CMHAA: Context Management and Hierarchical Addressing Architecture for Scalable IoT in the Future Internet

*Dr. Prasad Prakash Lokulwar[1] and Dr. Ganesh Khekare[2]**

[1]Postdoctoral Researcher, Lincoln University College, Petaling Jaya, Selangor Darul Ehsan- 47301, Malaysia;

[2] Department of Computer Science & Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu, India

pdf.prasad@lincoln.edu.my, khekare.123@gmail.com*

Abstract— The increasing adoption of the Internet of Things (IoT) and Future Internet has brought about new challenges in device management, scalability and efficient communication across heterogeneous devices. IoT systems typically use flat addressing methods and do not support contextual information processing, resulting in higher transmission costs, poor device organization, and insufficient scalability for big IoT networks. To overcome such limitations, this paper proposes a novel Context Management and Hierarchical Addressing Architecture (CMHAA). In the CMHAA approach, context acquisition, context processing, device categorization, clustering of devices based on context awareness, and hierarchical address assignment schemes are incorporated into an integrated architecture. The use of contextual parameters such as device type, residual energy, mobility, location, and QoS requirement helps in intelligent organization of devices. Additionally, the hierarchical addressing system can help provide address aggregation, simplify lookup procedures, and enhance communication efficiency. This proposed scheme was simulated using heterogeneous IoT applications consisting of up to 1000 nodes on MATLAB. Based on the experimental findings, the proposed CMHAA scheme provided a scalability of 95.6%, context processing accuracy of 97.4%, device classification accuracy of 96.2%, and address allocation efficiency of 98.8% while minimizing communication costs and address lookup costs. Therefore, the findings suggest that the proposed approach can form an efficient basis for next-generation Future Internet-based IoT systems.

Keywords — Cluster-Based Routing, Context-Aware IoT, Intelligent Routing, Energy Efficiency, Network Lifetime, Adaptive Routing, Wireless Sensor Networks, MATLAB Simulation.

Introduction

The Internet of Things (IoT) has been identified as one of the basic components behind the construction of the Future Internet through the provision of easy interconnection between billions of devices and smart objects. IoT systems are being used in a wide range of areas such as smart cities, health care, manufacturing industries, transportation, environment monitoring, and energy efficiency management. The rising number of devices in IoT systems has created several challenges with regard to effective communication and resource utilization, and thus, there is an increasing focus on designing intelligent networking systems.

Communication efficiency is vital in IoT networking, and it can be achieved by utilizing an effective routing technique. However, traditional methods of routing tend to experience challenges when dealing with the unpredictable and constrained environment in which IoT networks operate, thus causing high communication costs, energy utilization, and network lifetime. Some researchers have explored the application of artificial intelligence and energy-aware routing schemes for optimizing the efficiency of large-scale IoT networks [1]. Additionally, research findings have suggested that context-based routing strategies have the capacity to boost efficiency in communication by taking into consideration factors such as device status and QoS levels [2].

In addition to routing difficulties, the fast deployment of IoT infrastructure has generated a lot of concerns with regard to scalability and addressing schemes. Most of the schemes that exist in the current IoT communication systems are based on a flat address design scheme, which will be more and more inefficient in terms of the number of connected devices. This might result in higher routing complexity, more lookup burden and inefficiency of resource utilization. Research studies on energy-efficient routing protocols point out the need to design a communication architecture that supports scalability in heterogeneous environments [3]. Similarly, literature surveys of IoT routing systems emphasize the importance of efficient organization and management of the network [4].

Another difficulty to be dealt with in Future Internet systems is how to efficiently leverage the context information generated by IoT nodes. The type of the IoT node, its energy capacity, location, communication behavior, sensing capability and application demands are all context information that can help to optimize the network processes. The problem is that most of the present solutions merely address routing concerns without delivering any aid to handle context information and categorize devices. This becomes even harder in mobile IoT scenarios where topology may change dynamically [5].

In response to these challenges, this paper presents a Context Management and Hierarchical Addressing Architecture (CMHAA) that is suitable for the scalable operation of IoT networks in the Future Internet. The context management scheme, together with the hierarchical addressing scheme in the presented architecture, facilitates the effective classification of devices, aggregating their addresses, and managing communications among them. Through the classification of IoT devices based on contexts, the proposed solution is expected to be able to simplify the process of addressing, scaling up, and improving efficiency in the operation of the network. The architecture lays a platform for future developments in the domain of trust management, authentication, and secure routing mechanisms for large-scale context-aware IoT settings.

The rest of the paper is structured as follows. In Section II, a review of the related literature of existing context-aware and scalable IoT communication methods will be described. The proposed Context Management and Hierarchical Addressing Architecture will be discussed in Section III. The findings will be discussed in Section IV and concluded in Section V.

Related Work

An IoT security architecture design that incorporated trusted execution environment, semantic middleware, and blockchain techniques was proposed and examined using cryptographic efficiency, detection efficiency, and energy consumption parameters to show successful cross-layer security as well as its feasibility in resource-constrained IoT applications [6]. A trust-aware IoT routing approach that used Rider Foraging Optimization clustering along with Deep Reinforcement Learning routing secured a throughput of 17,560 kbps, 98.9 percent packet delivery ratio, and 68 percent energy consumption, thereby performing better than multiple existing IoT routing strategies in terms of performance, especially when simulated on larger networks [7]. A simulation analysis of the routing protocols of RPL, AODV, and LOADng on different 6LoWPAN structures using Cooja Simulator proved that the RPL protocol had minimal energy consumption compared to others [8]. The proposed adaptive clustering and trust aware routing (ACTAR) mechanism based on hybrid clustering, multi objective cluster head selection, and trust aware routing has enhanced malicious nodes' detection, packet delivery ratio, residual energy, and false positive detection over the state-of-the-art IoT-WSN routing techniques [9]. A context aware trust and reputation routing (CATR) scheme using the beta distribution based trust evaluation model and context based information has improved opportunistic IoT communications by decreasing latency, dropping messages, and number of hops by 22%, 15%, and 9%, respectively, over the state-of-the-art routing schemes [10]. Bio-inspired hybrid BOA-PSO routing scheme incorporating energy aware clustering and optimal path selection has increased residual energy by 17% and has improved throughput by 60% while decreasing packets drop by 60% and network lifetime extended from 10% to 20% over the benchmark routing techniques in disaster oriented IoT applications [11]. A hybrid routing scheme based on fuzzy clustering and PSO for cluster head selection has decreased energy consumption by 52%, increased throughput by 112%, packet delivery ratio by 83%, and extended network lifetime by 48% over the existing DEEC and LEACH algorithms [12].

Traffic-aware cluster-based routing protocol using the metrics of residual energy, traffic load, and distance during cluster-head and next-hop node selections was able to provide superior packet delivery ratio, low delays, energy savings, and lifetime of network in comparison with LoRaWAN under different network scenarios [13]. A scalable context-aware classification model based on dynamically switchable micro-classifier provided a better optimization of classifier selection and led to improvements in classification accuracy, computational efficiency, and latency in diverse IoT platforms [14]. Context-based classification and clustering technique for device clustering with the use of device characteristics such as device attribute, location, time, and communication provided dynamic clustering and leadership of cluster in IoT environment [15]. The proposed cluster-based approach for trusted routing that incorporates weighted trust evaluation, fire hawk optimizer-based clustering algorithm, and trusted routing within clusters outperformed existing approaches for secure routing in WSNs in terms of energy consumption, throughput, latency, packet loss, detection ratio, and routing accuracy [16]. The comparison of AODV and RPL using throughputs, packet delivery ratios, and end-to-end delays through simulations revealed the higher effectiveness of RPL in terms of packet delivery rate and throughputs for IoT communication networks [17]. The use of an enhanced routing technique based on RPL with security, including node authentication, multiple context parent selection, intelligent congestion management, deep packet inspection, and trickle timer mechanisms increased packet delivery ratio, load balancing, energy efficiency, delay, packet loss, and control overhead in IoT networks with malicious nodes [18].

The design of a static hub cluster-based routing protocol that combines clustering and multipath routing was able to eliminate unnecessary data transfers, reduce the cost associated with transmitting control packets, lower energy costs, and increase the operational lifetime of WSN-powered IoT [19]. The use of a trust-based routing scheme through trust-based clustering, mobile edge computing, Gray Wolf Optimization, and Artificial Bee Colony algorithm provided an improvement in trust levels by 58%, increased malicious node detection rates by 96.7%, and increased routing accuracy by 91.96% in IoT-based sensor networks [20]. A trust-aware clustering and routing system design that employs Bald Eagle Search optimization, trust-based clustering, and multi-objective routing provided better lifetime, stable period, and node survivability [21]. A QoS-aware clustering and multihop routing protocol based on an ensemble metaheuristic optimization using cross-entropy rain and oppositional chaos game optimization achieved higher levels of energy savings and network lifetime than traditional IoT-assisted WSN routing protocols [22]. The use of a load balancing approach to clustering and energy aware routing based on a 1.2-approximation algorithm and traffic segmentation enhanced scalability and communication efficiency in large IoT-enabled WSNs [23]. A context recognition optimization approach employing adaptive sensing node configurations, duty cycling, and multi-objective optimization saved up to 95% of energy consumption with high recognition rates [24].

Various research studies have already addressed the communication within the scope of IoT using trust-aware routing protocols, cluster-based optimization, context-aware classification, congestion control and energy-efficient routing protocols [6]–[24]. Even though such solutions have yielded positive results for enhancing the performance, reliability, security and energy consumption of wireless networks, most of them have concentrated only on routing algorithms optimization, trust assessment, clustering procedures, or context awareness as individual modules. Moreover, the issue of combining complete context management with scalable hierarchical addressing has not been considered widely by existing research solutions in order to effectively group heterogeneous IoT nodes in Future Internet environments [14], [15], [24]. It also should be mentioned that the issue of designing a unified approach to context management, device classification, context processing and address aggregation for simplifying and optimizing communications has not been explored. Consequently, an architecture providing the combination of these features should be developed.

Methodology

The Context Management and Hierarchical Addressing Architecture (CMHAA) architecture that is proposed would enhance the scalability and performance of IoT in the future internet environment. The architecture is composed of the following processes: context collection, context management, device classification, and hierarchical address allocation, as depicted in Figure 1.

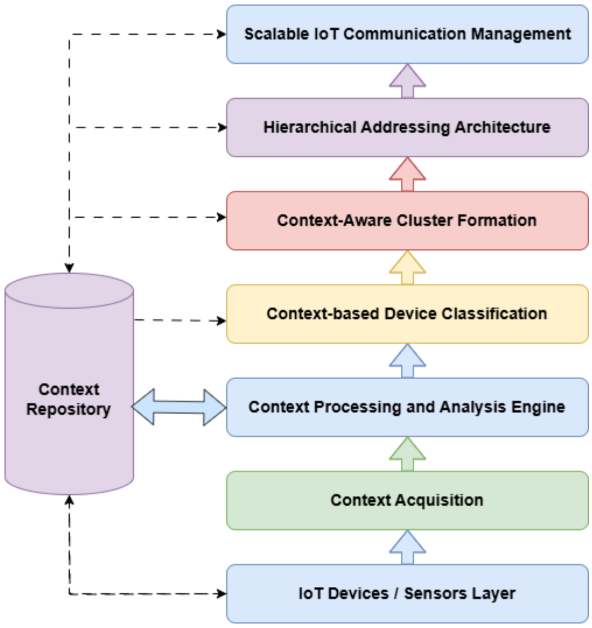

Figure 1. Proposed Context Management and Hierarchical Addressing Architecture (CMHAA) for scalable IoT communication in the Future Internet

Context Acquisition

The role of the context acquisition module is to gather contextual data from various types of IoT devices present in the future Internet environment. The device provides data in periodic intervals in terms of operational characteristics like remaining energy, type of device, location, mobility, communication frequency, and QoS requirement. All these help understand the current condition of the network and aid in making intelligent decisions. Because of the dynamics of the IoT environment, gathering context data helps adapt the architecture to the changes happening within the network. The context vector of IoT device *di* can be denoted by:

$$C_i = \{E_i, L_i, M_i, T_i, Q_i\}$$

Where:

- *Ei* = Residual Energy
- *Li* = Location Information
- *Mi* = Mobility Status
- *Ti* = Device Type

- Qi = QoS Requirement

The collected context information is forwarded to the Context Processing Engine for further analysis.

Context Processing and Analysis Engine

Context Processing Engines remove redundant and incomplete data from the acquired data on context. Extraction of features takes place to extract the most important feature affecting communication and device management. The idea here is to minimize overhead while still preserving meaningful data about context. A normalized value of the context is computed using:

$$C_{norm} = \frac{C_i - C_{min}}{C_{max} - C_{min}}$$

where Ci represents the current contextual parameter value.

With normalized context information, comparisons among devices with varying attributes can be made objectively. The processed context information is converted into context profiles which represent the attributes of the specific devices.

Context-Based Device Classification

Classification of devices takes place after feature extraction based on the context information of devices. This makes network administration easier by enabling efficient communication management. The context score of a device is determined using:

$$CS_i = w_1E_i + w_2Q_i + w_3M_i + w_4L_i$$

Where

$$w_1 + w_2 + w_3 + w_4 = 1$$

And wi represents the importance assigned to each contextual parameter.

The classification of devices as sensor nodes, actuator nodes, mobile devices, or gateway nodes is based on their context scores. This kind of classification helps in effective management of network resources.

Context-Aware Cluster Formation

To make the system scalable, the similar devices are clustered together to reduce communication overhead in the network. Context aware clustering makes the network scalable and manageable. The similarity between two devices is calculated using Euclidean Distance:

$$D(i,j) = \sqrt{\sum_{k=1}^{n} (C_{ik} - C_{jk})^2}$$

where:

- Cik = kth context attribute of device i
- Cjk = kth context attribute of device j

Devices with minimum distance values are grouped into the same cluster. The cluster representative is selected using:

$$CH = \max(CS_i)$$

where the device with the highest context score becomes the cluster representative.

Hierarchical Address Assignment Hierarchical Addressing Architecture

The architecture is proposed with hierarchical addressing to overcome the scalability difficulties of flat addressing systems. Hierarchical addressing provides address aggregation, simplifies routing table management, and provides efficient identification of the devices. The structure of the address is specified as:

$$HA = \{FI, CID, DT, NID\}$$

where:

- FI = Future Internet Domain ID

- *CID* = Cluster ID
- *DT* = Device Type Identifier
- *NID* = Node Identifier

An example address format is:

$$FI01.C05.SEN.102$$

The hierarchical structure facilitates scalable device management and lowers lookup complexity.

Context Repository Update

Every IoT device that has registered with the system has its addressing hierarchy and contextual profile stored in the context repository. Every time a device's state changes, the repository is updated. The context repository's update rate is:

$$UF = \frac{N_u}{T}$$

where:

- *Nu* = Number of context updates
- *T* = Observation time

Good repository management ensures that communication choices are made using the most up-to-date contextual information.

Scalable Communication Support

In the final phase, the use of context profiles and hierarchical addressing schemes makes communication among IoT devices scalable. Instead of broadcasting data throughout the whole network, only those clusters and addresses that matter can communicate. Communication cost is given by:

$$CO = \frac{N_m}{N_d}$$

where:

- Nm = Number of control messages
- Nd = Number of data packets

The suggested architecture is designed to decrease communication overhead and improve scalability and device accessibility. The proposed algorithm for CMHAA is as follows:

Algorithm: Context Management and Hierarchical Addressing Architecture (CMHAA)
Input: Input: IoT Device Set D *Output:* Context-aware classified devices with hierarchical addresses
Procedure: *Step 1:* Collect contextual parameters from each device *Step 2:* Perform context preprocessing *Step 3:* Extract contextual features *Step 4:* Classify devices based on context profile *Step 5:* Form context-aware clusters *Step 6:* Generate Cluster IDs *Step 7:* Assign hierarchical addresses *Step 8:* Store context and address information. *Step 9:* Update context dynamically

Step 10: Support scalable communication using hierarchical addressing

Experimental Results and Discussion

The suggested CMHAA architecture is tested using MATLAB R2024a. In an effort to examine the efficiency of the suggested design architecture, a large heterogeneous network of sensors, actuators, mobile devices and gateway nodes has been simulated. For this, the simulation space is chosen to be a square network field of size 1000 m × 1000 m and IoT devices range from 100 to 1000 nodes. The Context Management Engine for context acquisition, feature extraction and IoT devices classification is implemented using MATLAB scripts and the Hierarchical Addressing Module is designed to generate cluster-based hierarchical addresses and to manage address aggregation. The parameters of the simulation environment are provided in Table 1.

TABLE I. SIMULATION PARAMETERS

Parameter	Value
Network Area	1000x1000 m^2
Number of Nodes	100-1000
Cluster Formation	Context-Aware Clustering
Addressing Method	Hierarchical Addressing
Simulation Runs	20

We assess the proposed CMHAA architecture using the following metrics: Scalability Index (SI), Address Allocation Efficiency (AAE), Context Processing Accuracy (CPA), Communication Overhead Reduction (COR) and Average Address Lookup Time (ALT). These metrics give a detailed evaluation of the performance of the proposed Context Management and Hierarchical Addressing Architecture for scalable IoT communication in Future Internet.

$$SI = \frac{N_{supported}}{N_{total}}$$

$$AAE = \frac{N_{assigned}}{N_{requests}} * 100$$

$$CPA = \frac{N_{correct}}{N_{processed}} * 100$$

$$COR = \frac{CO_{existing} - CO_{proposed}}{CO_{existing}} * 100$$

$$ALT = \frac{\sum_{i=1}^{n} T_i}{n}$$

By increasing the number of IoT devices from 100 to 1000, the scalability performance was examined. The scalability behavior of the suggested CMHAA architecture in comparison to traditional flat addressing methods is shown in Table II.

TABLE II. SCALABILITY ANALYSIS

Number of Devices	Flat Addressing (%)	Proposed CMHAA (%)
100	91.8	98.5

250	86.7	97.9
500	79.2	97.1
750	71.4	96.3
1000	64.5	95.6

The findings show that even in dense network installations, the suggested hierarchical addressing scheme retains a scalability level above 95%. Context-based clustering and address aggregation, which greatly reduce address management complexity, are primarily responsible for the performance gain. As indicated in Table III, communication overhead was calculated as the ratio of control packets produced during address management and context updates.

TABLE III. COMMUNICATION OVERHEAD ANALYSIS

Method	Communication Overhead (%)
Traditional Flat Addressing	32.1
Cluster-Based Architecture	25.4
Proposed CMHAA	17.2

The MATLAB simulation results show that the suggested design reduces the communication overhead by about 46% compared to the conventional flat addressing systems. The reduction is achieved by processing the local environment and assigning hierarchical addresses. Efficient address resolution is of key importance for scaled IoT connection. The average address lookup time is evaluated for different network sizes as indicated in Table IV.

TABLE IV. ADDRESS LOOKUP TIME ANALYSIS

Number of Devices	Conventional (ms)	Proposed CMHAA (ms)
100	7.5	2.8
250	11.3	3.6
500	17.2	4.3
750	22.4	5.1
1000	28.8	5.8

The results show that the proposed hierarchical addressing architecture substantially reduces lookup latency because address aggregation minimizes search operations across the network. The effectiveness of the Context Management Engine was evaluated using classification accuracy and context processing efficiency, as shown in Table V.

TABLE V. CONTEXT PROCESSING PERFORMANCE

Metrics	Value (%)
Context Processing Accuracy	97.4
Device Classification Accuracy	96.2
Context Update Success Rate	98.1
Address Allocation Efficiency	98.8

The obtained results demonstrate that the proposed architecture effectively manages heterogeneous contextual information while maintaining high accuracy in device classification and address assignment. Since the proposed work focuses on context management, device classification, clustering support, and hierarchical addressing, the comparison is performed against the most relevant studies from the literature, as shown in Table VI.

TABLE VI. COMPARATIVE ANALYSIS WITH EXISTING METHODS

Method	Methodology	Scalability Support	Context Awareness	Results
TrustRIDR-Net [7]	Trust-Aware Routing	Medium	Partial	PDR = 98.9%
ACTAR [9]	Trust-Aware Clustering	Medium	No	Improved PDR & Energy
CACTUS [14]	Context Classification	Medium	Yes	Improved Accuracy & Latency
Context-Based Clustering [15]	Device Classification	Medium	Yes	Dynamic Clustering
Sec-RPL [18]	Multi-Context Routing	Medium	Yes	Reduced Delay & Packet Loss
CRPSH [19]	Cluster Routing	Medium	No	Improved Network Lifetime
Proposed CMHAA	Context + Addressing	High	Yes	Scalability = 95.6%, AAE = 98.8%

The suggested CMHAA architectural model differs greatly from the available solutions since they only concentrate on network routing and scalability, while the presented solution also concentrates on network addressing and scalability. Such models as TrustRIDR-Net [7], ACTAR [9], and Sec-RPL [18] apply contextual data analysis and trust computation. However, they do not feature any specific hierarchical addressing system. In their turn, the CACTUS model [14] and a contextual clustering solution [15] feature both classification and clustering but do not address aggregation and device identification solutions.

The experimental findings suggest that the context-processing accuracy, address allocation efficiency, and scalability achieved by CMHAA reach 97.4%, 98.8%, and 95.6%, respectively, while communication overhead becomes just 17.2% for networks consisting of up to 1000 IoT devices. Thus, the obtained results show that the integration of contextual management with hierarchical addressing makes it possible to create effective large-scale future internet systems.

The outcomes generated by simulations on MATLAB prove the efficiency of the proposed CMHAA. The integration of context acquisition, device categorization, context-aware clustering, and hierarchical addressing in one system increases the scalability of the system, addresses efficiency, and enhances communication. While other systems have concentrated mainly on routing, clustering, or evaluating trust among nodes, the proposed approach provides a scalable infrastructure for addressing and context management, which can then be used to implement trust-aware routing, authentication, and access control in subsequent studies. This makes the architecture highly suitable for next-generation IoT and Future Internet infrastructures.

Conclusions

Problem Statement Addressed / Motivation: The proposed CMHAA addresses the challenges of scalability, efficient device management, context management, and communication in large-scale IoT networks.

Method Used: The architecture integrates context acquisition, context processing, device classification, context-aware clustering, and hierarchical addressing, and was evaluated using MATLAB simulation and comparative analysis.

Key Findings: CMHAA achieved 95.6% scalability, 97.4% context processing accuracy, 96.2% device classification accuracy, and 98.8% address allocation efficiency, demonstrating improved performance over existing routing and clustering techniques.

Limitations and Future Work: The work is mainly simulation-based and has limited consideration of security and real-world deployment. Future work will incorporate trust management, secure routing, authentication, context-aware access control, and validation through real-world IoT testbeds.

References

[1] S. Thakur *et al*., "AI-driven energy-efficient routing in IoT-based wireless sensor networks: A comprehensive review," *Sensors*, vol. 25, no. 24, Art. no. 7408, 2025, doi: 10.3390/s25247408.

[2] A. M. Khedr, O. Alfawaz, P. R. P. V., and W. Osamy, "Advancing IoT-driven WSNs with context-aware routing: A comprehensive review," *Comput. Sci. Rev.*, vol. 58, Art. no. 100803, 2025, doi: 10.1016/j.cosrev.2025.100803.

[3] N. R. Saadallah and S. A. Alabady, "A comprehensive study on energy-efficient-based routing protocols in the Internet of Things Part I: Definition and classification," *Iran J. Comput. Sci.*, vol. 7, pp. 631–661, 2024, doi: 10.1007/s42044-024-00180-1.

[4] M. R. Poornima *et al*., "Holistic survey on energy-aware routing techniques for IoT applications," *J. Netw. Comput. Appl.*, vol. 213, Art. no. 103584, 2023, doi: 10.1016/j.jnca.2023.103584.

[5] Z. Shah *et al*., "Routing Protocols for Mobile Internet of Things (IoT): A Survey on Challenges and Solutions," *Electronics*, vol. 10, no. 19, Art. no. 2320, 2021, doi: 10.3390/electronics10192320.

[6] M. Imran, "Architecting Trust: A Framework for Secure IoT Systems Through Trusted Execution and Semantic Middleware," in *Proc. IEEE 15th Int. Conf. Commun. Syst. Netw. Technol. (CSNT)*, Al-Khobar, Saudi Arabia, 2026, pp. 507–513, doi: 10.1109/CSNT69054.2026.11502525.

[7] S. Shafiuddin and K. H. Krishna, "TrustRIDR-Net: A Hybrid Trust-Aware Routing Framework Using RFO and DRL for Scalable IoT Networks," *Eng. Technol. Appl. Sci. Res.*, vol. 15, no. 5, pp. 27421–27429, Oct. 2025, doi: 10.48084/etasr.12294.

[8] P. S. Chia *et al*., "Routing Protocols Performance on 6LoWPAN IoT Networks," *IoT*, vol. 6, no. 1, 2025, doi: 10.3390/iot6010012.

[9] V. Nagamani and K. Annapurna, "Adaptive Clustering and Trust Aware Routing (ACTAR) for Wireless Sensor Networks in IoT Environments," *Int. J. Commun. Syst.*, vol. 38, no. 2, Art. no. e6083, 2024, doi: 10.1002/dac.6083.

[10] J. Singh *et al*., "Context-aware trust and reputation routing protocol for opportunistic IoT networks," *Sensors*, vol. 24, no. 23, 2024, doi: 10.3390/s24237650.

[11] S. Ahmed *et al*., "Bio-inspired energy-efficient cluster-based routing protocol for the IoT in disaster scenarios," *Sensors*, vol. 24, no. 16, Art. no. 5353, 2024, doi: 10.3390/s24165353.

[12] C. Lei, "An energy-aware cluster-based routing in the Internet of Things using particle swarm optimization algorithm and fuzzy clustering," *J. Eng. Appl. Sci.*, vol. 71, Art. no. 135, 2024, doi: 10.1186/s44147-024-00464-0.

[13] H. Gul *et al.*, “A traffic-aware and cluster-based energy efficient routing protocol for IoT-assisted WSNs,” *Comput. Mater. Continua*, vol. 80, no. 2, pp. 1831–1850, 2024, doi: 10.32604/cmc.2024.052841.

[14] M. M. Rastikerdar, J. Huang, S. Fang, H. Guan, and D. Ganesan, “CACTUS: Dynamically Switchable Context-aware Micro-Classifiers for Efficient IoT Inference,” in *Proc. ACM Int. Conf. Mobile Syst., Appl., Services (MobiSys)*, 2024, pp. 505–518, doi: 10.1145/3643832.3661888.

[15] P. More and S. Sakhare, “Context-Aware Device Classification and Clustering for Smarter and Secure Connectivity in Internet of Things,” *EAI Endorsed Trans. Ind. Netw. Intell. Syst.*, vol. 10, no. 3, Art. no. e5, Oct. 2023, doi: 10.4108/eetinis.v10i3.3874.

[16] M. Hosseinzadeh *et al.*, “A cluster-based trusted routing method using fire hawk optimizer (FHO) in wireless sensor networks,” *Sci. Rep.*, vol. 13, no. 1, Art. no. 13046, 2023, doi: 10.1038/s41598-023-40273-8.

[17] C. Thiagarajan and P. Samundiswary, “Performance Comparison of Routing Protocols for IoT,” in *Proc. 2nd Int. Conf. Smart Technol. Syst. Next Gener. Comput. (ICSTSN)*, Villupuram, India, 2023, pp. 1–5, doi: 10.1109/ICSTSN57873.2023.10151577.

[18] M. M. Sithik and B. M. Kumar, “Intelligent agent-based virtual clustering and multi-context aware routing for congestion mitigation in secure RPL-IoT environment,” *Ad Hoc Netw.*, vol. 137, Art. no. 102972, 2022, doi: 10.1016/j.adhoc.2022.102972.

[19] R. K. Lenka *et al.*, “Cluster-based routing protocol with static hub (CRPSH) for WSN-assisted IoT networks,” *Sustainability*, vol. 14, no. 12, Art. no. 7304, 2022, doi: 10.3390/su14127304.

[20] A. Saleh *et al.*, “Trust-Aware Routing Mechanism through an Edge Node for IoT-Enabled Sensor Networks,” *Sensors*, vol. 22, no. 20, Art. no. 7820, 2022, doi: 10.3390/s22207820.

[21] K. Nagappan, S. Rajendran, and Y. Alotaibi, “Trust Aware Multi-Objective Metaheuristic Optimization Based Secure Route Planning Technique for Cluster Based IIoT Environment,” *IEEE Access*, vol. 10, pp. 112686–112694, 2022, doi: 10.1109/ACCESS.2022.3211971.

[22] A. K. Dutta *et al.*, “Design of QoS-aware routing protocol for IoT-assisted clustered WSN,” *Comput. Mater. Continua*, vol. 71, no. 2, pp. 3785–3801, 2021, doi: 10.32604/cmc.2022.023657.

[23] R. Yarinezhad and M. Sabaei, “An optimal cluster-based routing algorithm for lifetime maximization of Internet of Things,” *J. Parallel Distrib. Comput.*, vol. 156, pp. 7–24, 2021, doi: 10.1016/j.jpdc.2021.05.005.

[24] V. Janko and M. Luštrek, “A General Framework for Making Context-Recognition Systems More Energy Efficient,” *Sensors*, vol. 21, no. 3, Art. no. 766, 2021, doi: 10.3390/s21030766.