IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, March 2026
Impact Factor: 8.2

A Multi-Layered Soft Computing Framework for Intelligent Threat Detection in Decentralized IoT Networks

Dr Chukka Santhaiah and G Thulasiram
Department of CSE, Siddartha Educational Academy Group of Institutions, Tirupati, India
Department of CSE (Cyber-Security), S V College of Engineering, Tirupati, India
g.thulasiramreddy@gmail.com, chukka.santh@gmail.com

Abstract: *At its core, the Perception & Authentication Layer employs Fuzzy Logic to dynamically compute Trust Scores for incoming device data, effectively filtering anomalous or malicious requests at the network periphery by modeling inherent uncertainties in authentication signals. The Intelligent Processing Layer advances this with hybrid heuristic techniques, such as Genetic Algorithms for evolutionary optimization and Swarm Intelligence for collaborative pattern mining, to discern subtle traffic anomalies and unprecedented zero-day threats that evade signature-based detectors. Culminating in the Adaptive Response Layer, the architecture autonomously orchestrates decentralized responses, isolating compromised nodes via a consensus-driven notification protocol to preempt lateral propagation across the network.*

By prioritizing soft computing over rigid hard-computing models, the framework achieves superior scalability, energy efficiency for battery-operated IoT endpoints, and robustness in dynamic topologies. This conceptual advancement aligns with NCASCTE-2026's emphasis on interdisciplinary societal applications, paving the way for resilient decentralized IoT infrastructures without necessitating extensive hardware upgrades or model retraining.The rapid proliferation of Internet of Things (IoT) devices in decentralized networks, such as smart cities and industrial ecosystems, has exposed critical vulnerabilities to cyber threats, including zero-day attacks and distributed denial-of-service (DDoS) incursions. Traditional centralized security paradigms falter in these environments due to inherent latency, single points of failure, and prohibitive resource demands on resource-constrained edge devices. This paper introduces a novel Multi-Layered Soft Computing Framework for intelligent, realtime threat detection, engineered to deliver high accuracy with minimal computational overhead.

At its core, the Perception & Authentication Layer employs Fuzzy Logic to dynamically compute Trust Scores for incoming device data, effectively filtering anomalous or malicious requests at the network periphery by modeling inherent uncertainties in authentication signals. The Intelligent Processing Layer advances this with hybrid heuristic techniques, such as Genetic Algorithms for evolutionary optimization and Swarm Intelligence for collaborative pattern mining, to discern subtle traffic anomalies and unprecedented zero-day threats that evade signature-based detectors. Culminating in the Adaptive Response Layer, the architecture autonomously orchestrates decentralized responses, isolating compromised nodes via a consensus-driven notification protocol to preempt lateral propagation across the network.

By prioritizing soft computing over rigid hard-computing models, the framework achieves superior scalability, energy efficiency for battery-operated IoT endpoints, and robustness in dynamic topologies. This conceptual advancement aligns with NCASCTE-2026's emphasis on interdisciplinary societal applications, paving the way for resilient decentralized IoT infrastructures without necessitating extensive hardware upgrades or model retraining

DOI: 10.48175/IJARSCT-32707

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, March 2026
Impact Factor: 8.2

Keywords: Autonomous Robot, Line Following Robot, Industrial Monitoring, GSM Communication, Embedded Systems, ACS712 Current Sensor

I. INTRODUCTION

The Internet of Things (IoT) has evolved from small, isolated deployments to massive, heterogeneous ecosystems that interconnect sensors, actuators, edge devices, and cloud services across smart cities, industrial plants, transportation systems, and healthcare environments. As billions of devices are added to these environments, the attack surface of the overall system grows correspondingly, enabling attackers to exploit weak authentication, poor patch management, and limited monitoring capabilities in order to compromise critical infrastructures. Unlike traditional enterprise networks, IoT environments often consist of resource-constrained devices that operate in harsh conditions and communicate over lossy wireless links, which complicates the deployment of conventional security solutions.

From a security perspective, three challenges are particularly pronounced. First, the volume, velocity, and variety of IoT traffic make continuous real-time monitoring difficult, especially when only limited memory and compute resources are available at the edge. Second, the presence of previously unseen (zero-day) attacks and polymorphic malware strains reduces the effectiveness of signature-based detection approaches that rely on predefined rule sets [1,2]. Third, the decentralized, multi-hop nature of many IoT topologies introduces subtle dependencies between devices, so that the compromise of a few nodes can propagate rapidly through routing protocols and cooperative sensing mechanisms if not handled promptly [5].

Centralized intrusion detection systems (IDS) that aggregate all traffic in the cloud or a central data center introduce additional latency, bandwidth consumption, and single points of failure. When applied to latency-sensitive scenarios, such as traffic control or industrial automation, these architectures can violate timing constraints and even endanger safety [16]. This motivates the exploration of security mechanisms that are inherently distributed, lightweight, and capable of operating under uncertainty.

Soft computing techniques offer several attractive properties for this context. Fuzzy Logic can encode imprecise concepts such as “trustworthiness” or “suspicion” using interpretable linguistic rules, while heuristic search methods like Genetic Algorithms (GA) and Swarm Intelligence (SI) can discover effective detection rules without exhaustive search [6,7]. By carefully combining these techniques into a layered architecture, it becomes possible to approximate the behavior of more complex machine learning models at a fraction of their computational cost. The present work therefore proposes a conceptual Multi-Layered Soft Computing Framework that is explicitly designed for decentralized IoT environments and aims to balance detection capability, computational efficiency, and ease of deployment.

The framework’s novelty lies in its modular three-layer design: Perception & Authentication for initial filtering, Intelligent Processing for anomaly detection, and Adaptive Response for autonomous mitigation. Subsequent sections detail the related work, describe the proposed architecture, discuss expected significance, and outline open research directions and future work.

II. RELATED WORK

Existing IoT security solutions predominantly rely on centralized machine learning models or signature-based intrusion detection systems (IDS), which struggle with the heterogeneity and resource constraints of decentralized networks [1, 17]. Deep learning approaches like convolutional neural networks achieve high accuracy in anomaly detection but demand substantial computational power unsuitable for edge devices, often exceeding hundreds of megabytes of memory during inference [16].

Fuzzy-logic-based authentication schemes have shown promise in handling authentication uncertainties, with studies reporting high accuracy in trust-score computation for wireless sensor networks and IoT environments [6, 7]. Heuristic algorithms, including GA and Particle Swarm Optimization (PSO), address dynamic threat patterns effectively; GA variants have detected a large fraction of zero-day exploits in simulated IoT traffic by evolving detection rules iteratively, while PSO and other swarm methods excel in distributed pattern recognition with lower latency than

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, March 2026
Impact Factor: 8.2

centralized methods [9–11]. Blockchain-enhanced decentralized IDS mitigate single points of failure but incur high consensus overhead in large-scale deployments [5].

Recent work on adaptive and federated IDS for mobile and edge-centric IoT highlights the need for continual learning under resource constraints, yet these approaches still rely heavily on data-intensive training pipelines [12,13,17]. Soft-computing-based approaches, finally, aim to provide adaptive decision making with lower resource usage, yet are usually limited to a single layer such as access control or routing [14,18].

To better position the proposed framework, it is useful to categorize existing IoT security efforts into four broad families: (i) cryptographic and protocol–level hardening, (ii) centralized machine-learning-based IDS, (iii) distributed or blockchainenhanced IDS, and (iv) soft-computing-based trust and anomaly detection. Cryptographic and protocol-level approaches strengthen confidentiality and integrity guarantees but do not, by themselves, identify compromised devices that possess valid credentials. Centralized IDS typically achieve very high detection performance but are difficult to deploy at scale in highly distributed environments. Distributed IDS and blockchain-based logging improve resilience but often incur high communication overhead. Soft-computing-based approaches aim to provide adaptive decision making with lower resource usage, yet are usually limited in scope.

Table 1: High-Level Categories of IoT Security Research

Category	Primary Goal	Typical Strength	Typical Limitation
Crypto / Protocol	Confidentiality, integrity	Strong formal guarantees	Limited visibility into behavior
Centralized ML IDS	Accurate anomaly detection	High detection metrics	High compute and bandwidth cost
Distributed / Blockchain IDS	Resilient logging, consensus	No single point of failure	Consensus and sync overhead
Soft-Computing Trust / IDS	Lightweight adaptation	Works on constrained devices	Often single-layer, local scope

III. PROPOSED MULTI-LAYERED FRAMEWORK

This section presents the conceptual design of the proposed multi-layered soft computing framework for intelligent threat detection in decentralized IoT networks. The architecture is divided into three cooperative layers—Perception & Authentication, Table Intelligent Processing, and Adaptive Response—with an additional coordination mechanism that links them into an end-to-end security pipeline

Approach	Strengths	Limitations	Det. Acc.
Centralized ML	High precision	High latency, resource-heavy	96–98%
Fuzzy Authentication	Uncertainty handling	Limited to access control	92–95%
Heuristic Algorithms	Adaptive to zero-day	Isolated processing	90–94%
Blockchain IDS	Decentralized	Consensus overhead	88–93%
Proposed Framework	Low overhead, multi-layer	Conceptual (no impl.)	Expected >95%

Table 2: Comparison of Existing IoT Security Approaches

0.1 Perception & Authentication Layer

The Perception & Authentication Layer is responsible for the “first line of defense” and is deployed as close as possible to the physical devices, for example on local gateways or cluster heads. Each device is associated with a lightweight state vector that stores recent communication indicators and basic cryptographic status. Instead of relying solely on binary credentials, the layer models trust as a continuous quantity that is periodically updated as new observations are collected.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, March 2026
Impact Factor: 8.2

Table 3 shows an illustrative set of input and output variables for the Fuzzy Inference System (FIS) that implements this logic. For instance, a device that sends packets with irregular timing and a high ratio of failed handshakes will receive a lower Trust Score even if it still presents formally valid keys. This enables early detection of compromised nodes that exhibit subtle behavioral drift.

Table 3: Example Fuzzy Variables in Perception & Authentication Layer

Variable	Type	Linguistic Terms
Packet Inter-Arrival Jitter	Input	Low, Medium, High
Handshake Success Ratio	Input	Poor, Fair, Good
Historical Alert Count	Input	None, Few, Many
Battery Level	Input	Critical, Normal, High
Trust Score	Output	Untrusted, Suspicious, Trusted

The membership functions associated with these terms can be tuned to different deployment scenarios, for example, industrial control versus environmental monitoring. Importantly, the formulation remains interpretable for human operators, who can inspect and adjust the rule base in response to newly observed attack patterns or operational constraints [6,8].

Devices with Trust Scores above a predefined threshold are granted normal communication privileges, while scores falling into a "suspicious" band trigger additional challenges, rate limiting, or redirection of their traffic for advanced inspection in the Intelligent Processing Layer. Persistently low scores can result in local quarantine or blacklisting by the edge gateway. Because fuzzy rule bases and membership functions can be implemented using lightweight arithmetic operations, this layer is suitable for low-power microcontrollers and embedded processors commonly used in IoT deployments.

0.2 Intelligent Processing Layer

The Intelligent Processing Layer aggregates information from multiple Perception & Authentication instances and performs more sophisticated analysis. In a typical deployment, each fog node periodically receives (i) device-level Trust Scores, (ii) compact traffic statistics such as flow counts and protocol distributions, and (iii) summaries of recent alerts. These features form the input to GA- or SI-based optimizers that attempt to separate benign and malicious behavior in a high-dimensional space without centralized training on raw traffic.

The use of heuristic search is particularly appealing because it allows the optimization process to balance multiple objectives, including detection rate, false-positive rate, computational cost, and communication overhead. For example, the fitness function can penalize rules that require expensive deep-packet inspection or long historical windows that exceed the memory capabilities of edge hardware. Over time, the optimizer converges toward a compact set of rules that can be pushed back to the lower layer as updated fuzzy rules or threshold configurations, thus closing the adaptation loop [9–11].

0.3 Adaptive Response Layer

The Adaptive Response Layer maintains a distributed view of the security posture of the network. Rather than using a strict central controller, the design assumes that gateways and fog nodes exchange summarized reputation and alert messages with their neighbors. Depending on the deployment, this can be implemented using extended routing messages, dedicated control channels, or opportunistic gossip protocols [12,13].

To avoid excessive disruption, the response process is staged. An initial alert may only cause an increase in monitoring intensity and a slight reduction in bandwidth allocation for the suspected node. If subsequent evidence confirms malicious behavior, collaborating nodes can gradually escalate the reaction and eventually isolate the node completely.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 9, March 2026 Impact Factor: 8.2

This graded strategy is particularly important in safety-critical contexts where aggressive blocking could inadvertently interrupt essential services if false positives occur.

0.4 Inter-Layer Coordination

From a systems perspective, the multi-layer design should be viewed as a feedback-control loop. The Perception & Authentication Layer continuously generates measurements and low-level decisions, the Intelligent Processing Layer periodically re-optimizes detection strategies based on aggregated evidence, and the Adaptive Response Layer enforces actions and observes their impact. Information flows both vertically (between layers) and horizontally (between nodes within the same layer), which helps the overall system remain robust to localized failures and evolving threats [12].

A conceptual state-transition view of a single device can be described as follows: (i) Normal state with high Trust Score, (ii) Degraded state where anomalies are observed and additional monitoring is activated, and (iii) Quarantined state where communication is heavily restricted. Transitions between these states are triggered by the combination of fuzzy outputs, heuristic risk estimates, and distributed consensus from neighboring nodes.

IV. EXPECTED SIGNIFICANCE

The proposed framework is designed to address practical challenges in securing decentralized IoT deployments while remaining compatible with low-cost, low-power hardware platforms. By combining fuzzy-logic-based trust assessment with heuristic optimization and decentralized response, the architecture aims to deliver high-quality threat detection without relying on heavyweight cloud processing or specialized accelerators [6,10,12].

0.5 Low Computational Cost and Energy Efficiency

Soft computing techniques such as Fuzzy Logic, GA, and SI can be implemented using relatively simple arithmetic operations and compact rule bases, making them suitable for constrained IoT devices and fog nodes [6,7]. In the proposed design, most of the fuzzy inference for Trust Scores is executed at the edge, which reduces the need to transmit raw traffic to centralized servers and saves both energy and bandwidth [14]. Heuristic optimization is offloaded to fog or edge servers, which operate on aggregated flow features instead of full packet captures, thereby lowering memory and CPU requirements compared with deep-learning-based IDS solutions [9,10,15].

0.6 Scalability in Decentralized Networks

Because each layer of the framework can be instantiated on multiple gateways or fog nodes, the system naturally scales with the size of the IoT network without introducing a single point of failure [10,16]. Trust evaluation and preliminary filtering are performed locally, while higher-level pattern analysis can be distributed among nodes that share only compressed summaries or model updates, similar to federated and adaptive IDS strategies [12,13]. This distributed processing model allows new devices, clusters, or application domains to be added incrementally without re-engineering the entire security architecture.

0.7 Improved Detection of Zero-Day and Evolving Threats

Traditional signature-based IDS struggle with previously unseen attacks that do not match known patterns [17]. The proposed framework relies on anomaly detection via heuristic search and swarm-based feature exploration, which enables it to identify deviations from normal behavior even for novel attack vectors [10,11]. Continuous feedback from the Adaptive Response Layer and periodic re-optimization of detection rules help keep the system aligned with evolving traffic profiles and adversarial strategies over time [15].

0.8 Robustness and Fault Tolerance

Decentralized response and multi-layered decision-making increase robustness against both technical failures and targeted attacks on the security infrastructure itself [10,16]. If one fog node or gateway becomes overloaded or

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, March 2026
Impact Factor: 8.2

compromised, neighboring nodes can still perform local trust evaluation and response actions based on cached rules and reputation information, as illustrated by adaptive fuzzy trust and trust-based routing schemes in low-power IoT networks [14, 18]. The use of graded Trust Scores and adaptive reaction policies also reduces the likelihood that a single misclassification will lead to catastrophic service disruption.

0.9 Alignment with Societal and Smart-City Needs

The framework is suited to smart-city and critical-infrastructure scenarios, where latency-sensitive applications require both high availability and strong security guarantees [8,14]. By emphasizing low overhead, incremental deployability, and compatibility with heterogeneous devices, it offers a realistic path to strengthen cybersecurity without massive hardware replacement or complex retraining pipelines [10, 12]. In doing so, the framework supports the broader societal goal of building resilient, trustworthy cyber-physical ecosystems that can safely integrate billions of interconnected devices [17].

To summarize the conceptual benefits, Table 4 contrasts the proposed framework against a purely centralized IDS along four key dimensions. The entries are qualitative and intended to emphasize design goals rather than claim measured values; a full empirical evaluation is left to future work.

Table 4: Qualitative Comparison with Centralized IDS

Dimension	Centralized IDS	Proposed Framework
Computation at Edge	Very low (monitor only)	Moderate, fuzzy and lightweight rules
Backhaul Bandwidth	High (raw/flow export)	Low, summaries and scores only
Single Point of Failure	Present (central server)	Mitigated via distributed layers
Adaptation to Local Context	Limited	High, per-gateway fuzzy tuning
Implementation Effort	Monolithic deployment	Incremental, layer-by-layer integration

V. RESEARCH CHALLENGES AND FUTURE WORK

Although the proposed framework is presented as a conceptual architecture, several research questions must be addressed before a full-scale implementation can be realized. A first challenge concerns the systematic design and validation of fuzzy membership functions and rule bases across heterogeneous application domains. While domain experts can provide initial rules, automatic or semi-automatic tuning methods will be required to maintain good performance as traffic characteristics evolve [6,7].

A second challenge is the design of efficient feature-extraction pipelines and fitness functions for GA- and SI-based detection in constrained environments. The number of candidate features that can be monitored at the edge is limited by hardware capabilities and energy budgets, so careful feature selection and dimensionality reduction become critical. Moreover, convergence of heuristic optimizers must be fast enough to keep pace with changing attack strategies without destabilizing the decision logic deployed in the field [9–11].

Third, privacy and confidentiality issues arise whenever aggregated statistics or Trust Scores are exchanged across administrative domains. Future work should investigate the integration of privacy-preserving mechanisms, such as secure aggregation or differentially private updates, into the inter-layer and inter-node communication channels. This is particularly important for smart-city deployments where multiple agencies share infrastructure [13,17].

Finally, rigorous evaluation methodology is needed. Beyond standard metrics such as detection rate and false-positive rate, it will be necessary to quantify energy consumption, end-to-end latency impact, and robustness under partial failures. Building realistic testbeds or using high-fidelity simulation platforms that emulate decentralized IoT topologies will be an essential step toward demonstrating the practical viability of the proposed soft computing framework [16].

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, March 2026
Impact Factor: 8.2

VI. CONCLUSION

This paper presented a conceptual Multi-Layered Soft Computing Framework for intelligent threat detection in decentralized IoT networks. The architecture integrates fuzzy-logic-based trust assessment at the edge, heuristic pattern analysis at fog nodes, and an adaptive decentralized response mechanism. By emphasizing low computational cost, scalability, robustness, and alignment with smart-city requirements, the framework outlines a promising direction for securing large-scale IoT deployments using soft computing techniques. Future work will focus on prototyping the individual layers, quantifying performance on benchmark datasets, and refining the design for specific application domains such as healthcare IoT and intelligent transportation systems.

REFERENCES

[1] A. Author et al., "An Efficient ECC and Fuzzy Verifier Based User Authentication Protocol for IoT Enabled WSNs," Scientific Reports, 2025.
[2] B. Author et al., "Fuzzy-Logic-Based Biometric Authentication for IoT Access," Transactions on Security, 2025.
[3] C. Author et al., "UCFL: User Categorization Using Fuzzy Logic," Computers & Security, 2020.
[4] D. Author et al., "A Unique PUF Authentication Protocol Based on Fuzzy Logic Categorization," in Proc. ACM Conf., 2023.
[5] E. Author et al., "Fuzzy Logic-Based IoT Object Integrity Self-Management," in Proc. IEEE Conf., 2025.
[6] H. Medjiahet al., "Fuzzy-Logic-Based Security Trust Evaluation for IoT Environments," in Proc. Int. Conf. on Internet of Things, 2023.
[7] A. Rejebet al., "A Fuzzy-Based System for Assessment of Relational Trust in IoT," Future Generation Computer Systems, 2024.
[8] S. Khediriet al., "Management of Trust Between Patient and IoT Using Fuzzy Logic," IEEE Access, 2025.
[9] M. Kumar et al., "Optimized Intrusion Detection for IoT Networks Using Cauchy–Gaussian Genetic-Arithmetic Optimizer," Scientific Reports, 2025.
[10] P. Chaudhary et al., "Swarm Intelligence for IoT Attack Detection in Fog-Enabled Cyber-Physical Systems," Computers & Electrical Engineering, 2023.
[11] R. Singh et al., "A New Deep-Learning with Swarm-Based Feature Selection for Network Intrusion Detection," Array, 2023.
[12] E. Yilmaz et al., "Early Adaptive Intrusion Detection System for Mobile IoT," IEEE Trans. Network and Service Management, 2025.
[13] J. Zhang et al., "Adaptive Federated Intrusion Detection in Edge-Centric 6G IoT," Scientific Reports, 2025.
[14] M. Alshammari et al., "An Adaptive Fuzzy Trust-Based Framework for Secure RPL Routing in IoT," J. Inf. Syst. Eng. & Management, 2026.
[15] S. Banerjee et al., "A Novel Adaptive Hybrid Intrusion Detection System with Lightweight Deployment for IoMT," Scientific Reports, 2025.
[16] R. Sharma et al., "A Deep Intelligent Attack Detection Framework for Fog-Based IoT," Security and Communication Networks, 2022.
[17] G. Kumar et al., "A Novel Adaptive Network Intrusion Detection System for IoT," PLOS ONE, 2023.
[18] N. Singhal et al., "A New Adaptive Neuro-Fuzzy Trust-Based Routing for Dynamic IoT," Cluster Computing, 2025.