International Journal of Computational Methods and Experimental Measurements
https://www.acadlore.com/journals/IJCMEM

Hybrid Framework for Privacy and Integrity in the IoT Environment Using the Network Topology Measures and Deep Learning Techniques

H. C. Pavithra[1*], J. Rajeshwari [2], K. S. Rekha [3], M. Narender [4], Bhat Geetalaxmi Jairam[5], R. Sunitha [1]

[1] Department of Artificial Intelligence and Machine Learning, B N M Institute of Technology, 560070 Bangalore, India
[2] Department of Information Science and Engineering, Dayananda Sagar College of Engineering, 560078 Bangalore, India
[3] Department of Computer Science & Engineering, JSS Science & Technology University, 570006 Mysuru, India
[4] Department of Computer Science and Engineering, The National Institute of Engineering, 570008 Mysuru, India
[5] Department of Information Science and Engineering, The National Institute of Engineering, 570008 Mysuru, India

* Correspondence: H. C. Pavithra (pavitrahc06@gmail.com)

Received: 11-18-2025 **Revised:** 12-17-2025 **Accepted:** 12-26-2025

Citation: H. C. Pavithra, J. Rajeshwari, K. S. Rekha, M. Narender, B. G. Jairam, and R. Sunitha, "Hybrid framework for privacy and integrity in the IoT environment using the network topology measures and deep learning techniques," *Int. J. Comput. Methods Exp. Meas.*, vol. 13, no. 4, pp. 868–881, 2025. https://doi.org/10.56578/ijcmem130409.

Abstract: The Internet of Things (IoT) consists of a large interconnected system of devices that automatically gather, analyze, and transfer data. Securing the integrity and privacy of these devices is a significant challenge due to their distributed and heterogeneous nature. To address this issue, this paper presents a hybrid security framework that is designed in two phases: Node Topology Measures-based Vulnerable Node Detection (NTMVND) and Adoption-based Differential Evolution (ADE) with Elicited Genetic Algorithm (ADE2GA). The NTMVND component detects vulnerable nodes using important topological measures such as node degree, betweenness, clustering coefficient, and centrality to remove potential risks in the communication network. The ADE2GA component produces optimal and secure paths for data transmission by leveraging the adaptive exploration characteristics of Differential Evolution (DE) and the exploitative learning capabilities of the Genetic Algorithm (GA). The simulation results in Network Simulator-2 shows that the ADE2GA model performs best, resulting in 39% reduction in the end-to-end delay and 26% savings in energy consumption, while producing a 41% increase in throughput and a 10% increase in packet delivery ratio compared to standard Particle Swarm Optimization (PSO) and Differential Evolution with Genetic Algorithm (DEGA) models. The results substantiate the proposed framework's capability for promoting improved integrity, privacy, and efficiency in IoT settings.

Keywords: Differential evolution; Elicited genetic algorithm; Integrity; Internet of Things; Privacy

1 Introduction

The Internet of Things (IoT) is a smart age that is expanding quicklyto a variety of applications that enable the implementation of several routing protocols using machine learning techniques. The integration of new technologies such as 5G, edge computing, and machine learning is creating new prospects to address IoT security. In particular, Feng et al. [1] proposed that through service function chaining with machine learning, security functions at 5G edges can be enhanced by enabling dynamic adaptation to contemporaneous threats. Gatjens and colleagues further advanced these ideas proposing that transient IoT data can be managed through intelligent caching and consistency, which may enhance data reliability and system response times [2]. The implications of this extension are that AI-driven methods can be combined with network-based optimization approaches to offer additional resilience against cyberattacks in IoT than would be achieved by either method alone.

The IoT has established itself as a new paradigm that connects billions of distinct devices that are capable of autonomously collecting, processing, and disseminating information in a distributed fashion [3], and at a rapid rate, into critical sectors (healthcare, transportation, industrial automation) has become a fundamental element of contemporary cyber-physical systems. However, this development has also severely exposed the IoT infrastructure to multiple forms of security and privacy vulnerabilities that compromise data confidentiality, integrity, and availability [4].

Despite this, IoT ecosystems are still vulnerable to numerous forms of intrusion such as wormhole, denial-of-service (DoS), and ransomware attacks, which exploit the resource constraints associated with the diversity of devices that are connected. Alotaibi [5] introduced a meta-heuristic clustering approach based on Tabu Search and adaptive memory, which exhibited improvements with respect to convergence speed and accuracy. In relation to IoT security frameworks, optimization driven improvements can also be accomplished and provide real-time and longitudinal adaptability and resilience. Deshmukh-Bhosale and Sonavane [6] suggested a real-time network intrusion detection system for IoT networks based on the routing protocol for low power and lossy network (RPL) standard, and Zarpelão et al. [7] provide a survey of intrusion detection approaches in IoT ecosystems. Zahra and Shah [8] discussed the issue of ransomware spreading in IoT networks and stressed the need for proactive detection of these attacks. Furthermore, while threats have emerged at the network level, risks associated with the physical tampering of devices, and side-channel attacks still remain a risk at the device level [9, 10].

Research has increasingly aimed to enhance the trust and authenticity of IoT communications through privacy-preserving security models and, in particular, blockchain-based attestation mechanisms. Xu et al. [11] surveyed a privacy-preserving blockchain model for remote attestation in vehicular networks. Larsen et al. [12] developed efficient and privacy-preserving revocation mechanisms for cooperative intelligent transport systems in their study. Finally, Xiong et al. [13] studied a scalable and forward-secure method of network attestation with an emphasis on cloud-assisted IoT. These efforts reflect growing interest in hybrid or adaptable security architectures involving cryptographic, machine learning, and distributed trust elements.

Although there have been advancements in the field, the diverse and resource-constrained nature of IoT networks still complicates the development of secure models that can effectively scale. All of these gaps will need to be filled by potential solutions that can meet the competing constraints of energy efficiency, processing complexity and adaptive security services. Recently, several authors have investigated metaheuristics optimizations and deep learning techniques to improve analysis related to the optimization of network parameters and detection accuracy [14, 15].

This research work goal is to investigate how vulnerable certain network components are to interruption while taking autocorrelation and network architecture into consideration from the perspective of node integrity and privacy. To ensure the integrity and privacy of the IoT environment, this paper provides a hybrid model that considers several node topology methods together with deep learning approaches. This work is divided into two sections: Node Topology Measures-based Vulnerable Node Detection (NTMVND) and Adoption-based Differential Evolution (ADE) with Elicited Genetic Algorithm (ADE2GA). The responsibility of the NTMVND is to identify the susceptible nodes in the network by using several node topology metrics, including node betweenness, degree of the node, clustering, Centrality score, Proximity score, and overhearing. ADE2GA helps preserve the privacy of the sensor by identifying the optimal paths along with alternative paths. Experimental results indicate that the proposed technique works better than the state-of-the-art evolutionary algorithm. In contrast to asserting a basic transformation in the logic of developed systems, this research develops incremental progress by combining both topology-oriented vulnerability scanning and evolution-based routing with the assistance of adoption-oriented developments to create measurable improvements in both performance and security while supporting the application of IoT within real world scenarios

The structure of the paper is laid out as follows: Section II summarizes previous studies by various authors. In Section III, the proposed framework is described including the system model, formulation of the mathematical model, and multi-objective exploration of the research questions, without detailing each individual study. In Section IV, we present the set-up for a computational experiment with the simulation scenarios and performance measures. Section IV establishes the significant findings and contributions being developed through the work with implications for future research.

2 Literature Survey

In recent years, different works on the Internet of Things Security (IoTS) have focused on AI, deep learning, and optimization-based approaches to enhance detection, resilience, and efficiency of routing IoT devices. The current section is divided into three fields of related topics (i) identification of nodes most vulnerable to the physical architecture of a IoT network is a vulnerable structure; (ii) the application of Hybrid or Evolutionary algorithmic techniques to develop solutions for creating Secure managed routing in IoT including hybrid methods based on evolutionary algorithm based methods; (iii) a privacy oriented managed routing based on the principle of protecting surveillance over sensitive data from both node compromise and the ability of malicious actors to analyse traffic patterns.

Kalakoti et al. [16] investigated the use of Explainable AI for IoT botnet detection and also quantitatively measured the interpretability of AI models in order to enhance trust and transparency in automated Intrusion Detection Systems (IDS). Likewise, Altulaihan et al. [17] outlined a machine learning-based anomaly detection IDS to mitigate DoS attacks in IoT networks that yielded improved precision and recall numbers across various types of attacks.

Separately, Mohy-Eddine et al. [18] proposed a network IDS applied to the K-Nearest Neighbors (K-NN)

classifier with a feature selection process that improved model accuracy while lowering false alarm rates for IoTS. In a comprehensive survey of machine learning security in IoT networks, Tahsien et al. [19] illustrated the merit of both supervised and unsupervised approaches in combating continually evolving cyber threats. Sivasakthi et al. [20] advanced the field of resilience to hybrid and upcoming attacks, by proposing HybridRobustNet, a sophisticated deep learning model designed to detect hybrid attacks in IoT networks. Alangari [21], in comparison, employed unsupervised learning for anomaly and attack detection in IoT sensor data, providing more robust adaptability in his analysis, giving IoT security more independence from labeled datasets. Blockchain technology emerged as another pivotal enabler for building decentralised security solutions in IoT. Indrason and Saha [22] introduced a blockchain solution for securing IoT architectures based on Software-Defined Networking, while Truong and Le [23] extended this idea to the Metaverse, combining blockchain and machine learning for intrusion detection and data trust.

Concurrently, some scholars have conducted studies investigating IoT vulnerability analysis and intrusion prevention in the context of developing measures at the protocol-level and architecture-level of security studies. Braghin et al. [24] modelled a vulnerability assessment of an IoT protocol based on a Z-Wave case study, which identified vulnerabilities at the system level. Hazman et al. [25] proposed the Lightweight Intrusion Detection System for Smart IoT Environments using Ensemble Learning framework, which utilizes ensemble learning, for IoT-enabled smart environments to enhance detection rates across multiple attack scenarios. Beyond network security, IoT security principles are integrated in intelligent perception and control applications. Khan et al. [26] published a model for multi-sensory localization and human activity recognition that enhanced robustness in complex IoT-enabled physiological monitoring settings. Chen et al. [27] present a disparity-based multiscale fusion network to intelligently detect transportation, utilizing IoT data streams to assist mobility safety applications. Zhang et al. [28] employed enhanced deep reinforcement learning for task planning in multi-USV configurations, displaying the feasibility of coordinating autonomous IoT networks under secure communication constraints.

In terms of privacy and data protection, Dhavamani et al. [29] developed a differential privacy-preserving IoT data-sharing framework based on an enhanced Particle Swarm Optimization (PSO) algorithm and realized an effective balance between privacy guarantees and data utility in distributed settings. To build upon the optimization-based approach, Kumar [30] designed a secure hybrid routing algorithm based on a Genetic Algorithm (GA) that could maximize the network lifetime while preserving data integrity in IoT communication frameworks. Solangi et al. [31] conducted a comprehensive review of GA-based methods used in wireless sensor networks (WSNs) that highlight their adaptability toward topology optimization and energy-efficient routing.

The topics of routing based on energy efficiency and reliability has also been a focus. Varnshney et al. [32] developed a routing protocol optimized for IoT agricultural systems to enhance reliability and reduce packets loss. Park et al. [33] proposed probabilistic energy efficient snooting algorithm for IoT networks to reduce transmission costs based on topology. Norouzi and Zaim [34] employed GA optimization to WSNs to achieve performance balance under system lifetime and throughput, while Hampiholi and Vijaya Kumar [35] proposed modifying routing based on classical GA in order to achieve more scalability and fault tolerance. Dhumane et al. [36] developed an optimal routing algorithms developed for IoT enabling technologies that increased packet delivery and minimized latency of dynamic topologies. Lastly, Lal and Sharma [37] developed GAEER protocol, an energy efficient GA based routing protocol developed to improve energy efficiency and transport of data.

In conclusion, many studies show a convergence of management learning, blockchain, and evolutionary optimization for securing in IoT systems. Existing research does require hybrid implementations that can provide a simultaneous vulnerability detection, privacy preservation and secure Routing Optimization. This study proposes a hybrid ADE2GA model to compete in this space by using detect vulnerabilities and preventive measures, using deep learning, and topology aware GA with evolutionary optimization to achieve IoT security performance.

3 Proposed Method

A two-step process of a pipeline is suggested. The primary step utilizes the NTMVND method to identify any potentially vulnerable Node Vulnerability through Topology Measures; this occurs before a Routing Optimization is made since if the Routing Optimization is made prior to identifying any vulnerable nodes through Topology Measures, it will not be a guarantee of the truthful secure Routing process. In general, nodes with a high degree of Betweenness Centrality and Clustering Coefficient will be more vulnerable to attacks by an intruder, such as Man-in-the-middle/packet dropping route manipulation. Therefore, if you have nodes in your routing path that fall into either of these categories, then even if you take the most efficient route, it may connect vulnerable nodes that compromise either data confidentiality, data privacy, or both.

Hence, NTMVND is utilized to analyze the network topology (Degree, Closeness, Betweenness, Clustering Coefficient, and Neighborhood Connectivity) to assign a Vulnerability Score to each Node. If the Vulnerability Score for any Node is above a pre-defined threshold, that Node is isolated from Routing Graphs used in that step of the pipeline. The cleaned-up or reduced Routing Topology is then passed to the ADE2GA for Routing Optimization on only the network of non-vulnerable, trusted Nodes. Using this Sequential Dependency ensures that only non-

vulnerable Networks are used within the Routing Optimization process and creates a more secure Routing path with enhanced Data Preservation and Integrity.

This sections discuss the proposed solution for the IoT security concerns. The proposed model is designed to ensure the integrity and Privacy of the IOT environment. This is achieved with the help of Machine learning and encryption mechanisms. The proposed framework is divided into two functions: NTMVND and ADE2GA.

3.1 Node Topology Measures-Based Vulnerable Node Detection

Consequently, this paper's goal is to examine the susceptibility of individual network pieces to interruption from the standpoint of node integrity, while accounting for network architecture and autocorrelation. Network vulnerability is a pertinent concern in the development and execution of networked processes, particularly transportation, as evidenced by recent research. The primary focus of this research is to identify network elements that are particularly vulnerable to interruptions to their integrity. Although certain literature-based theories have suggested that the network's configuration may affect an element's susceptibility, a thorough analysis of the relationship between network structure and security has not been carried out.

3.1.1 Degree of the node

A node's degree indicates how connected it is to other nodes in the network. The following formula may be used to explain it: In the node relationship matrix M, m_{pq} represents the ik element, while $D_N(Ap)$ is the level of node Ap. These elements have a value of 1 if and only if there is a connection connecting nodes Ap and Aq, where N is the total number of nodes in the network. As a measure of a node's possible communication activity, its degree is seen to be significant as shown in Eq. (1).

$$D_N = \frac{\sum_{q=1}^{N} m_{pq}}{N-1} \tag{1}$$

3.1.2 Node closeness

It serves as an index that analyzes a network node's accessibility. where the geodesic path length among Ap and Aq is denoted by m_{pq}. By this metric, the shortest central node has the smallest sum of distances to all other nodes as shown in Eq. (2).

$$C_N = \frac{1}{\sum_{q=1}^{N} m_{pq}} \tag{2}$$

3.1.3 Node betweenness

Node betweenness is a measurement of the frequency with which a node is found on the shortest route among all node pairs in a network. It is thenode frequency of finding itself inside a given network space distance from other pairs of nodes Ap and Aq. You may think of Ap as a measure of network flow management since it depends on how many paths it uses to function as a connection between Ap and Aq.
where, N is the total number of nodes in the network, $B_N(Ap)$ is the betweenness of node Ap, $g_{pq}(Ar)$ is the number of shortest paths passing through node Ar between nodes Ap and Aq, and g_{pq} is the total number of possible paths between Ap and Aq as shown in Eq. (3).

$$B_N = \frac{\sum_{g_{pq}} \frac{Ap}{PP_{pq}}}{(N-1)(N-2)} \tag{3}$$

3.1.4 Node clustering

It measures a node's local transitivity, or the likelihood that a node's neighboring nodes are linked. The percentage of true edges between a node's neighbors out of all potential edges is known as clustering for node Ap. Where the entries of proximity matrix M are specified before m_{pq}. It is common to define clustering as the possibility that node's immediate neighbor hop will also be node's neighbor as shown in Eq. (4).

$$C_{clu} = \frac{\sum_{pq} arq\ apq\ arp}{D_N(Ap) - 1} \tag{4}$$

3.1.5 Neighborhood connectivity

Neighborhood connectivity is a metric that represents the typical connection of a node's neighbor nodes. It makes no difference how strongly linked node Ap is in and of itself because the metric is an average of the surrounding nodes. The meaning of this metric is that the total number of node surrounding the central node. $N(p)$ represents the number of node p's neighbors in this case as shown in Eq. (5). The node adjacency matrix M's pqelement, or M

raised to the q^{th} power, is represented by the value of m_{pq} in the Node Centrality measurement is shown in Eq. (6). When the neighbors of a node have high degrees, the node is central. Higher magnitudes suggest a slower decay, whereas the exponent q's amplitude suggests an ability of the impact to decrease across long distances. Where, β = 0.5, first order neighbors receive a weight of 0.5, second order neighbors receive a weight of 0.52.

$$C_{NC} = \frac{1}{\|N(p)\|} \sum_{j \in N(i)} D_N \left(A_q\right) \tag{5}$$

$$C_{Ce} = \frac{1}{\beta} \sum_{q-1}^{n} \sum_{p=1}^{N} \beta^q \left(m^q\right)_{pr} \tag{6}$$

Nodes with more neighbors receive better ratings based on node degree. Node proximity assigns greater values to nodes that are more centrally situated, meaning that their pathways to other nodes are shorter. Nodes that regularly serve as links between other nodes receive higher ratings for node betweenness. Highly transitive nodes that is, nodes that have a large number of friends in common with their neighbors tend to be rewarded by node clustering. When employing this metric, nodes with a large number of neighbors who are not necessarily related to one another typically receive lower scores.

Thus, by calculating a weighted vulnerability score for each node in the network based on the multiple topology measures' interconnectedness, we can form an overall unified vulnerability estimation; for each node, its vulnerability score $V(v)$ with D_v, C_v, B_v, Cl_v, and NC_v representing the degree, closeness, betweenness, clustering, and neighbourhood connectivity respectively.

$$V(v) = D_v * \text{weight}_1 + C_v * \text{weight}_2 + B_v * \text{weight}_3 + Cl_v * \text{weight}_4 + NC_v * \text{weight}_5 \tag{7}$$

$$\text{weight}_1 + \text{weight}_2 + \text{weight}_3 + \text{weight}_4 + \text{weight}_5 = 1 \tag{8}$$

In the current study, the weights assigned to degree and betweenness were weight_1 = 0.25 and weight_3 = 0.25 to reflect the importance of intercepting network traffic and manipulating routes. Nodes with vulnerability scores greater than τ will be identified as vulnerable and eliminated from the routing graph before optimizing routes.

3.2 Adoption-Based Differential Evolution with Elicited Genetic Algorithm

The detailed design and implementation of the second proposed functional module, ADE2GA, are covered in this component. The model is a hybrid optimization scheme that incorporates two evolutionary learning strategies ADE and Elicited Genetic Algorithm (EGA). Differential Evolution (DE) is a population comparison optimization methodology for solving global optimization problems, that is used in an iterative approach that generates new candidate solutions through applied evolutionary operations that include mutation, crossover, and selection. DE is an example of a heuristic method to minimize complicated, nonlinear, and non-differentiable continuous functions. In this regard, a heuristic method indicates a problem-solving technique that uses reasonable and experience-based techniques for reaching near-optimal solutions in a reasonable timeframe, particularly when a standard method is prohibitively costly or is otherwise likely to be stuck without a definitive solution.

The GA is a heuristic search method grounded on the idea of evolution. It emphasizes the survival of the fittest and draws inspiration from selection, crossover, mutation, and recombination operators. The cost function determines the solution's quality, whereas candidate solutions to optimization problems represent the people in a population. Following the repeated application of the GA operators, the population is next subjected to natural selection. In the actual world, GAs work best at approximating solutions to a variety of technical challenges. The following section explains the ADE framework to identify the optimal solutions excluding the malicious node. This algorithm incorporates the DE to ensure the integrity and privacy of the IoT environment. The IoT environment in which multiple nodes $N = \{n1, n2, \ldots np\}$ will be deployed over the wide range network area $M \times N$. The network area is divided into $N \times N$ matrices with an unequal number of nodes in each cluster. The following sections give the detailed steps with a mathematical model.

At the outset, the DE technique is used to find every possible shortest path from the source to the destination nodes. Once a set of candidate paths has been determined, some sequential evolutionary methods come into play to perfect those paths. The process begins with a mutation operator that will provide a mutant vector as an alternative solution that is generated by perturbing existing solutions for more effective search area exploration. Once mutation occurs, the crossover operator is completed using the mutant vector combined with the original vector, introducing more diversity and identification of an optimal solution in the search area. The DE process continues to iterate, if needed until an optimal value is found. The next evolutionary step occurs when the selection operator chooses the best solution from the mutant vector and orphan vector based on the fitness function in the principle of "survival of the fittest" for the next iteration and only keeps the vectors that are most optimal, when possible. If an optimal solution is not found, the original vector still remains. The brief optimization process of this methodology.

3.2.1 Malicious node/path selection

This section describes the exact design of the suggested optimization method. The ADE is a global optimizer using the population-based strategy that deals with both constrained and unconstrained situations. In order to improve resistance of real-world data to hostile attack, we proposed a new ADE operator which automates parameter adaptation to preferentially select the most fit candidate vectors from across the search space for optimization purposes. The operator was designed to automate parameter adjustments for groups of candidate vectors while optimizing convergence to the best solutions and while maintaining diversity at the population-level, by dynamically changing mutation and crossover behavior based on the current, local search space. It allows for environment-adaptive learning by providing considerable diversity for global exploration, followed by a focus on the most fit regions for local refinement. The method requires an agile, adjustment-driven selection mechanism, with the details of the selection mechanisms described in the forthcoming subsections.

Consider the network with the sensors as $Y = (y1,\ y2, y3, \ldots\ldots yn)$, $Y \in M^n$, objective function $f(Y)$, with constraint functions $gi(Y) \leq 1$, i = 1,2,3...p and the boundary constraints $yjk \leq yj \leq yjn$, j=1,2,3,$\ldots n$. DE is working on the population generation of candidate solutions on the individual nodes of the population as shown in Eqs. (9) and (10).

$$P_C = (Y_{1,C}, \ldots\ldots\ldots, Y_{MI,C}), C = 1, \ldots\ldots .C_{MAX} \tag{9}$$

$$Y_{j,C} = (Y_{1,C}, \ldots\ldots\ldots, Y_{j,C}\} \, j = 1, 2, \ldots\ldots MP, C = 1, , , , C_{MAX} \tag{10}$$

Here, j is used to index the population, I the real parameters, and G is the population generation. ADE initializes a population of candidates and continually creates new candidates from the current population by combining candidates that are crossed over, and then selects the one that is best according to a condition. Hence, the flow of the ADE algorithm is given below.

This stage is concerned with creating the first population for the optimization procedure. As was described in the proposed model, the first step is to create a group of random population members based on the details of the problem or application. We initialize each member of the population based on the problem's tuning parameters; however, we ensure the values generated fall within predetermined lower and upper bounds. The random initialization allows the algorithm to adequately explore the entire parameter space from the outset, enhancing diversity and preventing premature convergence. Thus, the initial population vectors are uniformly distributed within the search space. For example, we can mathematically express the population vectors as seen in Eq. (11).

$$Y_{j,k,1} = rnd_i[0,1]Y_k^{upper} - rnd_i[0,1]Y_k^{Low} + Y_k^{Low} \tag{11}$$

Here, $rnd_i\,[0,1]$ represents a random value distribution with the range 0 to 1 uniformly, Y_k^{Low} denotes variable lower bounds and Y_k^{upper} denotes the variable upper bounds, and $j = 1, 2, \ldots MP, k = 1 \ldots C$. In this section, we will be presenting the modified design approach of the original mutation operator in DE algorithm. This operator alters the best vector of the original ADE algorithm. For every target vector select three potential vectors randomly. Eq. (12) is used to obtain the mutant vector.

$$T_{j,k,G+1} = Y_{j,v5,C} + \{G\,(Y_{j,v3,C}) - G\,(Y_{j,v4,C})\} + \{G\,(Y_{j,v3,C}) - G\,(Y_{j,v1,C})\} \tag{12}$$

where, Yj is the variable, G is the function and $k = 1 \ldots Mf, j = 1, \ldots N, v1, v2, v3, v4, v5 \in (1, \ldots Mf)$, and $v1 \neq v2 \neq v3 \neq v4 \neq v5 \neq k$. This operator combine ADE technique based on the available search region. Eq. (13) illustrates the active adaption-based fitness function used to choose the best vector, along with the corresponding process.

$$Act = rand\left(D_{j,k}^{upper} - D_{j,k}^{Low}\right) \tag{13}$$

Here, Act refers to the current environment that is feasible based on the solution and the selection random best vector lower bound and upper bound. The pseudo-code of the proposed algorithm is given in Algorithm 1. An integral part of this study is to integrate this algorithm in the IoT environment in order to provide security analysers that take into account the stated objective functions.

Shortly after finalizing the mutation phase, the crossover operator is then carried out with the aim determining whether the mutant vector performs better in terms of adaptation value than the original vector, and to locate the best solution in the search space. If the best value has been found, it is possible to terminate the algorithm early, as the solution has been determined. Crossover improves diversity in the population by taking attributes from both the mutant vector and the parent vector, while also searching for solutions more broadly. Diversity can contribute to

solving premature convergence, as it allows the optimization process to robustly improve its search. The new trial vector computed by the crossover is defined in Eq. (14).

$$V_{q,p,c} = \begin{cases} P_{q,p,c} & if\ rand[0,1] \leq Cr \vee p = q \\ Y_{q,p,c} & else \end{cases} \tag{14}$$

Her, Cr is a real valued crossover factor that takes a value between 0 and 1. It governs the likelihood that a trial vector will be selected from the mutant vector as opposed to the current vector. Once the crossover step is finalized, the process moves onto the selection step, which essentially determines the best vector for the next generation. During this stage, the mutant and offspring vectors are considered based on their fitness function values. The survival of the fittest is assumed for this operation, and the selected solution is determined by considering which vector will carry forward to the subsequent iteration. If the trial vector exhibits a better (i.e. lower) cost function value than the existing vector, the trial vector will carry forward to the following iteration. If the trial vector does not outperform the current solution, the previous vector will remain unchanged. The greedy method of selection allows a consistent improvement of solutions across generations and does is a computationally efficient method of controlling the population. Since the DE isn't a gradient-based method, it achieves convergence to the global minima faster than many other evolutionary optimizations methods. The mathematical representation of the selection step is provided in Eq. (15).

$$Y_{p,C+1} = \begin{cases} V_{p,C+1} & if\ g\left(V_{p,C+1}\right) \leq g\left(Y_{p,C}\right) \\ Y_{p,C} & else \end{cases} \tag{15}$$

In boundary constrained problems, after reproduction, parameter values need to be inside the allowed ranges. To achieve this, the value of the parameters that breaches the boundary constraints is substituted by a random number generated within the feasible range as illustrated in Eq. (16).

$$Y_{j,k,c+1} = \begin{cases} rnd_i[0,1]Y_k^{upper} - rnd_i[0,1]Y_k^{Low} + Y_k^{Low} \\ if Y_{j,k,C+1} < Y_k^{Low} \text{ and } Y_{j,k,C+1} > Y_k^{Low} \\ Y_{j,k,C+1} \qquad else \end{cases} \tag{16}$$

where, $j = 1, 2, \ldots MP, k = 1 \ldots\ C$, an appropriate optimization algorithm must be applied to formulate a minimum of the discrete nonlinear function in Eq. (17), which should produce a favorable label placement.

$$g(y) = \sum_{i=0}^{m} \sum_{j=1}^{m} O(yi - yj) + \sum_{0}^{m} D(yi - di) \tag{17}$$

where, $O\left(yi - yj\right)$ and $D(yi - yj)$ are used to measure the overlapped probability labels and the distance measures. A well-known and strong method for generating an optimum solution is a global optimization method, for example, EGA.

ADE2GA uses an elite-guided inheritance method to define the adoption mechanism, which selects some of the gene segments of the candidate solution from historical elite candidates' gene segments. The i^{th} candidate solution in Generation g is denoted as X_i^g, and the elite candidate solution from the previous generation is denoted as X_{best}^{g-1}. The mutation phase of ADE2GA generates trial vectors U_i^g as follows: $U_i^g = X_i^g + F\left(X_{r1}^g - X_{r2}^g\right) + \alpha \cdot \mathrm{II}(p < P_{adopt}) \cdot (X_{best}^{g-1} - X_i^g)$, where F is a scaling factor used by the DE method, the random pairing of individuals X_{r1}^g and X_{r2}^g is performed, α is a parameter indicating the strength of inheritance, P_{adopt} is the probability that a candidate solution will adopt a segment from an elite candidate solution, I is the indicator function, and $p \sim U(0,1)$. This term provides a mechanism for the current generation's candidates to adopt gene segments from the best previous candidates, thereby allowing them to converge more quickly to a solution.

The adopted vector then goes through crossover and elitist selection processes from the GA, meaning that it has incorporated the advantages of both the DE and GA techniques, resulting in a combination of global exploration and local opportunities from historical information, producing a hybrid method for searching.

3.2.2 Hybrid approach

The hybrid evolutionary algorithms have been a commonly adopted approach in tackling complex optimization problems. This hybrid algorithm takes both advantages from EGA's search procedure of selecting fittest individuals and the mutation operator which produces chromosomes that are better than their parents in DE. Throughout multiple sequential iterations of the ADE2GA process, the algorithm first takes advantage of ADE's memory retention and group search features, and dynamically navigates its underlying search direction to the global minimum. To represent the entire set of features to label for the target map, which is composed of point, line, and area features, the parameter N will be used. While line and area features involve variable-length continuous quantities, an ADE2GA search for

these features can be quite intensive to carry out, and could be not effective at all. The purpose of making the search feasible and tractable is achieved through the utilization of discretization, where all features are sampled at eight candidate locations so that the number of candidate locations is consistent for each feature type. The generation of an initial population is a significant part of the process of ADE2GA, and it also affects the algorithm's diversity and convergence properties, which are also tied to performance. The initial population must be generated randomly, as using some type of algorithmic generation of candidate location does not show sufficient diversity. Generating an initial random population using real-number encoding is a good way to represent candidate position. Using real-number encoding promotes adequate diversity in the population to explore the solution space more broadly, consequently supporting the performance potential of receiving optimal or near-optimal solution candidates.

A quality metric was developed which is used as the algorithm fitness function which should be minimized. We can see from Eq. (18).

$$S = \sum_{j=1}^{6} S_j X W_j \tag{18}$$

Here, the assignment of W_j will directly impact the value of S. By adjusting according to the above trial experiments, the final settlings of the weight of each factor were obtained W_1 = 0.5, W_2 = 0.3, W_3 = 0.15 and W_4 = 0.05. Mutation operator is to generate new gene combination which increases the population diversity while not destroying the superior genes of fitness individuals. Thus, mutations generally affect the less fit. Mutation operator randomly alters one or segments of genes of a chromosome. Such as a gene position on a chromosome being decremented. Which basically follows a differential process for mutation operation hence enhancing the global solution search ability of the algorithm, and the ADE which indicates the core part of ADE is the evolutionary algorithm based upon the differential and mutation operation. Assuming we can use the variation operator for $y_j(p)$ which is the jth individual in the pth generation under sufficient conditions. The difference between two pair of two of the six vectors is scaled with a scaling factor S and the resulting vectors are added together to create a new variation vector $V_j(p)$ (as defined in Eq. (19)):

$$V_j\,(p) = F\,(v_{j1}\,(p) - v_{2j}\,(p)) + F\,(v_{j3}\,(p) - v_{4j}\,(p)) + \; F\,(v_{j5}\,(p) - v_{6j}\,(p)) \tag{19}$$

where, the vector $V_j(p)$ after the mutation operation can exceed the search space, thus needing a repair. Randomly select six different based on the population six $v_j1\,(p)$, $v_j2\,(p)$, $v_j3\,(p)$, $v_j4\,(p)$, $v_j5\,(p)$, and $v_j6\,(p)$. Chromosomes have gene values between 0 and 9 according to their coding rules. If the new chromosome has a gene value out of the acceptable range, the vector is adjusted to make it operable with a repair operator defined as formulated in Eq. (20).

$$V_j(p) = \begin{cases} 0, & if\ v_j(p) < 0 \\ 9, & if\ v_j(p) > 9 \end{cases} \tag{20}$$

where, the ADE utilizes a discrete hybrid operator, $\mu_j\,(p)$, to enrich the diversity of the evolving population. The hybrid operator differs from conventional evolutionary algorithms because it commonly employs several exchange vectors from the parent reference vector only. The ADE presents a more dynamic mechanism for hybrid operator application, as the hybrid operator interacts with the reference vector and a repaired vector v_j, allowing for more flexible and adaptive recombination within the evolving population. A greater value of H_r gives a larger probability to hybridize to stimulate exploration within the search space and counter premature convergence. This process is formally shown in Eq. (21), describing through a mathematical expression how the hybrid operator works to appropriately balance exploration and exploitation within the ADE mechanism.

$$\delta_j(p) = \begin{cases} v_j(p) & if\ rand[0,1] < Hr \\ h_j(p) & else \end{cases} \tag{21}$$

where, $v_j\,(p)$ denotes the repaired vector and $h_j\,(p)$ denotes the reference vector are selected based on hybridization probability (H_r) or probability to hybridize in the population. The proposed work presents a hybrid security and privacy-preserving framework for the IoT, composed of a NTMVND approach and an ADE2GA. In the NTMVND module, we use topological measures (betweenness, degree, clustering, and centrality) to identify vulnerable nodes to ensure that vulnerabilities can be identified early on. The ADE2GA component, developed, optimizes secure routing for privacy-preserving transmission paths to the extent that they avoid these vulnerable nodes, which contributes to data integrity and/or confidentiality.

4 Results and Discussion

This section presents the simulation framework that was introduced to assess the proposed security model that combines network topology metrics with a deep learning–based hybrid optimization method. The framework serves

to implement and assess the proposed method through the modelling of relevant security functions, including privacy and integrity as well as key network performance metrics. The framework also allows for performance comparisons with traditional evolutionary optimization algorithms in the same simulation context. The algorithm parameters and configurations discussed in the previous section are employed in various scenarios to ensure a comprehensive assessment that provides consistent measures of the model's efficiency, adaptability, and robustness in the IoT context.

The essential variables for simulating a wireless network in Network Simulator-2. In a 100 × 100 m region, there are 50 nodes in the simulation, each with a starting energy of 1 J. With an omnidirectional antenna, a range for transmission of 200 meters, and a packet size of 512 kilobytes, the network operates on the 2.5 GHz carrier frequency. With an extra 5 dB of antenna gain, the link margin, gain factor, and receiver noise are all set at 40 dB, 30 dB, and 10 dB, respectively. The proposed method was assessed through multiple runs of the various parameters for statistical validity and robustness. Each objective function (privacy and integrity) was run consecutively, and the appropriate statistical metrics were recorded. In order to comprehensively assess its optimization ability, proposed hybrid method was evaluated for 100, 200, 300, 400, and 500 generations with resulting fitness values displayed in Figure 1 and Figure 2. The value of the selection of parameters was based on quantifiable parameters based on empirical data on the stability of convergence. For example, a population size of 50 provided an adequate tradeoff between speed of convergence and the computational burden associated with generating solutions. The adoption probability was evaluated as Padopt between 0.1 and 0.5 in order to assess the relative effects of the parameter on the sensitivity of this parameter with 0.3 providing an optimal balance between diversity of exploration and speed of convergence.

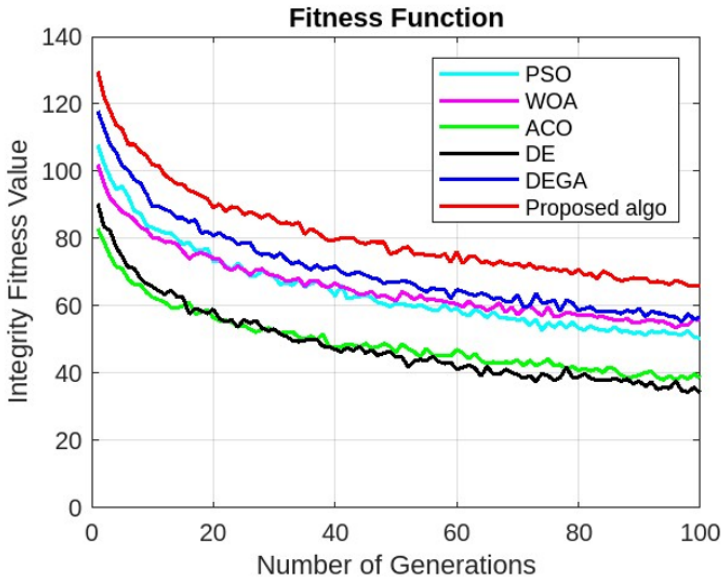

Figure 1. Integrityfitness function values comparison of the proposed framework with referenced methods

Fitness function was the main evaluation metric used, allowing a method performance comparison of the proposed method and several classic optimization methods. This included PSO [38], Whale Optimization Algorithm (WOA) [39], Ant Colony Optimization (ACO) [40], DE [41], and Differential Evolution with Genetic Algorithm (DEGA) [42]. As their evolutionary strategies differ, the methods referenced above show prior effectiveness in the optimization of complex problems. Utilizing environmental characteristics and convergence characteristics, the proposed method showed evidence of a greater level of adaptability and significantly increased convergence near the global optimum as identified in Figure 1.

A graph showing the performance of different optimization techniques over a predetermined number of generations is shown in the image. As a measure of optimization performance, the vertical axis is called the Fitness Value of the Integrity and the horizontal axis is called the Number of Generations, which illustrates how the algorithms have changed over time.

According to this, the proposed method outperforms the other algorithms in terms of maintaining the integrity fitness value throughout the number of generations. The fitness value of all algorithms decreases with the number of generations. As is common in optimization procedures where the solution gets better as the algorithm converges. All generations show that the proposed algorithm continues to perform better than the others with a greater fitness value indicating better optimization performance. ACO, WOA, DE, DEGA, and PSO all exhibit faster convergence, but to less ideal values. To assess scalability, tests were done on four densities of nodes in the same area (50, 100,

150, and 200 nodes). This test assesses the proposed framework's resilience when dealing with increased density and growth of the network. To ensure a fair, unbiased comparison, all baseline algorithms (ACO, WOA, DE, DEGA, and PSO) were tested with the same population size, stopping condition, transmission range, packet size and time of simulation.

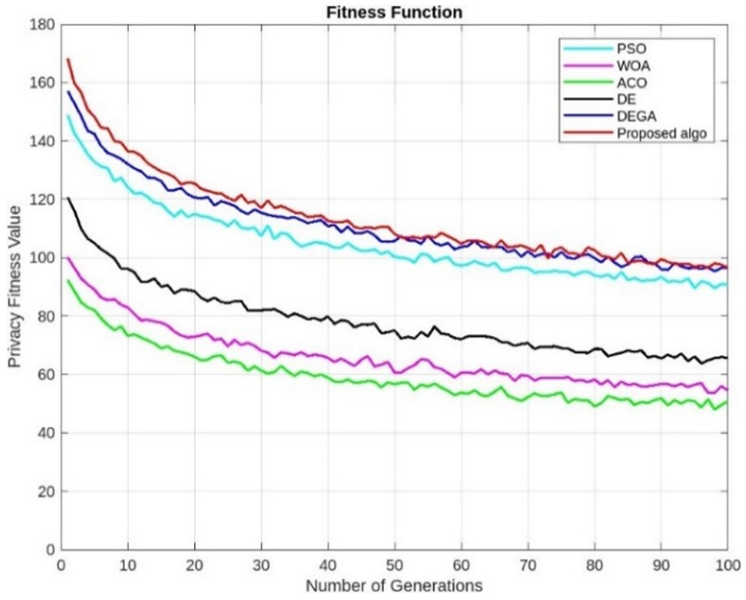

Figure 2. Confidentialityfitness function values comparison of the proposed framework with referenced methods

In Figure 2, the X-axis shows the number of generations, whereas the Y-axis depicts the fitness value for data privacy. Figure 2 demonstrates and compares the effectiveness of different optimization algorithms for maintaining node privacy in an IoT environment. The results show how the different algorithms progress across generations in optimizing the privacy objective function. The proposed ADE2GA method always produces a higher fitness value than the other algorithms, which illustrates ADE2GA's effectiveness for protecting data confidentiality and preventing privacy leaks when data are being transmitted. The most notable conclusion is that the proposed approach effectively maintains stronger privacy protection when compared to conventional evolutionary optimization algorithms over several generations. Compared to other optimization methods such as DE, WOA, PSO, ACO, and DEGA basic optimization methods, the proposed approaches achieved higher fitness values.

The proposed ADE2GA algorithm successfully enhances node privacy with higher stability and better optimized performance at generations. The overall results establish that the proposed method is more adaptive, reliable, and effective in terms of preserving privacy within IoT. PSO shown in cyan, begins with a high privacy fitness value and gradually decreases as generations increase. ACO is shown in green and it starts with a moderate privacy fitness value and declines fairly steadily before settling at a lower fitness value. DE is represented in black and has a smoother curve than PSO and WOA, but it starts with a lower privacy fitness value. This suggests that the reduction in privacy fitness value will happen more gradually. DEGA shown in blue it begins with a higher privacy fitness value than DE and performs better over time, but it is still less efficient than the proposed technique. The proposed algorithm is shown in red and always keeps the greatest privacy fitness value throughout all generations. Its slower fall in comparison to the other algorithms suggests that it performs better in terms of optimization when it comes to maintaining privacy.

The red line represents the proposed algorithm's superiority throughout 100 generations showing that it retains the greatest privacy fitness value. The algorithm appears to be more successful at maintaining privacy by striking a balance between exploration and exploitation as seen by the slower fall. Compared to the proposed algorithm and DEGA, the ACO and DE algorithms exhibit a more progressive fall, although they begin and conclude at lower privacy fitness levels. The proposed algorithm takes longer to converge, suggesting a more efficient search strategy that strikes a better compromise between protecting privacy by making use of well-known solutions and discovering novel ones.

Table 1 presents a comparison of the outcomes from the proposed ADE2GA with the other existing optimization schemes PSO and DEGA based on four metrics: End-to-End Delay, Throughput, Packet Delivery Ratio (PDR), and Energy Consumption. The results shows that ADE2GA significantly outperforms DEGA and PSO in all categories. For example, ADE2GA had an end-to-end delay of 70 ms, whereas DEGA had 95 ms, and PSO had 115 ms. The lower the time, the faster the data is transmitted due to the optimization routing process and avoidance of vulnerable

nodes. ADE2GA's throughput was higher than DEGA's and PSO's, being 580 kbps compared to DEGA's 480 kbps, and PSO's 410 kbps. Similarly, the Packet Delivery Ratio (PDR) of ADE2GA was 98%; compared to DEGA's 92%; while PSO had a higher PDR of 88%. The results show more reliable communication capability, secure transmissions can be done without concern for hackers or vulnerability. Lastly, ADE2GA results in the least energy consumed for each of the nodes at 0.50 J; DEGA had 0.59 J; and PSO consumed 0.68 J per node, ADE2GA's optimized routed is not only energy able to consume energy, it is likely to extend the life of an IoT network since energy consumed is an important component.

Table 1. Network performance comparison

Metric	Particle Swarm Optimization	Differential Evolution with Genetic Algorithm	Proposed Adoption-Based Differential Evolution with Elicited Genetic Algorithm
End-to-End Delay (ms)	115	95	70
Throughput (kbps)	410	480	580
Packet Delivery Ratio (%)	88	92	98
Energy Consumption (J/node)	0.68	0.59	0.50

Overall, these results substantiate that the proposed ADE2GA framework combines both hybridization and intelligence to optimize performance and reliability within an IoT network making the common tenets of integrity, privacy, performance and reliability in communication secure. Higher performance in ADE2GA can be attributed to its two stage design. The removal of structurally weak nodes using NTMVND reduces the area of search for reliable networks to only those areas of the network that are free of route failure. The adoption mechanism also speeds up convergence by allowing new solutions to incorporate the best genetic contributions of the top-performing individuals. The interaction between these two mechanisms produces a lower delay and higher throughput than the results observed for PSO and DEGA.

5 Conclusions

The IoT is a quickly expanding network of linked objects equipped with sensors to automatically gather and share data over the Internet without the assistance of a human. This paper describes a hybrid intelligent framework, ADE2GA, to enhance integrity, privacy, and performance in IoT networks, consisting of NTMVND to identify and isolate compromised nodes, combined with an ADE2GA to optimize secured routing paths. Incorporating adaptive mutation and crossover mechanisms into an evolutionary optimization approach allows the proposed approach to leverage the best of both worlds by managing exploration and exploitation during the path finding procedure to ensure reliable privacy-aware communication. Simulations confirm that ADE2GA outperforms previously reported optimization methods, such as PSO and DEGA, with decreased end-to-end delay (70 ms), increased throughput (580 kbps), an improved packet delivery ratio (98%), and decreased energy consumption (0.50 J per node).

The performance improvements promote the model's ability to continue providing secure, efficient, and energy-aware IoT operations. Future research will build on extending the proposed framework to dynamic IoT scenarios with opportunities for real-time learning mechanisms, and the validation of scalability across large-scale heterogeneous networks. While ADE2GA shows an improved performance over baseline algorithms, it was designed to work best in static moderate-density IoT networks. As the density increases and the design scales, performance will suffer because of the increased dynamic behaviour of the topology and computation overhead, so future work will explore how to adaptively tune weights and establish distributed estimates of vulnerability to improve performance in real-time in dynamic environments.

Author Contributions

Conceptualization, P.H.C., R.J.; methodology, P.H.C., R.J.; validation, R.K.S.; formal analysis, N.M.; investigation, B.G.J.; writing—original draft preparation, P.H.C.;writing—review and editing, S.R.; visualization, P.H.C.; supervision, R.K.S.; project administration, R.J. All authors were actively involved in discussing the findings and refining the final manuscript.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] B. J. Feng, H. Zhou, G. W. Li, Y. Zhang, K. Sood, and S. Yu, "Enabling machine learning with service function chaining for security enhancement at 5G edges," *IEEE Netw.*, vol. 35, no. 5, pp. 196–201, 2021. https://doi.org/10.1109/MNET.100.2000338

[2] B. J. Feng, A. Tian, S. Yu, J. Li, H. Zhou, and H. Zhang, "Efficient cache consistency management for transient IoT data in content-centric networking," *IEEE Internet Things J.*, vol. 9, no. 15, pp. 12 931–12 944, 2022. https://doi.org/10.1109/JIOT.2022.3163776

[3] H. S. Khati, K. Vishwakarma, S. Kumar, A. S. Bahuguna, Y. P. Pundir, K. Kumar, and S. Kala, "IoT-based water quality monitoring system," in *2025 IEEE International Conference on Computer, Electronics, Electrical Engineering & their Applications (IC2E3)*, Srinagar Garhwal, India, 2025, pp. 1–5. https://doi.org/10.1109/IC2E365635.2025.11167598

[4] D. Ameyed, F. Jaafar, F. Petrillo, and M. Cheriet, "Quality and security frameworks for IoT-architecture models evaluation," *SN Comput. Sci.*, vol. 4, p. 394, 2023. https://doi.org/10.1007/s42979-023-01815-z

[5] Y. Alotaibi, "A new meta-heuristics data clustering algorithm based on tabu search and adaptive search memory," *Symmetry*, vol. 14, no. 3, p. 623, 2022. https://doi.org/10.3390/sym14030623

[6] S. Deshmukh-Bhosale and S. S. Sonavane, "A real-time intrusion detection system for wormhole attack in the RPL based Internet of Things," *Procedia Manuf.*, vol. 32, pp. 840–847, 2019. https://doi.org/10.1016/j.promfg.2019.02.292

[7] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in Internet of Things," *J. Netw. Comput. Appl.*, vol. 84, pp. 25–37, 2017. https://doi.org/10.1016/j.jnca.2017.02.009

[8] A. Zahra and M. A. Shah, "IoT-based ransomware growth rate evaluation and detection using command and control blacklisting," in *2017 23rd International Conference on Automation and Computing (ICAC)*, Huddersfield, UK, 2017, pp. 1–6.

[9] S. Duangphasuk, P. Duangphasuk, and C. Thammarat, "Review of Internet of Things (IoT): Security issue and solution," in *2020 17th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON)*, Phuket, Thailand, 2020, pp. 559–562. https://doi.org/10.1109/ECTI-CON49241.2020.9157904

[10] X. Y. Yang, L. Shu, Y. C. Liu, G. P. Hancke, M. A. Ferrag, and K. Huang, "Physical security and safety of IoT equipment: A survey of recent advances and opportunities," *IEEE Trans. Ind. Informat.*, vol. 18, no. 7, pp. 4319–4330, 2022. https://doi.org/10.1109/TII.2022.3141408

[11] C. Xu, H. Liu, P. Li, and P. Wang, "A remote attestation security model based on privacy-preserving blockchain for V2X," *IEEE Access*, vol. 6, pp. 67 809–67 818, 2018. https://doi.org/10.1109/ACCESS.2018.2878995

[12] B. Larsen, T. Giannetsos, I. Krontiris, and K. Goldman, "Direct anonymous attestation on the road: Efficient and privacy-preserving revocation in C-ITS," in *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, Saarbrücken, Germany, 2021, pp. 48–59. https://doi.org/10.1145/3448300.3467832

[13] H. Xiong, Q. S. Mei, Y. F. Zhao, L. Peng, and H. Zhang, "Scalable and forward secure network attestation with privacy-preserving in cloud-assisted internet of things," *IEEE Sens. J.*, vol. 19, no. 18, pp. 8317–8331, 2019. https://doi.org/10.1109/JSEN.2019.2919508

[14] Y. Lu and L. D. Xu, "Internet of Things (IoT) cybersecurity research: A review of current research topics," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2103–2115, 2019. https://doi.org/10.1109/JIOT.2018.2869847

[15] F. Loi, A. Sivanathan, H. H. Gharakheili, A. Radford, and V. Sivaraman, "Systematically evaluating security and privacy for consumer IoT devices," in *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy*, Dallas, USA, 2017, pp. 1–6. https://doi.org/10.1145/3139937.3139938

[16] R. Kalakoti, H. Bahsi, and S. Nõmm, "Improving IoT security with explainable AI: Quantitative evaluation of explainability for IoT botnet detection," *IEEE Internet Things J.*, vol. 11, no. 10, pp. 18 237–18 254, 2024. https://doi.org/10.1109/JIOT.2024.3360626

[17] E. Altulaihan, M. A. Almaiah, and A. Aljughaiman, "Anomaly detection IDS for detecting DoS attacks in IoT networks based on machine learning algorithms," *Sensors*, vol. 24, no. 2, p. 713, 2024. https://doi.org/10.3390/s24020713

[18] M. Mohy-Eddine, A. Guezzaz, S. Benkirane, and M. Azrour, "An efficient network intrusion detection model for IoT security using K-NN classifier and feature selection," *Multimed. Tools Appl.*, vol. 82, pp. 23 615–23 633, 2023. https://doi.org/10.1007/s11042-023-14795-2

[19] S. M. Tahsien, H. Karimipour, and P. Spachos, "Machine learning-based solutions for security of Internet of Things (IoT): A survey," *J. Netw. Comput. Appl.*, vol. 161, p. 102630, 2020. https://doi.org/10.1016/j.jnca.2020.102630

[20] D. A. Sivasakthi, A. Sathiyaraj, and R. Devendiran, "HybridRobustNet: Enhancing detection of hybrid attacks in IoT networks through advanced learning approach," *Clust. Comput.*, vol. 27, pp. 5005–5019, 2024. https://doi.org/10.1007/s10586-023-04248-8

[21] S. Alangari, "An unsupervised machine learning algorithm for attack and anomaly detection in IoT sensors," *Wirel. Pers. Commun.*, vol. 144, pp. 1–25, 2024. https://doi.org/10.1007/s11277-023-10811-8

[22] N. Indrason and G. Saha, "Exploring blockchain-driven security in SDN-based IoT networks," *J. Netw. Comput. Appl.*, vol. 224, p. 103838, 2024. https://doi.org/10.1016/j.jnca.2024.103838

[23] V. T. Truong and L. B. Le, "Security for the metaverse: Blockchain and machine learning techniques for intrusion detection," *IEEE Netw.*, vol. 38, no. 5, pp. 204–212, 2024. https://doi.org/10.1109/MNET.2024.3351882

[24] C. Braghin, M. Lilli, and E. Riccobene, "A model-based approach for vulnerability analysis of IoT security protocols: the Z-Wave case study," *Comput. Secur.*, vol. 127, p. 103037, 2023. https://doi.org/10.1016/j.cose.2022.103037

[25] C. Hazman, A. Guezzaz, S. Benkirane, and M. Azrour, "lIDS-SIoEL: Intrusion detection framework for IoT-based smart environments security using ensemble learning," *Clust. Comput.*, vol. 26, pp. 4069–4083, 2023. https://doi.org/10.1007/s10586-022-03810-0

[26] D. Khan, M. Alonazi, M. Abdelhaq, N. Al Mudawi, A. Algarni, A. Jalal, and H. Liu, "Robust human locomotion and localization activity recognition over multisensory," *Front. Physiol.*, vol. 15, p. 1344887, 2024. https://doi.org/10.3389/fphys.2024.1344887

[27] J. N. Chen, Q. Wang, W. J. Peng, H. Y. Xu, X. D. Li, and W. Xu, "Disparity-based multiscale fusion network for transportation detection," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 10, pp. 18 855–18 863, 2022. https://doi.org/10.1109/TITS.2022.3161977

[28] J. Zhang, J. Ren, Y. Cui, D. Fu, and J. Cong, "Multi-USV task planning method based on improved deep reinforcement learning," *IEEE Internet Things J.*, vol. 11, no. 10, pp. 18 549–18 567, 2024. https://doi.org/10.1109/JIOT.2024.3363044

[29] L. Dhavamani, D. Ananthavadivel, P. Akilandeswari, and M. Nanajappan, "Differential privacy-preserving IoT data sharing through enhanced PSO," *J. Comput. Inf. Syst.*, pp. 1–17, 2024. https://doi.org/10.1080/08874417.2024.2364904

[30] R. Kumar, "Genetic algorithm based secure hybrid routing technique for IoT framework," *Int. J. Adv. Sci. Comput. Eng.*, vol. 6, no. 1, pp. 13–19, 2024. https://doi.org/10.62527/ijasce.6.1.194

[31] S. A. Solangi, D. N. Hakro, I. A. Lashari, K. U. R. Khoumbati, Z. A. Bhutto, and M. Hameed, "Genetic algorithm applications in wireless sensor networks (WSN): A review," *Int. J. Manag. Sci. Bus. Res.*, vol. 1, no. 4, pp. 152–166, 2017.

[32] K. Varnshney, S. Tripathi, and V. Purvar, "An efficient and reliable optimized routing protocol for IoT network in agriculture," in *2021 International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT)*, Bhilai, India, 2021, pp. 1–7. https://doi.org/10.1109/ICAECT49130.2021.9392553

[33] S. H. Park, S. Cho, and J. R. Lee, "Energy-efficient probabilistic routing algorithm for internet of things," *J. Appl. Math.*, vol. 2014, p. 213106, 2014. https://doi.org/10.1155/2014/213106

[34] A. Norouzi and A. H. Zaim, "Genetic algorithm application in optimization of wireless sensor networks," *Sci. World J.*, vol. 2014, p. 286575, 2014. https://doi.org/10.1155/2014/286575

[35] A. S. Hampiholi and B. P. Vijaya Kumar, "Efficient routing protocol in IoT using modified genetic algorithm and its comparison with existing protocols," in *2018 3rd International Conference on Circuits, Control, Communication and Computing (I4C)*, Bangalore, India, 2018, pp. 1–5. https://doi.org/10.1109/CIMCA.2018.8739759

[36] A. V. Dhumane, R. S. Prasad, and J. R. Prasad, "An optimal routing algorithm for internet of things enabling technologies," in *Securing the Internet of Things: Concepts, Methodologies, Tools, and Applications*. IGI Global Scientific Publishing, 2020, pp. 522–538. https://doi.org/10.4018/978-1-5225-9866-4.ch028

[37] R. Lal and K. Sharma, "GAEER: Genetic algorithm based energy efficient routing protocol in wireless sensor network," *Int. J. Sci. Technol. Res.*, vol. 9, no. 6, pp. 538–544, 2020.

[38] J. Kennedy and R. Eberhart, "Particle swarm optimization," in *Proceedings of ICNN'95-international conference on neural networks*, Perth, Australia, 1995, pp. 1942–1948.

[39] S. Mirjalili and A. Lewis, "The whale optimization algorithm," *Adv. Eng. Softw.*, vol. 95, pp. 51–67, 2016. https://doi.org/10.1016/j.advengsoft.2016.01.008

[40] M. Dorigo and T. Stützle, "Ant colony optimization: Overview and recent advances," in *Handbook of Metaheuristics*. Springer Nature, 2018, pp. 311–351.

[41] R. Storn and K. Price, "Differential evolution—A simple and efficient heuristic for global optimization over continuous spaces," *J. Glob. Optim.*, vol. 11, pp. 341–359, 1997. https://doi.org/10.1023/A:1008202821328

[42] P. Stubberud, "A hybrid genetic, differential evolution optimization algorithm," in *Ubiquitous and Pervasive Computing—New Trends and Opportunities*. IntechOpen, 2022. https://doi.org/10.5772/intechopen.106204