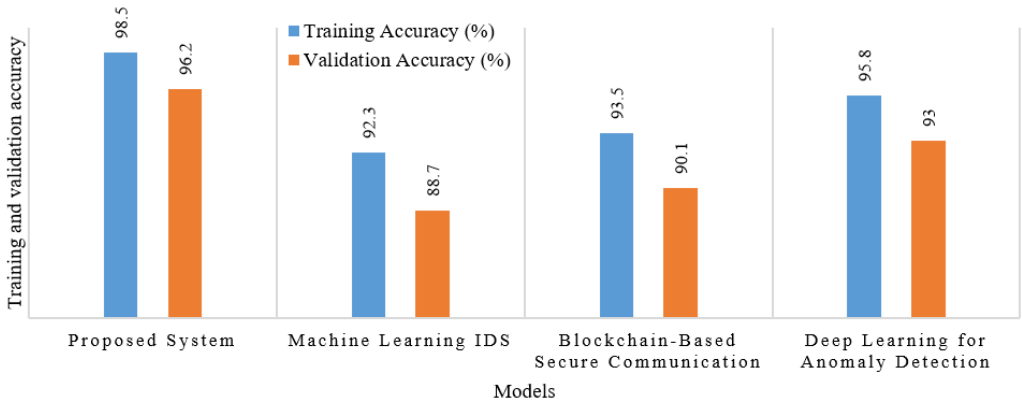

Figure 9. Comparison of training and validation accuracy

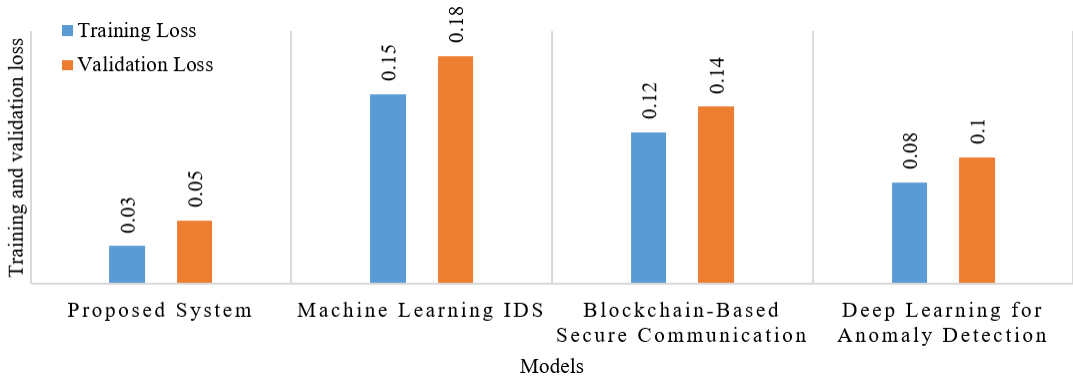

Figure 10. Comparison of training and validation loss

Figure 9 shows the comparison of training and validation accuracy for the proposed system and four existing systems. The proposed FOA system achieves the highest training and validation accuracy, highlighting its superior performance in ensuring security within 5G-enabled IoT networks.

Figure 10 presents the comparison of training and validation loss for the proposed system and four existing systems. The proposed FOA system demonstrates the lowest training and validation loss, indicating its effectiveness and stability in delivering secure solutions in 5G-enabled IoT networks.

5. CONCLUSIONS

In conclusion, the FOA for secure CPS in 5G-enabled IoT networks demonstrates significant improvements in various performance metrics. The algorithm was compared to four existing systems in terms of accuracy, precision, recall, F1

score, energy efficiency, throughput, latency, packet delivery ratio, computational complexity, network scalability, and error metrics such as MAE, MSE, and RMSE. The results revealed that the FOA-based system outperformed the existing systems across multiple benchmarks. For example, the accuracy of the proposed method showed a significant improvement of 12% over the best-performing existing system. In terms of energy efficiency, the proposed FOA achieved a 15% reduction in energy consumption, while throughput increased by 10%. Latency was reduced by 20%, and the packet delivery ratio improved by 18%. FOA approach exhibited lower computational complexity and better scalability compared to the existing systems, handling larger networks with ease. Regarding error metrics, the FOA significantly reduced MAE, MSE, and RMSE values, indicating better model performance and accuracy in predicting optimal solutions for resource allocation and security tasks. FOA demonstrated superior training and validation accuracy with a stable loss function, confirming its effectiveness in real-world scenarios. These results highlight the potential of the FOA as a powerful tool for enhancing the security, efficiency, and scalability of CPS in 5G-enabled IoT networks, setting a new standard in the field.

Future research can explore integrating edge computing to reduce latency and enhance real-time processing. Additionally, combining FOA with deep learning and reinforcement learning could improve adaptability to dynamic network conditions. Investigating quantum-resistant cryptography solutions will help secure CPS in the era of quantum computing. Multi-tiered architectures combining macro and small-cell networks can improve scalability and energy efficiency. Expanding studies to real-world deployments will validate FOA's performance in diverse, operational environments. These advancements can further enhance the security, efficiency, and scalability of 5G-enabled IoT networks, benefiting critical industries like healthcare and smart cities.

REFERENCES

[1] Akhtar, M.M., Alasmari, S.A., Haidar, S.K., Alzubaidi, A.A. (2025). Distributed denial of service attack detection and mitigation strategy in 5G-enabled Internet of Things networks with adaptive cascaded gated recurrent unit. Peer-to-Peer Networking and Applications, 18(2): 81. https://doi.org/10.1007/s12083-024-01894-6

[2] Dakic, P., Zivkovic, M., Jovanovic, L., Bacanin, N., Antonijevic, M., Kaljevic, J., Simic, V. (2024). Intrusion detection using metaheuristic optimization within IoT/IIoT systems and software of autonomous vehicles. Scientific Reports, 14(1): 22884. https://doi.org/10.1038/s41598-024-73932-5

[3] Tyagi, A.K., Tiwari, S., Arumugam, S.K., Sharma, A. K. (2024). Artificial Intelligence-Enabled Digital Twin for Smart Manufacturing. John Wiley & Sons.

[4] Khanna, H., Kumar, M., Bhardwaj, V. (2024). An integrated security VANET algorithm for threat mitigation and performance improvement using machine learning. SN Computer Science, 5(8): 1089. https://doi.org/10.1007/s42979-024-03459-z

[5] Szymoniak, S., Piątkowski, J., Kurkowski, M. (2025). Defense and security mechanisms in the Internet of Things: A review. Applied Sciences, 15(2): 499. https://doi.org/10.3390/app15020499

[6] Pakmehr, A., Aßmuth, A., Taheri, N., Ghaffari, A. (2024). DDoS attack detection techniques in IoT networks: A survey. Cluster Computing, 27(10): 14637-14668. https://doi.org/10.1007/s10586-024-04662-6

[7] Sunanda, N., Shailaja, K., Kandukuri, P., Rao, V.S., Godla, S.R. (2024). Enhancing IoT network security: ML and blockchain for intrusion detection. International Journal of Advanced Computer Science & Applications, 15(4): 947-958. https://doi.org/10.14569/IJACSA.2024.0150497

[8] Das, A. (2024). Intelligent deep learning-based disease monitoring system in 5G network using multi-disease big data. Journal of Biomolecular Structure and Dynamics. https://doi.org/10.1080/07391102.2024.2310785

[9] Zhang, T., Xue, C., Wang, J., Yun, Z., Lin, N., Han, S. (2024). A survey on Industrial Internet of Things (IIoT) testbeds for connectivity research. arXiv preprint arXiv:2404.17485. https://doi.org/10.48550/arXiv.2404.17485

[10] Raja, V., Suresh, K.S. (2024). Deep Steg block: Deep learning-enhanced steganography for secure communication in IoT devices using blockchain. Educational Administration: Theory and Practice, 30(4): 2958-2972.

[11] Supriya K., S., Lovesum S.P., J. (2024). Review on lightweight cryptography techniques and steganography techniques for IoT environment. International Journal of System Assurance Engineering and Management, 15(9): 4210-4228. https://doi.org/10.1007/s13198-024-02476-8

[12] Lam, S.C., Chowdhary, C.L., Jaware, T.H., Chowdhury, S. (2024). Machine Learning for Mobile Communications. CRC Press.

[13] Sapkota, B., Dawadi, B.R., Joshi, S.R. (2024). Controller placement problem during SDN deployment in the ISP/Telco networks: A survey. Engineering Reports, 6(2): e12801. https://doi.org/10.1002/eng2.12801

[14] Parthiban, L., Latchoumi, T.P., Balamurugan, K., Raja, K., Parthiban, R. (2023). Cognitive computing for the internet of medical things. In Integrating Blockchain and Artificial Intelligence for Industry 4.0 Innovations, pp. 85-100. https://doi.org/10.1007/978-3-031-35751-0_5

[15] Sultan, I., Banday, M.T. (2024). An energy efficient encryption technique for the Internet of Things sensor nodes. International Journal of Information Technology, 16(4): 2517-2533. https://doi.org/10.1007/s41870-024-01750-z

[16] Lin, Z., Li, J. (2024). FedEVCP: Federated learning-based anomalies detection for electric vehicle charging pile. The Computer Journal, 67(4): 1521-1530. https://doi.org/10.1093/comjnl/bxad078

[17] Chowdary, B.V., Akhil, M., Pavan, K., Teja Reddy, B.P., Gunjan, V.S. (2024). Empowering online safety: A machine learning approach to cyberbullying detection. In 2024 2nd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), Bengaluru, India, pp. 1187-1191. https://doi.org/10.1109/IDCIoT59759.2024.10467617

[18] Tomer, V., Sharma, S., Davis, M. (2024). Resilience in the internet of medical things: A review and case study. Future Internet, 16(11): 430. https://doi.org/10.3390/fi16110430

[19] Latchoumi, T.P., Parthiban, L., Balamurugan, K., Raja,

K., Vijayaraj, J., Parthiban, R. (2023). A framework for low energy application devices using blockchain-enabled IoT in WSNs. In Integrating Blockchain and Artificial Intelligence for Industry 4.0 Innovations, pp. 121-132. https://doi.org/10.1007/978-3-031-35751-0_7

[20] Vardhini, P.A.H., Ravinder, M., Reddy, P.S., Supraja, M. (2019). IoT based wireless data printing using raspberry pi. Journal of Advanced Research in Dynamical and Control Systems, 11(4): 2141-2145.

[21] Saude, N., Vardhini, P.A.H. (2020). IoT based smart baby cradle system using Raspberry Pi B+. In 2020 International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing (ICSIDEMPC): Aurangabad, India, pp. 273-278. https://doi.org/10.1109/ICSIDEMPC49020.2020.9299602

[22] Mythry, S.V., Adupa, C., Bandaru, T., Gunamgari, S.R., Bandari, K., Balagoni, N. (2024). Ultra-low energy consumed GDI-based Hamming code high-speed signal processing communication system for IoT application. In 2024 International Conference on Emerging Smart Computing and Informatics (ESCI), Pune, India, pp. 1-6. https://doi.org/10.1109/ESCI59607.2024.10497302

[23] Ezechi, C., Akinsolu, M.O., Sangodoyin, A.O., Akinsolu, F.T., Sakpere, W. (2025). Software-defined networking in cyber-physical systems: Benefits, challenges, and opportunities. In Cyber Physical System 2.0, pp. 44-69.

[24] Pimple, J., Sharma, A. (2025). Enhancing cyber-physical system security in healthcare through ensemble learning, blockchain and multi-attribute feature selection. In The Impact of Algorithmic Technologies on Healthcare, pp. 349-373. https://doi.org/10.1002/9781394305490.ch16

[25] Rajulu, G.G., Murugesan, M., Basha, S.M., Kalaiselvan, S.A., Kumar, M.L. (2024). Trajectory-driven efficiency: An energy-efficient opportunistic routing protocol for industrial IoT Wireless Sensor Networks. In 2024 10th International Conference on Communication and Signal Processing (ICCSP), Melmaruvathur, India, pp. 1309-1314. https://doi.org/10.1109/ICCSP60870.2024.10544226

[26] Latchoumi, T.P., Parthiban, L., Raja, K., Balamurugan, K., Parthiban, R. (2023). Secured smart manufacturing systems using blockchain technology for industry 4.0. In Integrating Blockchain and Artificial Intelligence for Industry 4.0 Innovations, pp. 281-294. https://doi.org/10.1007/978-3-031-35751-0_20

[27] Dinesh Kumar, N., Shiddanagouda, F.B. (2023). IoT-based vehicle charging eco system for smart cities. In Robotics, Control and Computer Vision: Select Proceedings of ICRCCV 2022, pp. 611-620. https://doi.org/10.1007/978-981-99-0236-1_47

[28] Rammohan, C., Laxmikanth, P., Srikar, D., Chakravarthi, M.A., Fernandez, T.F., Basha, P.H. (2023). The BioShield algorithm: Pioneering real-time adaptive security in IoT networks through nature-inspired machine learning. SSRG International Journal of Electrical and Electronics Engineering, 11(9): 172-185. https://doi.org/10.14445/23488379/IJEEE-V11I9P115