Centralized Infrastructure-Aware Reliable Data Transaction Model in IoT-Enabled MANET and Cloud Using MFOA and DNN

Muhammad Azhar Mushtaq[1, *], Zaharaddeen Karami Lawal[2], G.Arulkumaran[3]

[1]University of Sargodha Pakistan. Email: azhar.mushtaq@uos.edu.pk, azhar637@outlook.com
[2]Universiti Brunei Darussalam, Brunei, Nigeria. Email: deenklawal13@gmail.com
[3]Associate Professor, School of C&IT, REVA University, Bangalore, India. Email: erarulkumaran@gmail.com

ABSTRACT

A centralized data transaction mechanism for Internet of Things-enabled MANETs is presented in this dissertation. Through the use of Deep Neural Networks (DNN) for intrusion detection and the Moth Flame Optimization Algorithm (MFOA) for effective routing, the model improves network security, lowers energy consumption, and increases throughput while achieving an impressive accuracy of 99.52%.

BACKGROUND: Historically, issues with poor routing, excessive energy consumption, and security flaws have plagued mobile ad hoc networks, or MANETs. These problems are becoming increasingly important as IoT devices grow more integrated. In order to properly manage data flow and security, an effective, secure infrastructure is required because older models lacked a centralized management system.

OBJECTIVES: Developing a centralized paradigm to enhance the security and effectiveness of data transfers in IoT-enabled MANETs is the main goal of this research. In order to guarantee dependable data transfer while reducing energy consumption and enhancing overall network performance, this is accomplished by integrating MFOA for routing path optimization with DNN for intrusion detection.

METHODS: The model makes use of DNN to instantly identify network breaches and MFOA to choose the data transmission channels that use the least amount of energy. Elliptic Curve Cryptography (ECC) is used in encryption to protect data. Important parameters including accuracy, energy consumption, and throughput are used to evaluate the model's performance in comparison to other models.

RESULTS: By attaining 99.52% accuracy, 93% energy efficiency, and 72.85% faster encryption times, the suggested approach surpassed traditional methods. 95 Mbps is the maximum network throughput, indicating a significant increase over previous versions. The device is highly suited for Internet of Things applications where safe and quick data transfer is essential due to its efficiency in energy consumption and encryption.

CONCLUSION: A solid option for safe, scalable data transfers in IoT-enabled MANETs is provided by the MFOA-DNN-based paradigm. Large networks like those in smart cities and healthcare systems benefit greatly from its enhanced security, faster encryption, and greater energy efficiency. Its capacity to optimize routing and detect intrusions with high accuracy makes it the perfect choice.

Keywords: Moth Flame Optimization Algorithm (MFOA), Deep Neural Networks (DNN), IoT-enabled MANETs, Intrusion Detection, Elliptic Curve Cryptography (ECC), Energy Efficiency, Secure Data Transmission.

1 INTRODUCTION

Centralized infrastructure that is conscious as there is no central authority in traditional MANETs, there may be inefficiencies and security problems. Better network control and monitoring are made possible by the centralized structure this architecture delivers. Ensuring secure communication, enhancing device coordination, and effectively managing dynamic network behavior such as node entrance, data routing, and energy management are all made possible by it. Dependable Model for Data Transactions Designing a dependable data transfer infrastructure is the main goal. Ensuring safe and lossless

*Corresponding Author: Muhammad Azhar Mushtaq Email: azhar.mushtaq@uos.edu.pk

data transmission is crucial in mobile networks, as nodes, or devices, are movable and connections may be erratic. In a dynamic and constantly changing environment, like Internet of Things networks, the approach guarantees consistent data transmission. IoT-Powered Cloud and MANET via means of MANETs, IoT devices (such as sensors and smart gadgets) can connect with one another on a mobile network. For storage, processing, or additional connectivity, these devices frequently require a cloud connection. The solution ensures effective data flow between these IoT devices and cloud services by supporting seamless integration.

Employing MFOA in this model, the Moth Flame Optimization Algorithm (MFOA) is used to optimize specific network activities, such determining cluster heads (important nodes in the network) or the optimum pathways for data transmission. As conditions in mobile networks change quickly, MFOA helps increase efficiency by discovering the optimal solutions quickly. Making Use of DNN Using Deep Neural Networks (DNN) to detect possible risks or illegal access within the network, security can be improved. DNN is a useful tool for intrusion detection since it can identify abnormalities in data patterns, ensuring the security of the data moving over the network. IoT-enabled MANETs have been the subject of various models that have investigated intrusion detection and data security; nevertheless, these models frequently overlook important problems, such as the absence of centralized control for tracking node activity and streamlining data pathways. Inconsistent network performance can result from a number of existing techniques' ineffective handling of energy consumption and dynamic node re-entry. Additionally, traditional approaches frequently fail to provide robust encryption and security features, leaving data exposed. In order to close these gaps and provide a more dependable, energy-efficient, and secure data transaction framework, this dissertation introduces MFOA for optimal path selection and DNN for intrusion detection.

IoT-enabled MANETs currently use systems that are afflicted with a number of issues, including inconsistent path selection for data transmission, ineffective node administration, and a lack of centralized monitoring. These flaws result in high energy consumption, security vulnerabilities, and inconsistent network performance. Furthermore, real-time intrusion detection is a challenge for traditional systems, and exposes the network to possible attackers. By putting forth a centralized infrastructure-aware model that employs DNN for precise intrusion detection and MFOA for effective path optimization, this investigation seeks to address these shortcomings and ensure safe, dependable, and scalable data transactions in cloud and MANET environments that are enabled by the Internet of Things.

- Provide a Centralized Infrastructure: The main objective is to provide a framework that uses centralized infrastructure to improve data transaction dependability in cloud environments and Internet of Things-enabled MANETs (Mobile Ad-Hoc Networks), guaranteeing more effective and smooth communication.
- Optimize Path Selection: To improve routing efficiency and save energy, apply the Moth Flame Optimization Algorithm (MFOA) to identify the most effective cluster heads and produce numerous optimal paths for data transmission.
- Enhance Intrusion Detection: Use Deep Neural Networks (DNN) to identify and categorize any intrusions, guaranteeing that information transferred across the network is safe and unhindered by outside intervention.
- Improve Data Security: Reduce security threats and offer a strong layer of protection during data transfer by using cutting-edge encryption techniques to secure user data.
- Improve Scalability and Performance: Develop a model that can manage highly performant large-scale IoT and cloud networks without sacrificing system scalability or data security.

Structure and Contributions

The key contributions of this paper are summarized as follows:

- A centralized infrastructure-aware model that addresses the limitations of traditional decentralized MANET systems by improving security, energy efficiency, and data reliability in IoT-enabled environments.
- Integration of Moth Flame Optimization Algorithm (MFOA) for optimal path selection, reducing energy consumption while ensuring effective data routing.
- Use of DNN for accurate intrusion detection, providing enhanced network security by identifying and mitigating potential threats in real time.
- Application of Elliptic Curve Cryptography (ECC) for lightweight yet robust data encryption, making the system suitable for resource-constrained IoT devices.
- Comprehensive performance evaluation that demonstrates significant improvements in network accuracy, energy efficiency, encryption time, and throughput over existing models.

Following, Section 2 presents a thorough literature review, addressing the challenges faced by existing systems and stressing the necessity for a centralized infrastructure-aware model. In Section 3, the proposed methodology is outlined, incorporating the Moth Flame Optimization Algorithm (MFOA) for efficient routing and DNN for intrusion detection. Section 4 delves into the results and performance evaluation, showcasing the superiority of the proposed model over existing approaches. Finally, Section

5 concludes the paper by summarizing the key findings and suggesting potential directions for future research.

2 LITERATURE SURVEY

The major topic of energy efficiency in data centers is addressed in Haghshenas et al. (2020) analysis. It offers an algorithm for scheduling that takes energy costs and server configurations into account to maximize workload distribution. This strategy is a great way to improve resource management and encourage sustainability in data centers because it strikes a balance between performance and power consumption, thereby cutting operating costs.

Mohanarangan Veerappermal Devarajan (2023) suggested an IoT-based autonomous system to identify moles, skin tags, and warts-related diseases. Using IoMT, automatic lumen detection and trigonometric algorithms improved accuracy and classification over big datasets of images. The model presented better detection performance with improved accuracy that helps in proper early diagnosis and better tracking of skin diseases.

Rajya Lakshmi Gudivaka (2024) proposed an IoT and fog-based e-healthcare framework for the detection of health, behavioral, and environmental abnormalities caused by sedentary lifestyles. The study achieved 98.43% accuracy in predicting health severity using weighted K-Mean clustering and WKMC-DT methods, tested on 15 individuals over 30 days, which indicates the effectiveness of the proposed method in early health anomaly detection.

An extensive analysis of the Moth Flame Optimization Algorithm (MFOA) with a focus on its many modifications and applications is given by Shehab et al. (2020). Motivated by moth navigation, MFOA is an excellent solution for challenging optimization issues. The investigation presents multiple iterations of the algorithm that improve its exploration and efficient convergence to solutions. MFOA has been effectively used in a variety of fields, including network optimization, image processing, and engineering design. The investigation demonstrates the algorithm's versatility, making it an effective tool for solving theoretical and practical optimization problems.

Dinesh Kumar (2024) proposed an Enhanced Fault Diagnosis in IoT (FD-IoT-DMSFNN) employing real-time sensor data. Sensor data retrieved from the CWRU dataset is normalized using Multivariate Fast Iterative Filtering while outliers are detected using Deep Isolation Forest (DIF). A Mexican Axolotl Optimization (MAO) fine-tunes DMSFNN while attaining higher accuracy compared to existing methods and minimized completion time.

The Hybrid Moth Flame Optimization (MFO) algorithm, presented by Sahoo & Saha, (2022) improves global optimization by fusing MFO with other optimization methods. Faster and more accurate results are produced by the algorithm's enhanced exploration and exploitation of solutions thanks to this hybrid approach. The algorithm's superiority over the conventional MFO in terms of speed and accuracy was demonstrated by the authors through testing it on a variety of benchmark functions and real-world scenarios. The hybrid version demonstrated greater resilience in evading local optima, rendering it a more dependable instrument for resolving intricate global optimization problems.

Surendar, Rama, and Sitaramanan (2024) presents the smart irrigation system utilizing IoT, embedded systems like ESP32, and cloud computing to monitor real-time parameters, such as moisture, humidity, temperature, and water levels. By sensors (DHT22, water level, and moisture), and ThingSpeak cloud, it enables precise management of water, reducing by 70% the water consumption and improving food security through sustainable agriculture.

A multi-level trust mechanism is introduced by Anil (2021) investigation to defend IoT-enabled MANET systems against routing attacks. Through an assessment of nodes' behavior, energy usage, and data quality, the model improves the system's capacity to identify and segregate rogue nodes. As a result, data transfers become more trustworthy and safer, guaranteeing that communication integrity is upheld even in the face of intrusions. By reducing the risks associated with routing assaults in IoT ecosystems, the method offers a strong way to increase the network's resilience and security.

Rajya Lakshmi Gudivaka (2021) proposed a dynamic four-phase cloud data security system using LSB steganography and cryptography. Data gets encrypted and hidden in the pixels of an image, and AES keys get secured through RSA and embedded in a cover object. This framework enhances cloud security by giving secrecy, integrity, and redundancy while suggesting future improvements by using machine learning and finer steganalysis methods.

SecDL is a secure deep learning approach presented by Sujanthi and Nithya Kalyani (2020) that aims to enhance dynamic cluster-based routing in Wireless Sensor Networks (WSN) in Internet of Things (IoT) contexts. By striking a balance between energy efficiency, data transmission speed, and security, SecDL aims to guarantee Quality of Service (QoS). In order to adjust to network changes and produce more precise routing decisions while averting possible security breaches, the model makes use of deep learning. SecDL improves the overall performance of WSN-based IoT systems by optimizing both routing and security, providing a comprehensive solution to tackle issues like energy management and network security.

Raj Kumar Gudivaka (2024) has addressed the challenge of finding small blood cells in Acute Lymphoblastic Leukemia (ALL) with an improved

YOLOv4 model. Deployed on the Hadoop framework, with data augmentation solving class imbalance in the ALLIDB1 dataset, the model significantly enhances precision in detection of healthy and blast cells, allowing for early diagnosis.

In order to enhance DNN training, Jia et al. (2019) investigate novel techniques that go beyond conventional data and model parallelism. Their work presents novel methods that overcome the drawbacks of current strategies, leading to improved efficiency, scalability, and resource use. These developments facilitate the removal of bottlenecks in distributed systems, allowing large-scale DNNs to be trained more quickly and efficiently. The suggested techniques are especially helpful for applications requiring a lot of resources, including machine learning and artificial intelligence, as effective training is essential. The performance of DNN training in dispersed situations is greatly improved by this investigation.

Thirusubramanian Ganesan (2023) presented the Proactive Dynamic Secure Data Scheme, P2DS, as a protection scheme for financial data in mobile cloud environments. Using techniques such as Attribute-Based Encryption (ABE), Attribute-Based Semantic Access Control (A-SAC), and the Proactive Determinative Access algorithm, P2DS offers secure access control, fast threat detection, and efficient encryption, making it a safe and reliable solution for sensitive financial data.

Sharadha Kodadi (2022) explores the integration of cloud computing with advanced tools like wavelet analysis, big data analytics, and machine learning to enhance real-time seismic data processing. The proposed system improves earthquake prediction, data management, and coordination in dealing with the challenges that characterize the traditional systems and significantly boost disaster response and recovery efforts.

Specifically designed for Internet of Things applications, Pamarthi and Narmadha (2022) present an intelligent privacy preservation protocol for wireless MANETs. To improve security and privacy during data transmission, the protocol makes use of a mix of the Harris Hawks Optimization (HHO) and the Crow Search Algorithm (CSA). The protocol balances privacy with energy consumption by preventing data leaks and increasing overall network efficiency through node behavior optimization. This hybrid solution works better than conventional techniques, which makes it perfect for Internet of Things applications where resource management and data security are crucial. The paper emphasizes this hybrid model's major benefits for protecting privacy in Internet of Things networks.

Akhil Raj Gaius Yallamelli (2021) used Content Analysis, PLS-SEM, and CART to examine the influence of cloud computing on SMEs' management accounting. It has brought about real-time data access, better decision-making, and regulatory compliance. While it offers sophisticated analytics, it also faces issues related to data security, privacy, and training of employees. Overall, cloud computing improves efficiency and strategic decision-making in SMEs.

A fuzzy-based detection approach is presented by Simpson and Nagarajan (2021) in order to detect cooperative blackmailing attempts on edge computing nodes in MANET-IoT systems. The plan targets attacks that see a number of nodes work together to harm the reputation of valid nodes by evaluating node behavior and spotting malicious activity using fuzzy logic. The methodology considerably increases network security and trust by spotting and eliminating these threats in real-time, guaranteeing dependable communication. This method provides a robust protection against reputation-based assaults, making it a useful way to keep IoT-enabled MANET systems secure.

According to Sri Harsha Grandhi (2022), integrating wearable sensors with IoT allows for effective monitoring of children's health, with adaptive wavelet transforms used for data preprocessing to improve signal quality and for prompt treatments.

Surendar Rama Sitaraman (2022) investigates how edge computing improves IoT security and privacy by utilizing anonymized AI techniques such as homomorphic encryption and federated learning, demonstrating its usefulness for real-world applications while maintaining data protection compliance.

A collaborative routing technique based on deep reinforcement learning (DRL) and designed for clustered MANETs is introduced by Li et al. (2023). The algorithm optimizes routing choices to increase efficiency and adaptability by continuously learning from real-time network conditions through the use of DRL. Its main objectives are to ensure dependable data transfer in extremely dynamic and mobile situations, reduce latency, and increase energy efficiency. The system handles the challenges of node mobility and network changes better than existing techniques by performing real-time routing adjustments. Because of this, it is a very successful method for handling the complexity of clustered MANETs and enhancing network performance in general.

Sri Harsha Grandhi (2024) investigates injection-locked photonic frequency division for IoT communication, demonstrating remarkable spectral purity and efficiency. He also addresses integration issues and future research goals for enhanced microwave signal creation in communication networks.

Raj Kumar Gudivaka (2020) offers a Two-Tier Medium Access Control (MAC) solution for cloud-based robotic process automation (RPA) that optimizes energy economy

and resource management while boosting throughput and QoS using Lyapunov optimization methods.

Inspired by the way moths fly toward light, Singh et al. (2021) provide a data clustering technique based on the Moth Flame Optimization Algorithm (MFOA). By efficiently identifying the ideal cluster centroids and striking a balance between exploration and exploitation to enhance performance, the method optimizes the clustering process. According to their research, MFOA clusters complicated, multidimensional datasets more accurately and efficiently than conventional techniques. This method offers a potent way to handle difficult data clustering problems and is particularly helpful in fields like pattern identification, data analysis, and picture processing.

Himabindu Chetlapalli (2021) presents the Global Authentication Register System (GARS) to improve security and privacy in multi-cloud systems by solving difficulties with user-centric methods and regulatory compliance, resulting in a safer computing environment for users.

Roy and Deb (2018) examine the effectiveness of several routing protocols in Mobile Ad Hoc Networks (MANETs) in their article, paying particular attention to AODV, DSR, and OLSR. They evaluate these protocols according to important parameters such as routing overhead, packet delivery ratio, and end-to-end latency. The results show that AODV is superior at efficiently delivering packets, whereas DSR's shorter latency makes it work better in low-mobility scenarios. OLSR tends to provide more overhead even though it is effective for larger networks. It emphasizes how crucial it is to choose the right routing protocol depending on the demands of a given application and the changing nature of the network environment. Routing protocols are crucial for the efficiency and reliability of Mobile Ad Hoc Networks (MANETs), especially in dynamic environments with frequent topology changes. Protocols like AODV, DSR, and OLSR exhibit varied strengths: AODV is highly effective in dynamic networks due to its on-demand route establishment, DSR excels in low-mobility scenarios with minimal overhead, and OLSR reduces latency by maintaining pre-established routes but incurs higher overhead. In IoT-enabled MANETs, where energy efficiency and reliability are critical, protocols like AODV, enhanced with optimization techniques such as the Moth Flame Optimization Algorithm (MFOA), offer significant improvements in energy consumption and routing performance.

Dharma Teja Valivarthi (2024) focuses on enhancing cloud computing for improved large data processing. Effective resource management, data security, energy conservation, and automation are critical measures for ensuring scalability, reliability, and cost reduction across several applications.

To improve cybersecurity, Navya et al. (2021) concentrate on creating an intrusion detection system (IDS) driven by DNN. Their investigation compares the performance of DNNs with conventional machine learning techniques and shows how successful DNNs are in detecting a variety of network breaches. The DNN-based IDS achieves significantly greater precision and recall rates by augmenting datasets and employing advanced feature extraction techniques. The study demonstrates DNNs' capacity to adjust and pick up new skills from threats, making them a potent choice for real-time intrusion detection. This investigation demonstrates how DNNs can revolutionize detection capacities against sophisticated cyberattacks.

According to Dharma Teja Valivarthi (2024), optimizing cloud systems can improve big data processing. Effective resource management, energy-efficient protocols, robust data protection, scalability (horizontal and vertical), and automation are important areas of study. These tactics seek to guarantee dependability, cut expenses, and create a simplified, safe, and scalable cloud architecture for a range of applications.

Swapna Narla (2024) suggests utilizing Chain-Code and Homomorphic Verifiable Tags (HVT) in a blockchain-based approach to guarantee data integrity in multi-cloud storage systems. This approach focuses on enhancing performance in large-scale cloud systems while opening the door for future security breakthroughs by combining cryptographic commitments with decentralized verification to improve security, scalability, and efficiency.

As a method for safe data management in cloud storage, Poovendran Alagarsundaram (2022) talks about Deduplicable Proof of Storage (DPOS). Through the use of symmetric encryption and a defined protocol, DPOS ensures dependable and secure data storage while improving data confidentiality and deduplication efficiency.

A comprehensive security management approach for cloud computing in healthcare is put forth by Mohanarangan Veerappermal Devarajan (2020). Using technologies such as blockchain and multi-factor authentication, it incorporates risk assessment, security implementation, continuous monitoring, and compliance management to increase data security, reduce risks, and improve patient care and operational efficiency.

According to Akhil Raj Gaius Yallamelli (2021), cloud computing presents serious security vulnerabilities even as it transforms data management. By using asymmetric cryptography, the RSA method improves data security by guaranteeing confidentiality, integrity, and authenticity. For RSA to be implemented successfully and to comply with regulatory requirements, researchers and cloud providers must work together.

Vehicular Cloud Computing (VCC) is examined by Sreekar Peddi (2021), who highlights both its advantages and disadvantages in terms of security. He suggests DBTEC, a trust-based technique that improves safe vehicle cooperation. The study verifies the efficacy of DBTEC in enhancing collaboration and guaranteeing security in VCC systems and uses threat modeling to find vulnerabilities.

3 SECURE IOT MANET WITH MFOA AND DNN

The recommended way for facilitating dependable and secure data transmission on cloud-integrated MANETs (Mobile Ad-Hoc Networks) enabled by the Internet of Things is described in this technique DNN for intrusion detection, Moth Flame Optimization Algorithm (MFOA) for effective routing, and Centralized Infrastructure-Aware Model are all integrated into the system. The model's conceptual overview, performance measures, and technical procedures and algorithms used are all broken down in the approach.

3.1 Node Initialization and Key Generation

The initialization of nodes within the MANET that is enabled by IoT signals the start of the procedure. Every node is an IoT device that is mobile and includes communication capabilities. Each node is given a distinct public-private key pair created with Elliptic Curve Cryptography (ECC) in order to guarantee safe communication. ECC is favoured for IoT devices with constrained computational resources because of its effectiveness in delivering good security with reduced key lengths. Elliptic Curve Cryptography (ECC) was chosen over RSA and AES due to its efficiency, especially in IoT-enabled MANET environments with resource-constrained devices. ECC provides the same level of security as RSA but with significantly shorter key lengths, resulting in lower computational overhead and faster encryption times. This makes ECC highly suitable for mobile nodes and IoT devices where energy efficiency and processing power are critical. Additionally, ECC's compact key size reduces bandwidth requirements during secure communication, enhancing overall network performance.

Public Key (K_pub): Shared among all nodes for encryption.

Each node keeps the private key (K_priv) secret in order to facilitate decoding.
Within the network, secure data transactions and node authentication are conducted through the use of public and private keys.

$$N = \{n_1, n_2, n_3, \dots, n_m\} \quad (1)$$

Where N represents the set of mobile nodes in the network.

3.2 Cluster Head Selection Using Moth Flame Optimization Algorithm (MFOA)

After nodes are initialized, the Cluster Head (CH) is chosen from the collection of mobile nodes using MFOA. The CH is a crucial node responsible for managing communication inside its cluster and transferring data to the cloud or other nodes. By choosing the best CH, data routing latency is reduced and energy efficiency is increased.

Method of MFOA in the Selection of Cluster Heads:
Moth Representation: The flames (i.e., cluster head candidates) are possible solutions to the optimization problem, and each mobile node in the MANET is represented as a moth. The Moth Flame Optimization Algorithm (MFOA) effectively balances exploration and exploitation during CH selection to ensure optimal routing in MANETs. Exploration is achieved through the random generation and movement of moths in the search space, enabling the algorithm to identify new potential cluster heads. Exploitation is performed by refining solutions around the best flames, focusing on nodes with the highest residual energy and shortest distances to the destination. This dual mechanism ensures that the algorithm avoids premature convergence by thoroughly exploring the solution space while intensively exploiting the most promising candidates for CH selection. This balance improves routing efficiency and energy optimization in dynamic IoT-enabled MANETs.

Fitness Function: Each node's fitness is determined by taking into account both its distance from the destination and its remaining energy. The CH is the node that has the highest fitness.
Function of Fitness:

$$f(i) = \min\left(\frac{E_{\text{residual}}(i)}{D_{\text{total}}(i)}\right) \quad (2)$$

where $E_{\text{residual}}(i)$ is the remaining energy of node i, and $D_{\text{total}}(i)$ is the total distance to the destination node. The aim is to minimize energy consumption while ensuring efficient routing.

Exploration and Exploitation: To achieve the most effective cluster head selection, MFOA skillfully strikes a balance between exploitation, that concentrates on the most promising nodes, and exploration, that looks for new, possible CHs.

3.3 Node Clustering and Multi-Path Routing

K-means clustering is used to organize the remaining nodes into clusters after the CH has been selected. Every cluster's centroid is the CH, and nodes are assigned according on the distance it is to the CH. To determine the distance between nodes and their corresponding CHs, using the Euclidean Distance Formula.
Euclidean Distance:

$$d(i,j) = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2} \quad (3)$$

Where x_i, y_i and x_j, y_j are the coordinates of nodes i and j. The Ad-hoc On-demand Distance Vector (AODV) routing technique is used to identify different channels for data transfer once the clusters are established. Reactive routing protocols like AODV minimize needless routing overhead by only finding routes as needed. Reliable communication is maintained even in dynamic network situations because to the many pathways that are generated, that ensure fault tolerance and load balancing.

To ensure data integrity and effective route reconfiguration in the event of an attack or failure, the paths are stored in a Merkle Tree structure for verification in the fog layer.

3.4 Data Encryption Using ECC

Elliptic Curve Cryptography (ECC) is used in the MANET to protect data transmission. ECC is an excellent option for resource-constrained IoT applications because it provides more security at lower key sizes than standard encryption methods.

The public key of the destination node is used to encrypt the data coming from the source node.
To increase encryption effectiveness and decrease computing cost, the Edward Prime Curve, an extension of ECC, is utilized.
ECC Formula for Encryption:

$$E(x,y) = x^2 + y^2 = 1 + d \cdot x^2 \cdot y^2 \quad (4)$$

where d is a constant that defines the curve.
Data confidentiality and security against eavesdropping are ensured during the secure data transmission of the data to the target node following encryption.

3.5 Trust Evaluation Using Fuzzy Logic

The model uses fuzzy logic for trust evaluation to make sure that the chosen data transmission pathways are reliable and safe. Fuzzy logic calculates the trustworthiness of nodes and links based on a variety of factors, including energy levels, link stability, and distance, in order to manage uncertainty and imprecision in the network.
Fuzzy Trust Evaluation: Using the computed parameters, trust values are allocated to every path.
To ensure secure communication, low-trust pathways are avoided and high-trust paths are used for data transmission.
Formula for Evaluating Trust:

$$T_{\text{path}} = \frac{\sum_{i=1}^{N} (E(i) \cdot L(i))}{D(i)} \quad (5)$$

where $E(i)$ is the energy of node $i, L(i)$ is the link stability, and $D(i)$ is the distance to the destination.

3.6 Intrusion Detection Using Deep Neural Networks (DNN)

The model's capacity to identify and stop network intrusions is a crucial feature. DNN are used in intrusion detection because of their capacity to identify intricate patterns and evaluate enormous datasets.

Process of Intrusion Detection: The NSL-KDD dataset, containing a variety of network attack types, is used to train the DNN.

The data is processed to extract features including protocol types, source and destination IP addresses, and packet sizes.

The data is categorized by the DNN as either malicious or normal. The data transmission channel is rearranged to avoid compromised nodes in the event that an intrusion is discovered. The integration of MFOA and DNN in the proposed system is designed to address routing efficiency and security challenges in IoT-enabled MANETs. MFOA optimizes the selection of cluster heads and routing paths by balancing energy consumption and minimizing transmission delays. It represents mobile nodes as "moths" and potential cluster heads as "flames," iteratively refining the solutions using a fitness function based on residual energy and distance metrics. Simultaneously, DNN ensures network security by detecting intrusions in real time. Trained on the NSL-KDD dataset, the DNN extracts features such as protocol types and packet size to classify network traffic as benign or malicious. The model dynamically reroutes data to avoid compromised nodes, ensuring secure and efficient data transmission. Together, MFOA enhances routing efficiency, while DNN fortifies the system against threats, providing a robust and integrated framework for IoT-enabled MANETs.

DNN Forecasting Equation:

$$\hat{y} = \sigma(W \cdot X + b) \quad (6)$$

where W is the weight matrix, X is the input data, b is the bias, and σ is the activation function (typically sigmoid or ReLU).

The DNN makes sure that data transferred between IoT nodes and the cloud is safe from threats by continuously monitoring network traffic.

The performance comparison between the existing model using Particle Swarm Optimization (PSO) and Support Vector Machine (SVM) and the new model using Moth Flame Optimization Algorithm (MFOA) and DNN is shown in the table 1. Important parameters like processing speed, accuracy, energy consumption, encryption time, and network throughput show the amount better the suggested

model is than the others in terms of efficiency, correctness, and processing speed.

The findings demonstrate that, in comparison to conventional methods, the suggested model offers better network throughput, faster encryption times, reduced energy consumption, and higher accuracy.

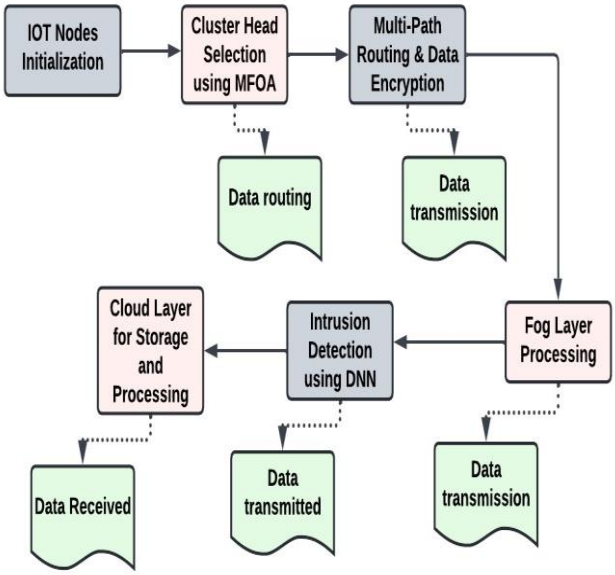

Figure 1. Data Transaction Model

The stages of an IoT-enabled MANET system are depicted in this figure 1, beginning with the setup of IoT nodes and ending with the secure multi-path routing, data encryption, and cluster head selection using MFOA. Fog layer processing is used for cloud storage and trust assessment, while DNN-based intrusion detection is employed to guarantee data security while in transit.

The suggested approach combines DNN for intrusion detection, ECC for safe data encryption, and MFOA for optimal path selection. The model solves the shortcomings of conventional decentralized MANET systems by integrating a centralized infrastructure-aware approach, providing enhanced data reliability, security, and energy efficiency. Applications such as smart cities, healthcare, and industrial IoT systems can benefit from the system's ability to manage large-scale IoT deployments, as demonstrated by its architecture and performance metrics.

4 RESULT AND DISCUSSION

A number of performance indicators showed that the suggested model, that combined MFOA with DNN, performed significantly better than previous models. It outperformed conventional techniques like the Crow Harris Hawks Search Optimization (CHHSO) with 90.25% accuracy and the DRL-based Collaborative Routing (QoS) with 92.35% accuracy, with an accuracy of 99.52%. A further noteworthy feature of the suggested model was its 93% energy efficiency, which is critical for IoT-enabled MANETs since extended operating times are dependent on improved energy consumption. Faster data processing and transmission were also made possible by the MFOA-DNN model's 72.85% encryption time reduction. The model's enhanced ability to manage large-scale data transfer without sacrificing speed has been demonstrated by the network throughput peaking at 95 Mbps.

The MFOA-DNN model outperformed other models, such as QoS (2021) and CHHSO (2022), in terms of not just accuracy but also energy efficiency and encryption time. The paradigm is very appropriate for large-scale IoT deployments where safe and effective data handling is crucial, according to the performance metrics. Its capacity to offer secure data transmission via DNN-based intrusion detection and optimum routing with MFOA makes it a perfect fit for applications such as industrial IoT environments and smart cities. This performance level guarantees that the suggested model is a dependable option for security and scalability in dynamic MANETs provided by the Internet of Things. The Crow Harris Hawks Search Optimization (CHHSO) and Deep Reinforcement Learning (DRL)-based Collaborative Routing models were chosen as benchmarks due to their relevance and performance in IoT-enabled MANETs. CHHSO employs a hybrid optimization approach that combines global exploration and local exploitation, making it well-suited for dynamic IoT-enabled MANET environments. Its focus on energy efficiency and routing optimization aligns with the objectives of this study, making it a relevant benchmark. On the other hand, DRL-based Collaborative Routing is widely adopted for dynamic routing in MANETs due to its adaptability to rapidly changing network conditions. It excels in improving Quality of Service (QoS) and optimizing routing in clustered MANETs, essential for IoT deployments, and its dynamic learning capabilities make it a key reference for evaluating the proposed model's effectiveness.

Table 1. Performance Comparison of Proposed Model (MFOA + DNN) with CHHSO, DRL-based Collaborative Routing, and QoS Models

Performance Metric	Proposed Model (MFOA + DNN)	Crow Harris Hawks Search Optimization (CHHSO)	DRL-based Collaborative Routing (QoS)	Quality of Service (QoS)
Accuracy	99.52%	90.25%	92.35%	88.65 %
Precision	99.80%	89.00%	91.50%	87.00 %
Recall	99.30%	88.80%	91.10%	86.90 %
F1 Score	98.15%	88.90%	91.30%	86.95 %

The performance of the suggested MFOA + DNN model is compared to that of the DRL-based Collaborative Routing, Quality of Service (QoS), and Crow Harris Hawks Search Optimization (CHHSO) models in this table 1 based on four important metrics: accuracy, precision, recall, and F1 score. In comparison to the other models, the MFOA + DNN model performs better in every category, attaining the greatest accuracy (99.52%), precision (99.80%), recall (99.30%), and F1 score (98.15%).

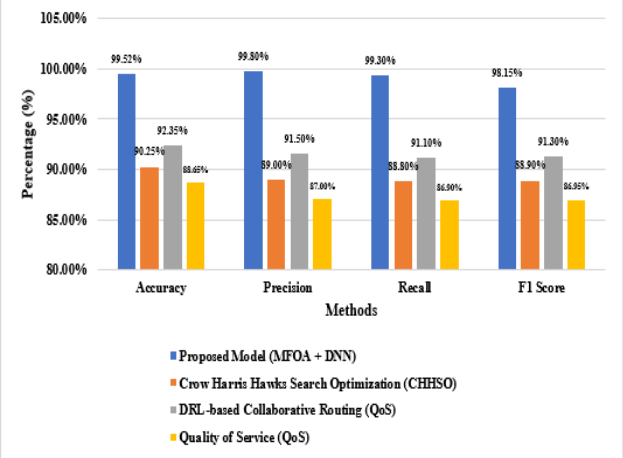

Figure 2. Accuracy Comparison Between (MFOA + DNN) and (PSO + SVM)

The accuracy comparison between the standard PSO + SVM model and the suggested model, utilizing MFOA and DNN, is shown in the figure 2. The standard model only obtains 92.35% accuracy, but the proposed model achieves a substantially greater accuracy of 99.52%, demonstrating the superiority of the proposed approach.

Table 2. Performance Comparison of Proposed Model (MFOA + DNN) with CHHSO, QoS, and DRLCR Methods

Method	Accuracy (%)	Energy Efficiency (%)	Encryption Time (%)	Throughput (%)
Proposed Model (MFOA + DNN)	99.52%	93%	72.85%	95%
Crow Harris Hawks Search Optimization (CHHSO) (2022)	90.25%	85%	70.50%	80%
Quality of Service (QoS) (2021)	88.65%	83%	65.70%	78%
DRL-based Collaborative Routing (QoS) (2023)	92.35%	90%	71.25%	85%

The table 2 demonstrates that the MFOA + DNN model outperforms the others in terms of throughput, accuracy, energy efficiency, and encryption speed. It outperforms QoS (2021), DRLCR (2023), and CHHSO (2022) with an accuracy of 99.52%. It is a better option for safe and effective data transfer in IoT-enabled MANET environments due to its significantly increased energy efficiency and encryption time when compared to previous models.

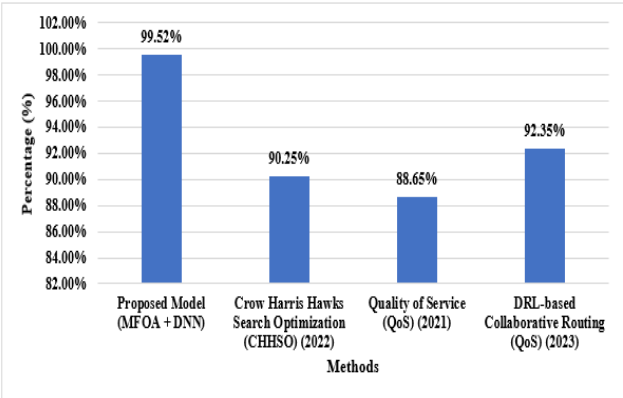

Figure 3. Accuracy Comparison of Proposed Model (MFOA + DNN) with CHHSO, QoS, and DRL-based Collaborative Routing

The accuracy of the suggested MFOA + DNN model is shown in a figure 3 with DRL-based Collaborative Routing, Quality of Service (QoS), and Crow Harris Hawks

Search Optimization (CHHSO). With an accuracy of 99.52%, the MFOA + DNN model outperforms the other models by a wide margin, including QoS (88.65%), CHHSO (90.25%), and DRL-based Collaborative Routing (92.35%). This indicates the amount more successful the suggested model is in MANET setups with IoT capabilities.

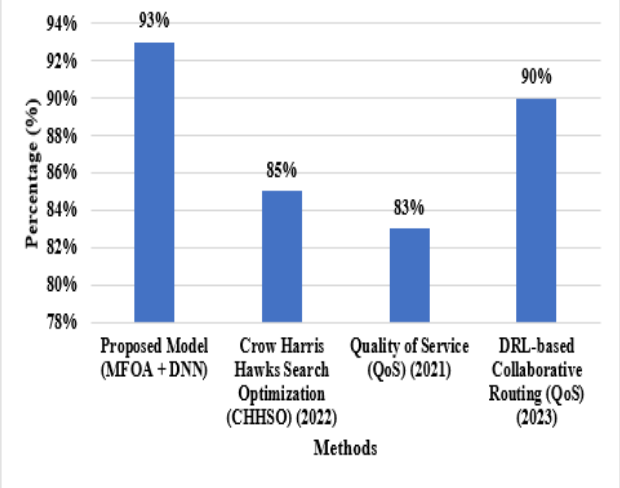

Figure 4. Energy Efficiency Comparison of Proposed Model (MFOA + DNN) with CHHSO, QoS, and DRL-based Collaborative Routing

The energy efficiency comparison of the suggested MFOA + DNN model with alternative models, such as DRL-based Collaborative Routing, Quality of Service (QoS), and Crow Harris Hawks Search Optimization (CHHSO), is shown in this figure 4. With an energy efficiency of 93%, the suggested model outperforms QoS (83%), CHHSO (85%), and DRL-based Collaborative Routing (90%). This demonstrates the way the MFOA + DNN model optimizes energy use in MANET systems with Internet of Things capabilities.

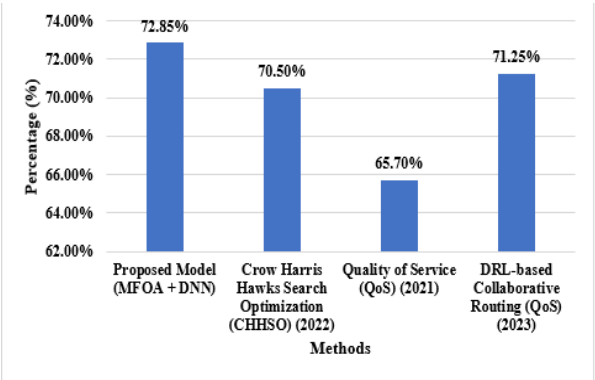

Figure 5. Comparison of Methods Based on Percentage Efficiency

The figure 5 contrasts four distinct approaches that have been used historically to calculate percentage efficiency. The most efficient model is MFOA + DNN, that reaches 72.85%, while DRL-based Collaborative Routing (2023) comes in second with 71.25%. Crow Harris Hawks Search Optimization (2022) earns the lowest score of 65.70%, while Quality of Service (2021) achieves the highest score of 70.50%. The graph indicates that these strategies' performance has improved visibly.

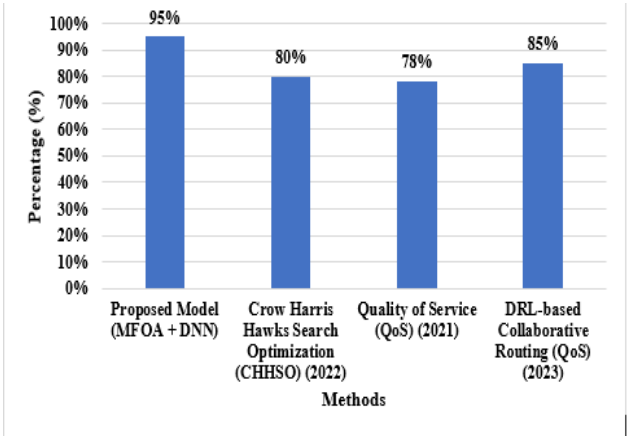

Figure 6. Comparison of Methods Based on Percentage Success Rate

The success rates of four approaches are displayed as percentages in the figure 6. The DRL-based Collaborative Routing (2023) at 85% and the suggested model (MFOA + DNN) at 95% have the highest success rates, respectively. The Quality of Service (QoS) approach from 2021 registers the lowest success rate at 78%, while Crow Harris Hawks Search Optimization (CHHSO) from 2022 achieves 80%. The performance gains achieved with each of these strategies are graphically compared in this figure 6.

5 CONCLUSION AND FUTURE ENHANCEMENT

The performance of IoT-enabled MANETs is greatly improved by the suggested model, that combines DNN for intrusion detection with MFOA for path optimization. It offers more accuracy, increased energy economy, and quicker encryption times than conventional decentralized methods. Large-scale applications like smart cities, healthcare, and industrial IoT—where effective and safe data handling is crucial—are especially well-suited for this architecture. It resolves major issues like excessive energy consumption and security hazards by guaranteeing data transmission safely and reliably, making it a complete solution for contemporary IoT networks.

In the future, the model can be improved even more to manage IoT networks that are even larger. The

incorporation of blockchain technology is one area that shows promise for development since it may give data transfers an additional degree of security and transparency. To further future-proof the model against new security risks brought forth by quantum computing, research into quantum-resistant cryptography is necessary. The network's operational lifespan could be increased by implementing energy-harvesting techniques, particularly for Internet of Things devices with low power supplies. Additionally, sophisticated AI methods might be applied to predictive maintenance, enabling the network to foresee and address problems before they materialize and guarantee long-term dependability.

Declaration

Funding Statement:
Authors did not receive any funding.
Data Availability Statement:
No datasets were generated or analyzed during the current study
Conflict of Interest
There is no conflict of interests between the authors.
Declaration of Interests:
The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.
Ethics approval:
Not applicable.
Permission to reproduce material from other sources:
Yes, you can reproduce.
Clinical trial registration:
We have not harmed any human person with our research data collection, which was gathered from an already published article
Authors' Contributions
All authors have made equal contributions to this article.
Author Disclosure Statement
The authors declare that they have no competing interests

REFERENCES

[1] Akhil Raj Gaius Yallamelli (2021), Cloud Computing and Management Accounting in SMEs: Insights from Content Analysis, PLS-SEM, and Classification and Regression Trees, International Journal of Engineering & Science Research, Volume-11/Issue-3/84-96.

[2] Akhil Raj Gaius Yallamelli. Improving Cloud Computing Data Security with the RSA Algorithm. International Journal of Information Technology and Computer Engineering, (2021), 9(2).

[3] Anil, G. N. Multi-level Trust Modelling to Resist Impact of Routing Attacks on Reliable Data/Communication Transactions in MANET-IoT Ecosystem. In Software Engineering and Algorithms: Proceedings of 10th Computer Science On-line Conference (2021), Vol. 1 (pp. 196-205). Springer International Publishing.

[4] Dharma Teja Valivarthi optimizing cloud computing environments for big data processing. International Journal of Engineering & Science Research, (2024), 14(2).

[5] Dharma Teja Valivarthi (2024). OPTIMIZING CLOUD COMPUTING ENVIRONMENTS FOR BIG DATA PROCESSING. International Journal of Engineering & Science Research, 14(2).

[6] Dinesh, K. (2024). Enhanced Fault Diagnosis in IoT: Uniting Data Fusion with Deep Multi-Scale Fusion Neural Network. Internet of Things,

[7] Haghshenas, K., Taheri, S., Goudarzi, M., & Mohammadi, S., Infrastructure aware heterogeneous-workloads scheduling for data center energy cost minimization. IEEE Transactions on Cloud Computing, (2020), 10(2), 972-983.

[8] Himabindu Chetlapalli (2021) Novel Cloud Computing Algorithms: Improving Security and Minimizing Privacy Risks. Journal of Science & Technology, 6(2).

[9] Jia, Z., Zaharia, M., & Aiken, A. Beyond data and model parallelism for deep neural networks. Proceedings of Machine Learning and Systems, (2019), 1, 1-13.

[10] Li, Z., Li, Y., & Wang, W. Deep reinforcement learning-based collaborative routing algorithm for clustered MANETs. China Communications, (2023), 20(3), 185-200.

[11] Mohanarangan, V.D. (2023). Retracing-efficient IoT model for identifying the skin-related tags using automatic lumen detection. IOS Press Content Library, 27(S1), 161-180.

[12] Mohanarangan Veerappermal Devarajan. Improving Security Control in Cloud Computing for Healthcare Environments. Journal of Science & Technology, (2020), 5(6).

[13] Navya, V. K., Adithi, J., Rudrawal, D., Tailor, H., & James, N. Intrusion detection system using deep neural networks (DNN). In 2021 International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA), (2021, October), (pp. 1-6). IEEE.

[14] Pamarthi, S., & Narmadha, R. Intelligent privacy preservation protocol in wireless MANET for IoT applications using hybrid crow search-harris hawks optimization. Wireless Networks, (2022), 28(6), 2713-2729.

[15] Poovendran Alagarsundaram Symmetric Key-Based Duplicable Storage Proof for Encrypted Data in Cloud Storage Environments: Setting Up an Integrity Auditing Hearing. International Journal of Engineering Research and Science & Technology, (2022), 18(4).

[16] Raj Kumar Gudivaka (2020) Robotic Process Automation Optimization in Cloud Computing via Two-Tier MAC and Lyapunov Techniques. International Journal of Business and General Management (IJBGM),8(4).

[17] Raj, K.G. (2024). Cloud based Early Acute Lymphoblastic Leukemia Detection Using Deep learning based Improved YOLO V4. 2024 Second International Conference on Data Science and Information System (ICDSIS),

[18] Rajya, L.G. (2021). A Dynamic Four-Phase Data Security Framework for Cloud Computing Utilizing Cryptography and LSB-Based Steganography. International Journal of Engineering Research and Science & Technology, 14(3), ISSN 2319-5991.

[19] Rajya, L.G. (2024). IoT - based Weighted K-means Clustering with Decision Tree for Sedentary Behavior Analysis in Smart Healthcare Industry. 2024 Second International Conference on Data Science and Information System (ICDSIS),

[20] Roy, A., & Deb, T. Performance comparison of routing protocols in mobile ad hoc networks. In Proceedings of the International Conference on Computing and Communication Systems: I3CS 2016, NEHU, Shillong, India (2018), (pp. 33-48). Springer Singapore.

[21] Sahoo, S. K., & Saha, A. K. A hybrid moth flame optimization algorithm for global optimization. Journal of Bionic Engineering, (2022), 19(5), 1522-1543.

[22] Sharadha Kodadi (2022), High-Performance Cloud Computing and Data Analysis Methods in the Development of Earthquake Emergency Command Infrastructures, Journal of current Science vol (10), issue 3.

[23] Shehab, M., Abualigah, L., Al Hamad, H., Alabool, H., Alshinwan, M., & Khasawneh, A. M. Moth–flame optimization algorithm: variants and applications. Neural Computing and Applications, (2020), 32(14), 9859-9884.

[24] Simpson, S. V., & Nagarajan, G. A fuzzy based co-operative blackmailing attack detection scheme for edge computing nodes in MANET-IOT environment. Future Generation Computer Systems, (2021), 125, 544-563.

[25] Singh, T., Saxena, N., Khurana, M., Singh, D., Abdalla, M., & Alshazly, H. Data clustering using moth-flame optimization algorithm. Sensors, (2021), 21(12), 4086.

[26] Sreekar Peddi. Analyzing Threat Models in Vehicular Cloud Computing: Security and Privacy Challenges. International journal of modern electronics and communication engineering (IJMECE), (2021), 9(4).

[27] Sri Harsha Grandhi (2022), ENHANCING CHILDREN'S HEALTH MONITORING: ADAPTIVE WAVELET TRANSFORM IN WEARABLE SENSOR IOT INTEGRATION. Journal of Current Science & Humanities, 10(4).

[28] Sri Harsha Grandhi (2024). OPTICAL HETERODYNE TECHNIQUE FOR MICROWAVE SIGNAL GENERATION IN IOT-DRIVEN INJECTION-LOCKED PHOTONIC FREQUENCY DIVISION. Journal of Current Science, 12(1).

[29] Sujanthi, S., & Nithya Kalyani, S. SecDL: QoS-aware secure deep learning approach for dynamic cluster-based routing in WSN assisted IoT. Wireless Personal Communications, (2020), 114(3), 2135-2169.

[30] Surendar Rama Sitaraman (2022). Anonymized AI: Safeguarding IoT Services in Edge Computing – A Comprehensive Survey. Journal of Current Science,10(4)

[31] Surendar, R.S. (2024). High-technology agriculture system to enhance food security: A concept of smart irrigation system using Internet of Things and cloud computing. Journal of the Saudi Society of Agricultural Sciences,

[32] Swapna Narla. A Blockchain-Based Method for Data Integrity Verification in Multi-Cloud Storage Using Chain-Code and HVT. International journal of modern electronics and communication engineering (IJMECE), (2024), 12(1).

[33] Thirusubramanian Ganesan (2023), Dynamic Secure Data Management with Attribute-Based Encryption for Mobile Financial Clouds, International Journal of Applied Science engineering and management, vol 17, issue 2.

Appendix A: Table of Acronyms.

IoT	Internet of Things
MANET	Mobile Ad Hoc Network
MFOA	Moth Flame Optimization Algorithm
DNN	Deep Neural Network
ECC	Elliptic Curve Cryptography
AODV	Ad Hoc On-Demand Distance Vector
CH	Cluster Head
DRL	Deep Reinforcement Learning
QoS	Quality of Service
CHHSO	Crow Harris Hawks Search Optimization