Computers, Materials & Continua

Tech Science Press

https://doi.org/10.32604/cmc.2026.076553

ARTICLE

Performance Evaluation of Malicious Node Detection and Mitigation of IoT-Based Trust Model for Wireless Sensor Network

Anil Kumar[1], Abhay Bhatia[1], Amit Singh[2], Preeti Rani[3,*], Vincent Omollo Nyangaresi[4,*] and Mahendihasan S. Heera[5]

[1]Department of Computer Science & Engineering, Roorkee Institute of Technology, Roorkee, Uttarakhand, India
[2]Faculty of Engineering, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
[3]College of Computing Sciences and IT (CCSIT), Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
[4]Department of Computer Science and Software Engineering, Jaramogi Oginga Odinga University of Science & Technology, Bondo, Kenya
[5]Faculty of Computer Science and Application, Gokul Global University, Siddhpur, Gujarat, India

*Corresponding Authors: Preeti Rani. Email: preetiresearcher1@gmail.com;
Vincent Omollo Nyangaresi. Email: vnyangaresi@jooust.ac.ke

Received: 22 November 2025; Accepted: 03 April 2026; Published: 08 May 2026

ABSTRACT: The Internet of Things (IoT) enables seamless real-time monitoring and data exchange across distributed and heterogeneous environments with wireless sensor networks (WSNs). The open architecture and resource constraints of wireless sensor networks (WSNs) make them highly vulnerable to internal security threats caused by malicious or compromised nodes, particularly in Internet of Things (IoT) environments. To address this issue, we proposed Dynamic Trust Evaluation Model (DTEM), designed to provide a secure, scalable, and efficient framework for IoT-based WSNs. The proposed model identifies the role of trust management in routing, data aggregation, and intrusion detection, including trust-based protocols. DTEM incorporates a lightweight elliptic curve cryptography (ECC) mechanism to ensure secure communication, protect trust information from manipulation, and enhance overall system reliability. In addition, machine learning techniques are employed to improve malicious node classification accuracy. Component-wise analysis demonstrates that the dynamic trust evaluation forms the core detection mechanism, while ECC enhances communication security and machine learning improves malicious node classification accuracy. A large-scale network simulation is conducted to evaluate DTEM's performance under various attack scenarios. Results demonstrate improved malicious node detection accuracy, higher packet delivery ratios, reduced energy consumption, and lower communication overheads. The proposed DTEM framework proves to be a robust and scalable solution for securing IoT-based wireless sensor networks, making it suitable for real-world applications.

KEYWORDS: Internet of Things; node detection; security threats; security and protocols; wireless sensor network

1 Introduction

IoT-connected devices are rapidly transforming conventional aspects of city life into intelligent, future-generation smart cities, where real-time data from IoT devices is used to make decisions. The smart city effort relies heavily on intelligent transportation systems (ITS), including connected automobiles [1,2]. Connected car technology will enable cars to interact with one another and with other roadside devices and infrastructure, such as current road conditions, heavy traffic, and vehicular crashes. As long as there are connected devices, the number of malicious devices will grow. Smart city cybersecurity demands differ from

traditional security concerns in that they continually evolve due to new technical developments and application scenarios [2]. Frequent topological changes and the high mobility of connected autos may exacerbate network design difficulties, making it easier for attackers to bypass authorised and authenticated users [3]. Because smart cities face cybersecurity issues, it was necessary to devise a novel method for establishing trust among devices in an untrustworthy environment [3]. In one technique, devices communicate with one another and learn whether to trust certain devices based on data analysis by developing and implementing trust management systems. While the second device has produced more trustworthy data, it has also been acting out or malfunctioning to a far lower degree of trust [2]. Trust management systems may be able to detect more rapidly which other devices are broadcasting legitimate data and which are broadcasting malicious or erroneous data. The following devices can agree on the accuracy of the data representation, raising or reducing trust in a device by inspecting the message's correctness using the device's own sensors. If the other devices agree that the message is genuine, the trustworthiness of the originating device will increase; if the message is mistakenly determined to be genuine, it will decrease [4]. Devices will be able to receive and act on data more rapidly and confidently if trust is established in smart cities. Smart cities and connected automobiles operate in a risky environment, making it challenging for cars to assess the dependability of incoming signals. According to [5], trust management systems are successful at mitigating risk; nevertheless, colluding attacks, which reward hostile vehicles for attaining a majority consensus on harmful material rather than being removed from the system, target the consensus processes of trust management techniques. Simply adopting the most widely used technologies will not be enough to reduce risk. As a result, a system that tracks both device data and behaviour is vital and urgently needed [6,7]. The research focuses on using driving data from linked vehicles to create a behavioral model specific to an area's typical driving patterns. This model helps analyse future data for consistency. Instead of relying on a majority vote, this approach uses data analysis to assess device trustworthiness accurately. Traditional trust systems use majority voting, but this proposal introduces a new method to reduce risk by integrating AI and machine learning. Machine learning processes data from various sensors to create a common behavioural model for connected vehicle networks [8]. This innovation enables smart cities and connected networks to detect and address hazards in real time.

The Internet of Things (IoT)-based wireless sensor networks (WSNs) operate in dynamic and open environments where internal attacks from compromised or malicious nodes significantly threaten network reliability and security. In such environments, attacks including malicious node behaviour, false data injection, packet dropping, selective forwarding, and man-in-the-middle interference directly disrupt routing, trust relationships, and data integrity. Although numerous trust-based security mechanisms have been proposed, most existing approaches rely on static trust computation, lack adaptability to dynamic network conditions, and often treat secure communication and intelligent detection as separate problems rather than as part of an integrated framework. Furthermore, many current models do not clearly distinguish between core trust evaluation mechanisms and supporting techniques, resulting in limited detection accuracy and weak resilience against evolving internal threats. To address these limitations, this study proposes a Dynamic Trust Evaluation Model (DTEM) designed to continuously assess node behaviour and accurately identify malicious nodes in IoT-based WSNs. The proposed framework establishes a structured and adaptive trust evaluation mechanism as its primary contribution, while lightweight cryptographic protection and machine learning–based classification act as supporting components to enhance communication security and detection precision. By integrating dynamic trust computation with complementary secure communication and intelligent classification mechanisms, the proposed approach improves malicious node detection accuracy, network reliability, and energy efficiency, thereby providing a comprehensive and scalable solution for secure IoT-based wireless sensor network environments. Recent studies have also explored machine learning-based

approaches to evaluate wireless sensor networks using radar signal analysis; however, these approaches mainly focus on network testing rather than adaptive trust evaluation for malicious node detection.

This paper clarifies the roles of trust evaluation, elliptic curve cryptography (ECC), support vector machines (SVM), and neural networks. This work presents a dynamic trust-based malware detection framework, with cryptographic and machine-learning components providing additional security and accuracy benefits. This paper focuses on internal security threats coming from compromised or malicious network nodes. Threat models considered include malicious node behavior, false data injection, packet dropping, selective forwarding, and man-in-the-middle (MITM) attacks. The attacks directly affect node-to-node trust relationships and disrupt routing, data aggregation, and decision-making.

A. Security Threats in Different Layers of IoT

An act that endangers safety takes advantage of an arrangement's safety constraints or negatively influences it by diminishing the organization's perceived worth. Fig. 1 demonstrates a range of possible attacks on IoT devices at various levels.

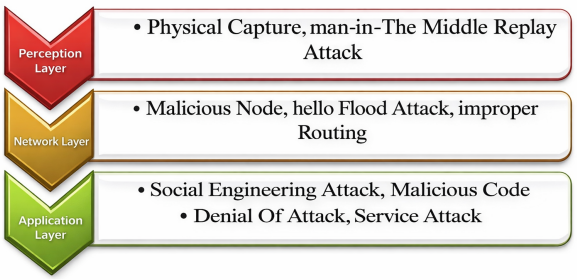

Figure 1: Attacks in different layers of IoT.

B. Security Issues in the Perception Layer in IoT

The intellect deposit is also called the sensing layer. This layer is accountable for gathering information and collecting physical data from all relevant devices. Data access and collaboration are the main functions of the vision layer. It has various sensors, including temperature and humidity sensors, GPS, RFID tags, and cameras. RFID knowledge or sensor system technology is the key equipment used in this layer. In the Internet of Things, the topology of dynamic networks or the sharing of features can lead to attacks or security threats [9]. Many different types of attacks can be carried out on so-called objects in the IoT scenario. Even though many applications that incorporate the concepts of the Internet of Things (such as smart homes, smart networks, and health surveillance) have improved, they still have significant weaknesses [10]. A recent study of safety vulnerabilities in IoT devices, such as garage door openers, has shown that anyone who might intrude can access the device, leading to other serious consequences. The protection of these IoT devices has prompted researchers to remove security vulnerabilities or shield them from multiple attacks.

C. Methods to Connect Various Devices

The potential benefits of vehicle-to-vehicle (V2V) communication for traffic enhancement and collision prevention are evident through the wireless transmission of nearby cars locations and speeds [11]. It is a way in which neighbouring automobiles exchange information about potential hazards that could cause accidents, according to the National Highway Traffic Safety Administration (NHTSA) [12]. While car manufacturers have yet to adopt connected vehicles fully, estimates suggest that equipping a basic vehicle with the necessary communication devices and sensors could cost around $350 [13,14]. The integration of

ultrasonic, camera, and radar systems, along with other sensors, aims to provide drivers with comprehensive environmental information beyond their immediate field of view. Sensor nodes in a Wireless Sensor Network (WSN) can monitor a wide range of physical and environmental properties without requiring extensive infrastructure [15]. However, managing WSNs is challenging due to interconnectedness, resource limitations, complexity, scalability, dynamics, and the nature of random node deployment with decentralised topology [16]. Uneven distribution of resource-constrained nodes in response to dynamic network changes and behaviour poses difficulties, and routing is identified as a primary contributor to these constraints [17]. As random node deployment and decentralised network topology present challenges, efficient mechanisms are needed to enable nodes to make accurate, autonomous decisions. Among various approaches, trust-based mechanisms have proven effective in aiding nodes in decision-making. The purpose of this paper is to propose distributed decision-making protocols leveraging trust-based mechanisms for randomly distributed and decentralised WSNs [18,19]. The objective is to enhance routing efficiency by facilitating improved forwarder selection and mobile sink relocation within these networks.

D. Objectives of the Study

The main objectives of this study are as follows:

- To develop a dynamic trust evaluation model capable of accurately identifying trustworthy and malicious nodes in IoT-based wireless sensor networks under dynamic and resource-constrained environments.
- To mitigate the impact of security threats, including false data injection, packet dropping, and man-in-the-middle attacks, by incorporating trust-based decision-making mechanisms.
- To enhance overall network performance in terms of security, energy efficiency, and reliability by integrating lightweight trust assessment and secure communication techniques.

2 Literature Review

The literature review includes a range of research perspectives on IoT security and trust management. The Internet of Things is transforming the real world into a virtual network [20]. As the Internet of Things develops, security becomes more challenging. As a result, trust is an essential component of IoT device security. Reducing uncertainty between communication parties is the goal of the Trust Management System (TMS). An approach that builds trust by directly interacting with servers, guided by user experiences, emerges as a potential solution. As part of this work, we explore how users' experiences of interacting with servers in different contexts can be leveraged in a context-based trust management system. The Naïve Bayesian classification approach serves as the foundation for the strategy. In a context-based trust-building process, filtered and categorised direct user experiences across different contexts are used to build and continuously update trust over time. Web services datasets were used to test the suggested protocol, and the findings indicate that trust-building that accounts for contextual information offers a viable option.

The extensive collection of data and interconnectedness of IoT devices, coupled with inadequate IoT security, make it relatively easy for attackers to access data traffic. Routing protocol IPv6 is widely used for Internet of Things networks that operate in low-power, lossy networks (RPL). However, RPL exhibits limited defence against specific attacks inherent to WSNs and RPL-specific threats in IoT applications. Moreover, the constrained resources of IoT devices hinder the effective implementation of conventional internet and routing security solutions. Various strategies have been proposed to address IoT routing and security concerns, including machine learning and intrusion detection systems. Despite existing trust-based methods, little attention has been given to node mobility, especially for mobile sink nodes, in countering RPL attacks. The paper presents SM-Trust, a concept for securing the Internet of Things routing protocol using mobility-based trust metrics. With SM-Trust, it will be protected against common RPL assaults, including

Rank, Version Number, Black-Hole, and Grey-Hole attacks. Currently, DCTM-RPL and SecTrust-RPL do not account for sensor or sink node mobility, which is where the advances lie. Improved network performance, more accurate attack detection, and better scalability than existing trust models are expected outcomes. It is appropriate for a mobile IoT context for this reason. When incorporated into RPL, the suggested SM-Trust design as a secure routing protocol will guarantee availability, secrecy, and integrity in IoT networks and in communication between sensor nodes throughout the routing process [21].

In the IoT ecosystem, building trust amongst decentralised entities is essential. It can be addressed by combining blockchain technology with trust evaluation methods. However, both technologies encounter limitations in the IoT landscape, which this study aims to tackle. Initially, the paper assesses various trust approaches based on blockchain, highlighting their strengths and weaknesses within decentralised IoT communities. Following this, it introduces a multi-layered adaptive trust model based on weighted trust considerations. The study also describes many trust-metric parameters and the accompanying mathematical models. A smart contract and control loop are also presented as a novel approach to rewarding actions in the IoT marketplace. In the end, the study confirms that the suggested trust model is reliable. The provided approach offers greater resilience against a variety of attacks than current ones, according to experimental results from diverse scenarios [22]. Internet of Things (IoT) refers to a new era of technology in which people, computers, and objects exchange information through the internet. Building trust among decentralised entities within the IoT ecosystem is of significant importance. Consequently, integrating blockchain technology with trust evaluation methods has emerged as a promising avenue. However, both technologies face limitations in the IoT sphere, prompting this research to address these challenges. First, the paper examines the advantages and disadvantages of blockchain-based trust strategies in decentralised IoT networks. A multilayer adaptive trust system with weighted trust factors is then introduced as part of an enhanced trust model. In addition to describing trust-metric parameters, the article also provides mathematical models for evaluating trust. The paper also presents a novel way to reward members' continuous improvement through control loops and smart contracts in the IoT marketplace. In the end, the investigation confirms that the suggested trust model is reliable [23].

In transportation, the Vehicular *Ad Hoc* Network (VANET) allows vehicles to communicate critical information—such as road warnings—in real time, enhancing safety and comfort. However, ensuring a secure environment within VANET is imperative to prevent attacks that could spread misleading information among network nodes. Establishing trust between vehicle nodes is one useful method of managing network security and dependability. VANET Trust Models (TMs) can be categorised into three types (ETM, DTM, and HTM). These models employ a range of procedures to assess confidence based on data received, the vehicle itself (entity), or a combination of the two. This essay compares these three Trust Models in VANET environments. They also contrasted these TMs with additional security, trust, and service quality criteria. Based on simulation studies, all of these TMs exhibit short end-to-end durations, low event-detection probabilities, and high false-positive rates [24]. There are three levels at which the trust value is calculated: SN, CH, and BS. Timing windows are necessary for measuring on-off attacks and accounting for time. It is based on the success or failure of contacts or transactions that the trust value is calculated. Each node is assigned one of the three trust states: trusted, untrusted, or undefined. Each CH periodically asks CMs to report their trust state, and thus CH estimates each CM's trust value. Functions of a BS include maintaining BS-CH past interaction and estimating the trust value for all CHs. Group-Based Trust Management Scheme (GTMS) does not require large data storage or processing power, and it is resistant to the effects of malicious nodes [25].

The trust mechanisms are generally divided into: (1) behavior-based trust evaluation models, (2) cryptography based trust-based mechanisms; methods to elect nodes with no/less malicious intent based

on machine learning algorithms and hybrid-trust management models. We show that the most relied-on factors in our behaviour-based models are (i) packet forwarding behaviour, (ii) interaction history and (iii) recommendation trust. However, these methods suffer from the static trust calculation problem, and are not well-adapted to dynamic environments. In general, cryptography based schemes in the literature are focused on enhanced secure communication and authentication [6], but concerns to balance data confidentiality and integrity rather than maintaining continuously assessing nodes' behavior trust. Machine learning–based methods can improve detection accuracy, but usually have more computational overhead and therefore not suitable for resource-constrained IoT environments.

The proposed SMART model provides enhanced security and accuracy by generating trust values in a fast and trustworthy manner [26]. A novel ML algorithm is used to derive multiple trust features, including co-location relationships (CLRs), co-work relationships (CWRs), and cooperativeness-frequency-duration (CFD). A hybrid framework, Trust-Enhanced Anomaly Detection (TEAD), is proposed to enhance intrusion detection in IoT-WSNs by integrating trust evaluation and anomaly detection based on machine learning [27]. TEAD dynamically calculates trust scores based on communication weight ratio, communication link reliability, and communication frequency deviation for network nodes. A trust-aware edge-assisted model is proposed, which enhances routing performance and is more reliable [28]. Data privacy and coherence are achieved through localized computing in keeping with global trust models. Additionally, the IoT-ITS environment includes a blockchain ledger for tamper-proof and transparent computing. An evolutionary particle swarm optimization scheme, EPSTM, is proposed for authentication of IoT nodes and the mitigation of malicious behavior [29]. For secure routing, the scheme uses network-specific metrics, including proximity to devices, energy consumption, reliability of data transmission, and message delivery timing. Author [30] presents a Trust-Based RPL Intrusion Detection System (TIDSRPL) as an advanced design. A complex trust is transferred from the root node to TIDSRPL, which evaluates the node trust in accordance with the network behavior. This strategic shift preserves energy, storage, and compute resources at the node level.

Recent studies have also explored machine learning techniques to improve the reliability and evaluation of wireless sensor networks. Author [31] investigates the use of radar signal analysis combined with machine learning algorithms to evaluate the behaviour and reliability of wireless sensor networks. The study demonstrates that machine learning techniques can effectively identify abnormal network behaviour and improve system evaluation in emerging WSN environments. However, such approaches mainly focus on signal-based testing and performance evaluation rather than continuous trust assessment among communicating nodes. Many of the current solutions do not adapt the trust dynamically against behavioural changes, are unable to resist orchestrated internal attacks and security-energy communication tradeoffs. These constraints reveal the need for a context-aware and flexible trust model that combines lightweight security elements with intelligent trust estimation. To address these gaps, in this paper we present a structured and dynamic trust computation mechanism suitable for the dynamic IoT based WSNs environment named Dynamic Trust Evaluation Model. It has been proven the ability to observe in real-time the behavior of nodes which guarantees close trust exchange information and accurate detection to malicious nodes as well as DoS resistant. Because the proposed scheme puts emphasis on the revealed drawbacks of existing schemes, however as a result, we get higher detection rate and more reliable; more secure against inside attacks than other recent trust models.

A. Comparative Study of Different Trust Schemes

Various trust management systems address efficiency and security in distributed environments, each with distinct strengths and limitations as mentioned in Table 1. GTMS reduces communication and memory overhead through clustered grouping in hybrid architecture but requires additional resources and is

vulnerable to on–off attacks. TMA similarly lowers overhead and handles dynamic trust in a hierarchical structure, though it remains susceptible to attacks and unreliable recommendations. LDTS improves security and reduces energy use but relies on a static trust function. The method in [32] enhances resilience to on–off attacks using binomial and weighted distributions, yet it is sensitive to false positives. ADCT decreases overhead and filters untrustworthy recommendations but lacks explicit attack detection. LTS further reduces overhead and improves security with Beta-based clustering, although it does not account for misbehaviour frequency or weight. ETS lowers communication and memory costs through an energy-based clustered mechanism but features inflexible punishment and reward schemes, moderate complexity, and vulnerability to Sybil attacks.

Table 1: Comparative study of different trust schemes.

Schemes	Objective	Mechanism	Architecture	Gap
GTMS [25]	Communication and memory overhead reduction	Group (clustered)	Hybrid	More resources, not resilient to on-off attacks
TMA [33]	Minimising communication and memory overhead, the dynamic aspect of trust	Group	Hierarchical	Vulnerable to attacks, untrustworthy recommendations
LDTS [15]	Overhead reduction, energy saving, and more security	Weight (clustered)	Hybrid	Static trust function, vulnerable to attacks
ADCT [34]	Reduce untrustworthy recommendations, reduce overhead	Distribution Beta (clustered)	Hybrid	No attack detection
ETS [35]	Communication and memory overhead reduction	Energy system (Clustered)	Hybrid	Punishment and reward are not flexible, modest complexity; owing to the Sybil attack, a small percentage of misbehaviour cannot be detected

3 Methodology

The Dynamic Trust Evaluation Model (DTEM) is proposed to be an integrated model where dynamic trust computing is taken as the kernel, while secure communication and intelligent classification are regarded as auxiliary approaches to further improve reliability of trust and system detection performance. In DTEM mechanism, trust estimation serves as the key decision factor and keeps a vigilant eye on node behavior by computing dynamic trust values based on factors like packet forwarding confidence, interaction history and packet drop ratio for identifying potentially malicious nodes underpinning secure routing decisions. Machine learning is adopted as an assistant module based on which the computed trust features and behavioral parameters are exploited in order to enhance classification performance of malicious nodes, especially under complicated and uncertain network situations instead of replacing with a trust evaluation.

Meanwhile, ECC-based authentication is adopted to securely register nodes, exchange keys and transmit trust information over the network, based on its lightweight cryptography feature for resource-constrained

IoT setting. With secure communication and dynamic trust computation based on machine learning-assisted classification, the proposed DTEM framework is capable of offering an integrated and adaptive solution for accurate malicious detection and remediation in IoT-based wireless sensor networks, thereby mitigating the challenge of identifying trustworthy participants in IoT systems designed to serve as smart-city infrastructure while featuring the use of dynamic blocklist/allowlist mechanisms aimed at enhancing service reliability and network performance.

There is also an approach for estimating trust in clustered WSNs. The SN, CH, and BS levels determine the trust value. To measure on-off attacks and ignore the impact of time, a timing window is necessary, using successful and unsuccessful interactions or transactions as a measure of trustworthiness. A node's trust state can be trusted, untrusted, or undefinable. Each CH periodically asks CMs to send their trust states, and thus CH estimates each CM's trust value. Functions of a BS include maintaining BS-CH past interaction and estimating the trust value for all CHs. GTMS resists the effects of malevolent nodes, and Computational resources and large data storage are not required. Eq. (1) is used to estimate trust value. Using the following equation, node x calculates node$y's$ trust:

$$T_{x,y} = \left[100 * \frac{\left(S_{x,y}\right)}{\left(S_{x,y} + U_{x,y}\right)\left(S_{x,y} + 1\right)} \right] \tag{1}$$

Though determining trustworthiness solely based on successful and unsuccessful interactions may not accurately reflect a node's exact honesty. Nevertheless, GTMS is robust to attacks provided that $S_{x,y} \leq U_x$. In this work, an agent node is tasked with monitoring the performance of sensor nodes within a network and classifying behaviour as genuine or malicious. An agent node keeps an individual count of good and bad behaviour and saves the results into rows. The agent, hence, saves computational resources and energy. ATSN does not calculate recommendation trust. However, it estimates only the direct trust value, and the model does not account for updating trust value. The author aims to minimise communication and storage overhead using a hierarchical trust management scheme. It comprises a high-power node, a superior node (base station), a CH, and multiple sensor nodes forming a cluster. The sensor nodes gather data from their environments and transmit it directly to the CH, either in a single hop or via multiple hops. Sponsors and targets are present in this scheme as nodes in the communication process. Sponsor nodes initiate all transactions between nodes, and target nodes are selected by sponsor nodes to collaborate. Target nodes can be more than one. Each node computes direct trust for every other node and sends it to CH. CH stores this information as indirect trust information. Each node's direct trust value is also stored in CH. By combining the direct trust value with the group's trust value, the CH now calculates the integrated trust value. The scheme maintains cooperation records. Eq. (2) can be used to calculate the AI trust value based on this table [36].

$$t_{Ai} = 100 * \frac{S_i}{CC_i} \tag{2}$$

In Eq. (2), CC_i is cumulative cooperation and S_i is the number of successes, and its value lies between 0 and CC_i. The trust value is measured on a scale of 0 to 100. This scheme is suitable for a dynamic environment, as it allows nodes to move between clusters while preserving their trust records. The proposed arrangement is compared with GTMS, as both schemes have a similar architecture. A clustering method, LDTS, in which nodes with high processing power are designated as CH, was proposed. In the suggested work, CH evaluates the trustworthiness of the CMs in its cluster. Since CH takes care of it, respectful CMs are not required to retain feedback from other CMs. Dependency improved trust-evaluation methods between CHs, as they need large amounts of data to be forwarded. A self-adaptive weighting technique is part of LDTS.

By observing both successful and unsuccessful interactions, it determines the neighbours' trust at the CM level. Trust is calculated based on previous interactions at the CH level. CH then gives BS trust values. The trust between CM-CM and CH-CM exists within a cluster, and the trust between CM-CH and CM-BS exists between clusters [15].

$$T_{x,y}(\Delta t) = \left[10 * \frac{S_{x,y}(\Delta t)}{\left(S_{x,y}(\Delta t) + U_{x,y}(\Delta t)\right)}\right]\left(\frac{1}{\sqrt{U_{x,y}(\Delta t)}}\right) \tag{3}$$

Trust value is set to [37]; therefore, lower memory and transmission overhead. However, when calculating trust value, LDTS employs a strict punishment coefficient along with a static trust function. An increase in the number of unsuccessful transactions quickly leads to the punishment feature $1/\sqrt{U_{x,y}(\Delta t)}$. The arrangement calculates both direct and indirect trust. BTMS has better resistance to attacks. In this scheme, data safety is ignored, but most prevailing trust models focus on data trust as a core concern [38]. A robust and lightweight trust estimation approach is proposed here. To make this approach lightweight and trustworthy, it computes the weights of the misbehaviour and misbehaviour-frequency components. The rate of misbehaviour is determined using a time-window notion for the time unit j, as shown in Eq. (4).

$$R_j = \begin{Bmatrix} 0 & \text{if } \dfrac{U_j}{U_j + S_j} \le \theta \\ \dfrac{U_j}{U_j + S_j} & \text{Otherwise} \end{Bmatrix} \tag{4}$$

According to the above rate, SN evaluates the weight of false behaviour (misbehaviour) using Eq. (5).

$$W_{tk}^{m} = \max(\alpha 1 r 1, \alpha 2 r 2, \ldots, \alpha_L r_L) \tag{5}$$

This model gives more weight—and, consequently, greater importance—to recent achievement while devaluing prior, measured behaviour. The older observations are ignored using an exponential reduction algorithm. This strategy aims to protect against on-off attacks, which cause behaviour to switch between good and bad states over time. Therefore, this strategy reduces the impact of on-off attacks when malicious nodes alternate between good and harmful behaviour. Eq. (6) calculates the trust value,

$$T_{tk} = 1 - W_{tk}^{m} \tag{6}$$

Eq. (7) calculates the frequency of misbehaviour,

$$f_{tk}^{m} = \frac{O_{tk}}{O_{tk} + P_{tk}} \tag{7}$$

where, O_{tk} and P_{tk} are on and off periods, respectively. Following recognition of node status, the final trust value is calculated by aggregating W_{tk}^{m} m and f_{tk}^{m} mas as shown in Eq. (8).

$$T_{tk} = \begin{Bmatrix} \left(1 - W_{tk}^{m}\right) & \text{if } W_{tk}^{m} > f_{tk}^{m} \\ \beta * \left(1 - f_{tk}^{m}\right) + (1 - \beta) * \left(1 - W_{tk}^{m}\right) & \text{otherwise} \end{Bmatrix} \tag{8}$$

There is a greater risk of false-positive alerts with the scheme than with other current schemes. However, it has been verified to be better than GTMS [25] and LDTS [15]. The plan is limited to one-off attacks. The suggested work, by highlighting the trust function's adaptability based on packet loss and application error tolerance, ADCT facilitates nodes' cooperation. A network's cooperativeness is assessed by evaluating

communication and data trust between SNs. It is suggested that clustered WSNs be used in the proposed plan. It is familiar with a filtering method used by ADCT. This function allows ADCT to assess SN's reputation at the BS and CH levels despite unreliable recommendations. When a recommendation deviates further from the average of all recommendations, BS may disregard communication trust feedback. The equation for direct trust calculation is given as follows,

$$T_{ij} = 10 * p\,(1-p)\,\alpha \tag{9}$$

$$P = \left[\frac{S_{x,y}\,(\Delta t)}{\left(S_{x,y}\,(\Delta t) + U_{x,y}\,(\Delta t)\right)} \right] \tag{10}$$

For both direct and indirect trust, LWTS proposes a self-adaptive weight distribution method using Eqs. (11) and (12) at the CH level as follows to overcome the difficulties associated with weight allocation,

$$W_1 = 1 - \left(\frac{S^{direct}_{chi,chj}}{S^{direct}_{chi,chj} + S^{indirect}_{BS,chi}} \right) \tag{11}$$

$$W_2 = 1 - \left(\frac{S^{indirect}_{BS,chi}}{S^{direct}_{chi,chj} + S^{indirect}_{BS,chi}} \right) \tag{12}$$

where W_1 provides more weight to direct trust while W_2 provides more weight to indirect trust. Where $S^{direct}_{chi,chj}$ is the successful interaction between ch_i & ch_j and $S^{indirect}_{BS,chi}$ is the positive or constructive recommendations about chi gathered by BS from other adjoining CH. To reduce communication overhead, LWTS allows every CM to connect directly with the CH. Based on the findings, LWTS performs better in terms of memory and communication overhead than both GTMS [25] and LDTS [15]. However, scalability has not been addressed in the suggested work [39]. Outstanding features comprise the anticipated LTS. In addition to being immune to attacks, it offers a robust trust estimation function. At CH, mild or basic trust aggregation is used. To combat rogue nodes, data trust and communication trust must be combined. Initially, each SN is assigned a unique identity to facilitate transmission and protect it from external threats. A well-recognised algorithm is used to form clusters. Through its distributed and centralised strategies, LTS ensures that trust judgments are made appropriately at both intra- and inter-cluster levels. To track interactions and determine their success, a timing-window method is used. Due to its ability to customise the penalty coefficient and the trust function's harshness according to application requirements, the method is novel. The Eq. (13) to calculate communication trust between CMs is given as follows:

$$T^{C}_{x,y}\,(\Delta t) = \left[4 * \frac{S^{C}_{x,y}\,(\Delta t)}{\left(S^{C}_{x,y}\,(\Delta t) + U^{C}_{x,y}\,(\Delta t)\right)} * \left(\frac{1}{\sqrt{U^{C}_{x,y}\,(\Delta t)}} \right) * \left(\frac{S^{C}_{x,y}\,(\Delta t)}{S^{C}_{x,y}\,(\Delta t) + 1} \right) \alpha \right] \tag{13}$$

A domain of trust value is a simple averaging scheme for aggregating trust values among cluster heads, introduced to address the limitations of existing schemes. Collusion and on-off attacks cannot be mitigated very well with LTS. The proposed ETRES is used to assess a sensor node's reputation and trust. This method determines the node's reputation and trustworthiness using an exponential distribution. In addition to the state of a successful encounter, it can create a TMS without accounting for additional states. The confidence factor, computed from many successful interactions, is redefined. It can quickly lower the direct trust value, lessening the effect of rogue nodes. The suggested plan is capable of effectively fending off internal outbreaks (attacks). The scheme's performance results are compared with those of the beta approach, and they show

a modest difference. The proposed hybrid TMS model estimates the trustworthiness of the sensed data item by inspecting data consistency using a data correlation technique. This approach doesn't work for estimating trust for non-numeric data. Data semantics can be used for non-numeric data. Moreover, a misbehaviour component is absent from trust estimation. The proposed RFSN approach enables nodes to estimate other nodes' trustworthiness based on reputation. It evaluates the behaviour of neighbouring nodes using a watchdog mechanism and characterises node reputation using Beta distributions. The scheme is robust. The recommendation trust is not taken into consideration. It is not resistant to several internal attacks.

A. Algorithm Procedure

The proposed methodology aims to strengthen IoT networks by leveraging elliptic curve cryptography for robust security. The process involves a multi-step approach encompassing network initialization, secure key generation, device registration, and authentication. According to the proposed methodology, the steps are as follows:

Step 1: Initialise the network with network specifications.

Step 2: IoT nodes location evaluations and coverage area evaluation.

Step 3: Create a secure network that uses a lightweight authentication protocol to reduce the impact of attacks in the Internet of Things.

Step 6: Implement the Attack to evaluate network performance.

Step 5: Use a supervised neural network with backpropagation to optimise the model.

Step 6: Evaluate the network's performance to enhance network life or security.

Public key encryption based on algebraic organisations of elliptic curves over finite fields [23]. The area over which an elliptic curve is distinct is known as the size of the elliptic curve key. It does not always correspond to the precise size of the private key. Below is a high-level explanation of the algorithm:

Key Mechanism: In AWSC, the private key is either utilised to generate a signature or is known by the sender (signer). The public key can be established by a trusted party or disseminated to all communication partners.

Key Generation: In this algorithm, the sender chooses a private key and the receiver's public key. Where d' denotes the sender's specific key, and 'A' regulates the elliptical curve.

Key Distribution Method: An exchange of Diffie-Hellman keys or another key-exchange mechanism is used to send the recipient's public key, while the sender's private key remains secret.

Signing Mechanism: Using a reliable hash function, this procedure begins by preparing the hash or decrypting the message to be signed. Using a numerical calculator to determine a numerical value is the second step. This neutral integer serves as a value for the elliptic curve computation. The email will then be signed, or the sender will give the receiver a random number along with the signed email.

Verification Mechanism: This is the third mechanism. When a signed communication is delivered to the recipient, it is the signing method. In this instance, the verifier's (the sender's) public key can be utilised to confirm the message's authenticity. An elliptic curve's equation is:

$$Y^3 = X^3 + ax + b \tag{14}$$

Eq. (14) defines the curve where X and Y are coordinates on the curve, and a and b are constants that determine its shape and properties. The nature of this elliptic curve serves as the foundation for generating secure cryptographic keys and facilitating secure communication between parties in the system. Using Eq. (14), we derive the public key through the procedure defined in [40]:

$$Q = d \times p \tag{15}$$

This Eq. (15) defines the random number selected from 1 to n−1; p denotes the private key; Q denotes the public key.

A. Encryption

In the context of elliptic curve cryptography, the process involves transmitting a message m represented by the point M on the curve E. To ensure security, a random value k is selected from the range $[1 - (n - 1)]$, leading to the creation of two cypher messages C_1 and C_2.

$$C_1 = k \times P \tag{16}$$

Using Eq. (16), we can retrieve the original message:

$$M = C_2 - d \times C_1 \tag{17}$$

Utilising the private key d, the original message M is obtained by subtracting the product of d and C_1 from C_2. This process ensures the recovery of the original message from the cypher messages. In this process, IoT devices and gateways will be initialised with a pre-defined security code. Before any data-gathering operations can be performed, a new device must register with the gateway. To verify and register the new device, the intermediary gateway generates a hidden value v. Before attempting to connect to other devices on the network, each new device must complete this registration process. This process starts with exchanging ID and password at the gateway. First, the device or gateway will use ECC to secure the main contract and transmit the device's certificates to the gateway. A symmetric key is placed between two companies to complete the registration process. It helps prevent the attacker from flying while sending a device certificate.

B. Phase of Device Authentication

Step 1: Compute the symmetric key and generate a random number.

Step 2: Now, it computes the symmetric key using an intermediate hidden value and a decryption technique to produce a random number.

Step 3: It sends the messages to the receiver after decryption using a symmetric key.

Step 4: After this process, it is recovered using a symmetric key via decryption and computes session key 0.

Step 5: After completion of this process, it will be reversed.

Step 6: And then we use the same encryption-decryption technique with the same symmetric key and session key.

By incorporating attack models for trust evaluation, this protocol identifies and addresses malicious and selfish nodes that can generate misleading network traffic, thereby establishing accurate trust values among neighbouring nodes. The objective of these trust models is to enhance application security by ensuring that data is double-checked before transmitting prescription information to users. The proposed protocol ensures secure data exchange among devices, prioritising accuracy through verification and lightweight computation, and is particularly suitable for devices within patient, employee, or server networks, as illustrated in Fig. 2. The DTEM framework operates in three logical stages: secure communication using ECC, trust computation based on node behavior, and machine learning–based classification for malicious node detection.

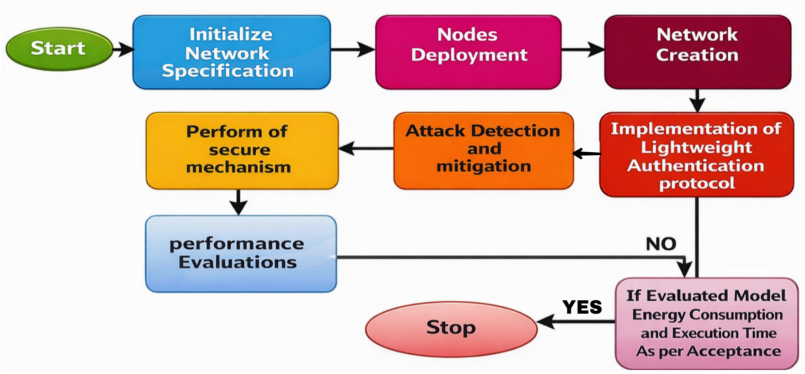

Figure 2: Proposed flow diagram.

This methodology integrates advanced cryptographic techniques and secure protocols to strengthen IoT network integrity and ensure secure data transmission between devices and gateways. DTEM integrates secure communication, dynamic trust evaluation, and intelligent classification into a unified framework for malicious node detection in IoT-based WSNs. To clearly analyse the individual contribution of each component in the proposed Dynamic Trust Evaluation Model (DTEM), an additional component-wise evaluation is conducted. The DTEM framework consists of three main elements: dynamic trust evaluation, ECC-based secure communication, and machine learning–based classification. The dynamic trust evaluation mechanism serves as the primary decision-making component responsible for monitoring node behaviour and computing trust values based on packet forwarding behaviour, interaction history, and packet drop rate.

The ECC module provides lightweight cryptographic protection to ensure secure key exchange and prevent manipulation of trust information during node communication. This component primarily enhances communication security rather than directly affecting malicious node detection accuracy. The machine learning component (SVM classifier) utilises behavioural trust parameters as input features to improve the classification accuracy of malicious nodes under dynamic network conditions. Therefore, machine learning acts as a decision-support module that refines trust-based detection rather than replacing the trust computation process. To evaluate the effectiveness of each module, three experimental configurations are analysed: (1) trust-based detection without additional security mechanisms, (2) trust evaluation combined with ECC-based secure communication, and (3) the complete DTEM framework integrating trust evaluation, ECC security, and machine learning classification. This component-wise analysis highlights the contribution of each module to the overall detection accuracy and network performance.

4 Results and Discussions

The performance of the proposed model is evaluated in a MATLAB simulation environment based on 500 × 500 network area, with randomly placed 30 sensor nodes to simulate the actual wireless sensor network scenario. All essential assets of simulations, such as network topology, node density, communication range, trust evaluation intervals and machine learning settings are now clearly described for reproducibility. Towards practical WSN operation, the experimental setup provides two communication modalities: node-to-node interaction and node-to-base station communication. Due limited resources, this class of networks is vulnerable to various security threats and in particular the work concentrates on potential attacks like Man-in-the-Middle (MITM) attacks where the attacker can eavesdrop or modify genuine communication between nodes.

The proposed DTEM combines secure communication, trust-based monitoring and machine learning-supported detection for improved intrusion detection and secure routing. The selected baseline techniques have been convincingly justified in relation to a number of recently proposed trust-based and secure IoT–WSN schemes. We provide the formal definition of performance metrics and analytically discuss the factors that lead to difference in performing among approaches. These modifications are beneficial in terms of methodological transparency and clearly illustrate how combining dynamic trust evaluation, ECC-based authentication and intelligent classification improves the malicious node detection probability and secure communication for IoT-based WSN.

The simulation is built on a network of 30 nodes, as seen in Fig. 3. The Fig. 4 shows the device registration along with the nodes in the network. We employ an administrator to monitor the network for potential threats. MATLAB 2024b was used to perform the simulation. In this section, machine learning-based solutions can be used to identify harmful behaviour, enhance security, and utilize symmetric-core protocols and ECC encryption for device authentication. The source routing node of the region gets information about the selected route from the public node and adds it to its source routing header to execute the route request. Transmitting data packets does not require a direct connection to the source routing node, since relay paths match source paths in the packet headers. This method efficiently reduces the system's energy consumption. The overall configuration of the zone is determined by energy efficiency between the source routing node and the public node. Energy efficiency determines which resource node locations are better suited to the public domain, thereby prolonging the network's lifespan. It is possible to create zones by controlling communication between the public node and the source-routing node by distributing route request packets (RREQ) to other nodes from a source node as shown in Fig. 5.

Request path packets are used to convey many messages in a network, since they are forwarded from a source node to a destination node. A source transport package includes a default record field that contains every path from the source to the destination. The source data transmission feature of the data packet enables the network address to be included at an intermediary hop between the source and target nodes as the packet moves from the target to the source (RREP). When a point is inadvertently introduced into the network and placed at the centre of the data stream, between two sensors and a router node, a route is generated. Source nodes can use the path to transmit data packets to destinations.

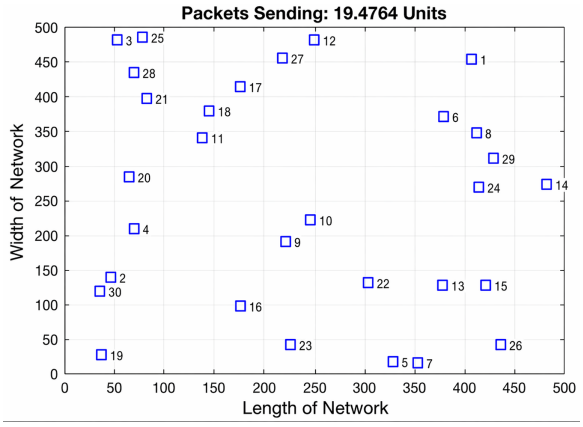

Figure 3: Initializing the network.

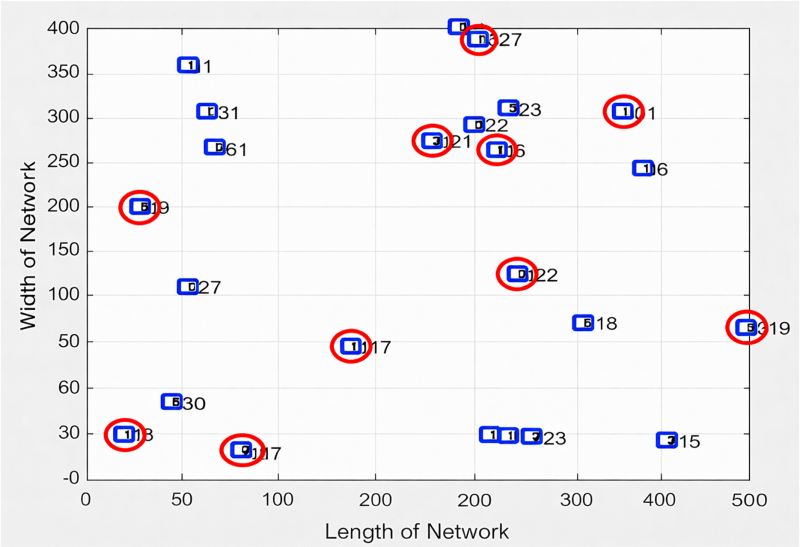

Figure 4: Device registration.

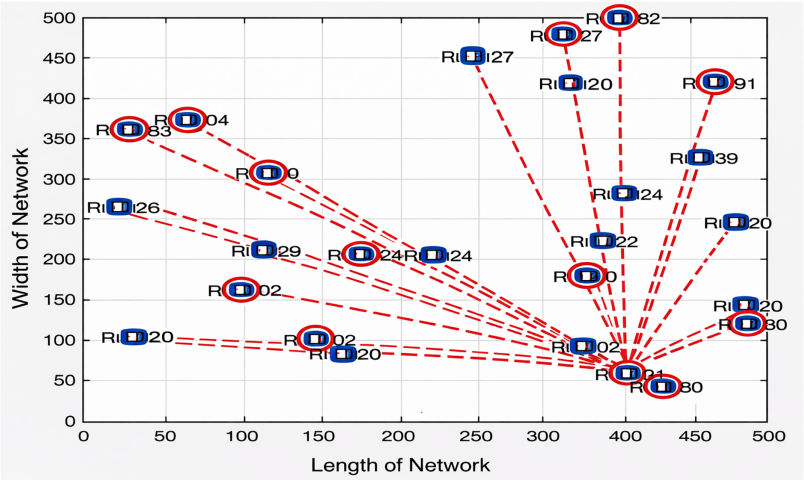

Figure 5: A source node broadcasts a route request packet (RREQ) to other nodes in the network.

Ultimately, the malicious node blocks its path and creates an incorrect neighbour by sending the designated data packet to the intended destination node. The changed application data must then be located and inserted into the target node by capturing the data packet. The package will be stored, and the capture operation will be repeated when the unclean area is unable to handle interesting traffic. The main target of MITM attacks will be data entering for other nefarious purposes between clients and servers. MITM attack, however, can employ other attacks. Therefore, we characterize MITM attackers as those who can develop an independent rapport with the target and persuade them that they are still having a personal conversation as shown in Fig. 6. Attackers can transmit, block, or inject new packets of data. MITM attacks primarily target the interception and exfiltration of data to enable other malicious operations between clients and servers. The MITM attacks occur very frequently. As a result, the MITM attacker can build a rapport with the target and persuade them that they are still having a personal chat. Attackers can transmit, block, or inject new packets as indicating in the Fig. 7.

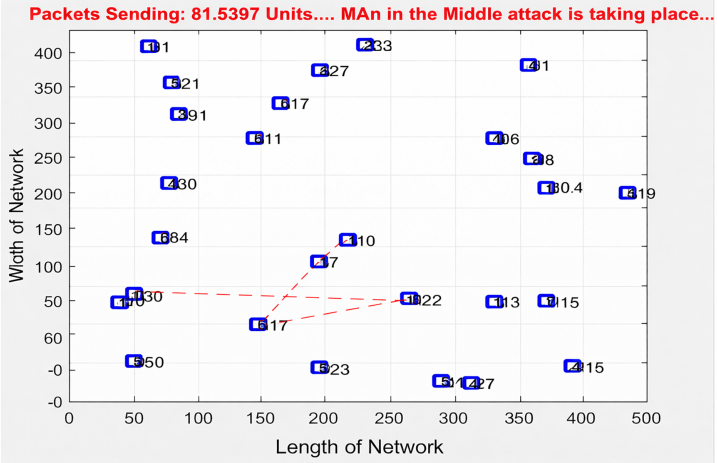

Figure 6: MITM attack in the network.

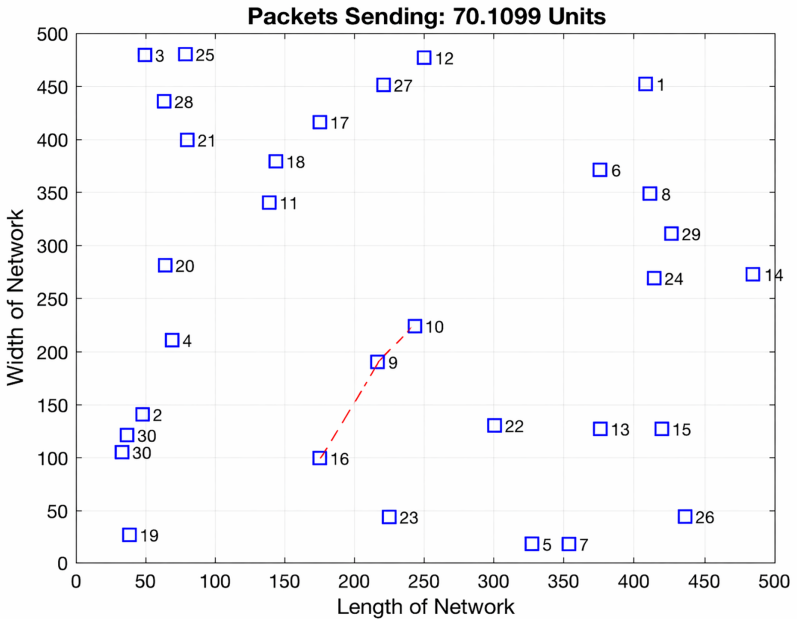

Figure 7: Searching path and rerouting.

Elliptic Curve Cryptography is a type of public-key cryptography. The user or device connected to the connection usually has two keys—public and private—as well as several functions associated with them for performing encryption operations. The Fig. 8 shows the encoded message bits using ECC algorithm. When data is erased and locked in a symmetric account using a common shared key, secure key communication becomes a serious problem. Since it's not always possible to share keys, the private key is known only to the private users, while everyone connected to the link has access to the public key.

As shown in Fig. 9, network latency, the time it takes data to travel across a network, is a measure of how fast data travels. The time elapsed during the communication's journey to and from its destination is typically used to determine its duration. With the data frame on the x-axis and the amount of data per second on the y-axis, Fig. 10 displays the number of attacks per second for each data frame.

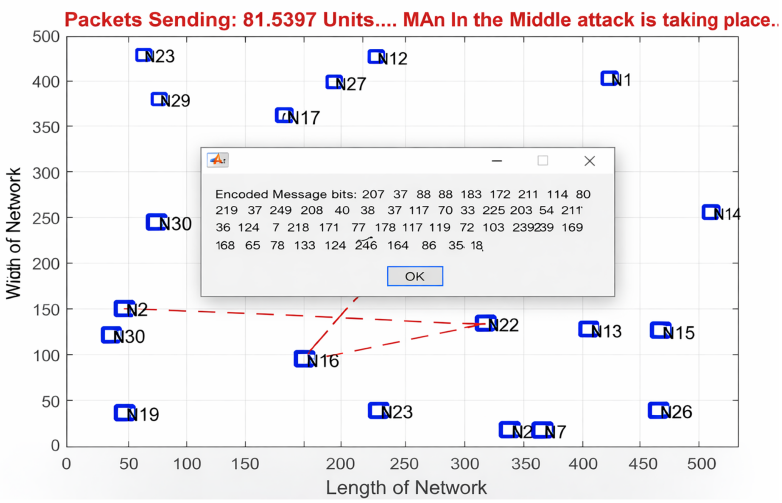

Figure 8: Message bits for an elliptic curve cryptography (ECC).

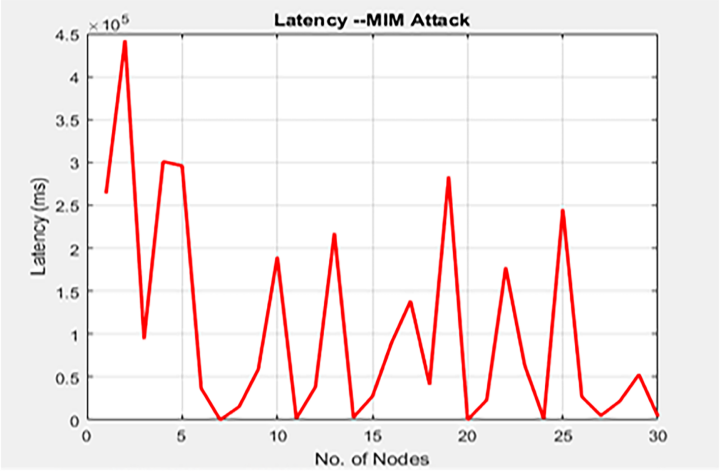

Figure 9: Latency MITM attack.

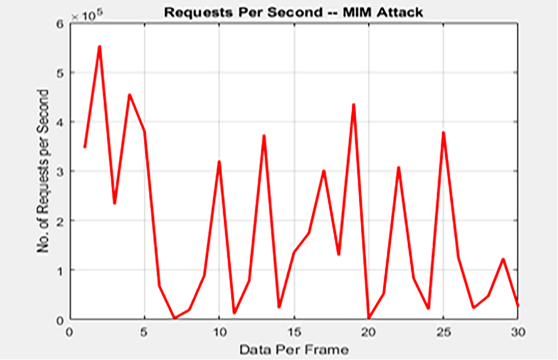

Figure 10: MITM attack requests per second.

Fig. 11 shows energy consumption during an MITM attack in a wireless network, where data transmission consumes the majority of energy. An energy measurement is shown on the y-axis, along with the number of nodes involved in packet transmission. In Fig. 12, the total number of packets that must be sent from one node to another is shown as the overhead. It covers the overhead associated with a sensor node's packet preparation, routing table, and routing execution. As shown in the graph, the x-axis represents nodes, and the y-axis represents overhead.

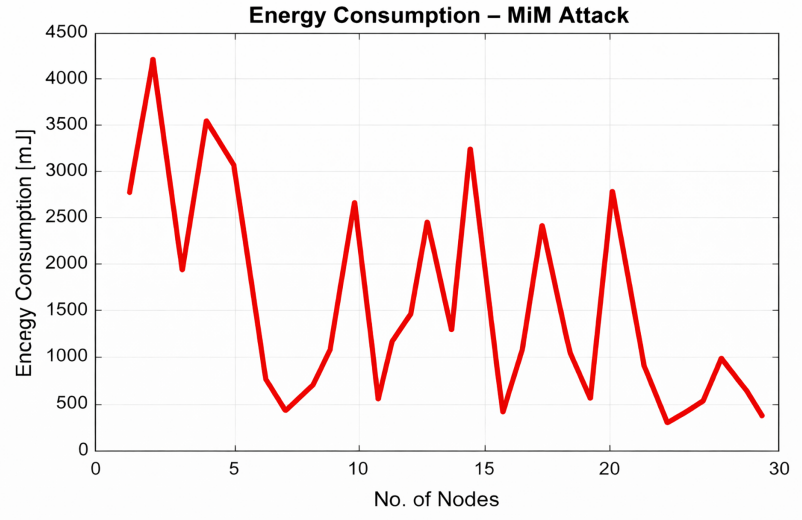

Figure 11: Energy usage during the MITM attack.

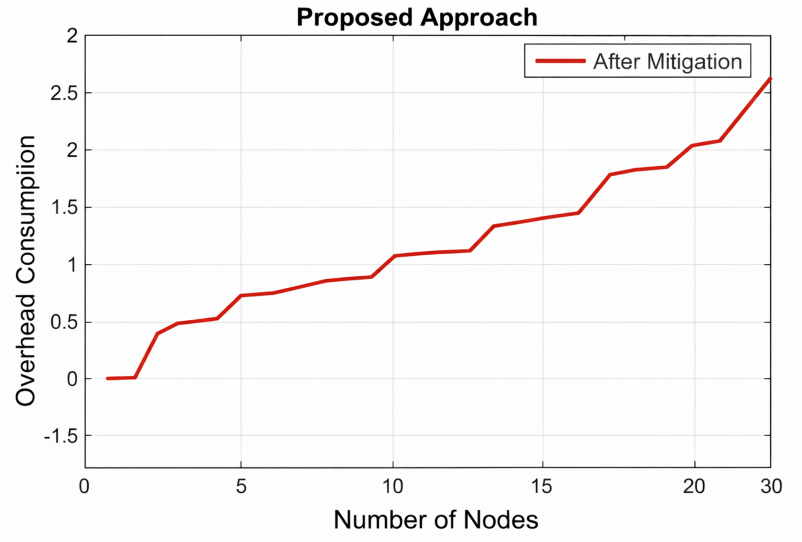

Figure 12: Overhead consumption.

When a sender sends a message to a recipient, the first bit takes time to traverse the link in Fig. 13. Fig. 14 shows the system's energy utilisation. Because each CH is located a certain distance from each member, energy consumption increases with coverage area. The energy balance depends on the equipment's energy

consumption and the wireless sensor network's transmission power. Fig. 14 illustrates the relationship between energy usage and nodes on the *y*-axis.

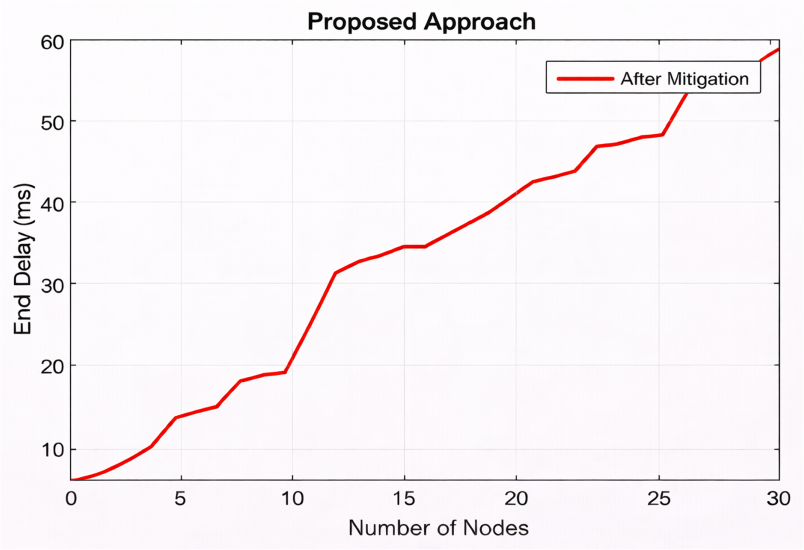

Figure 13: End delay.

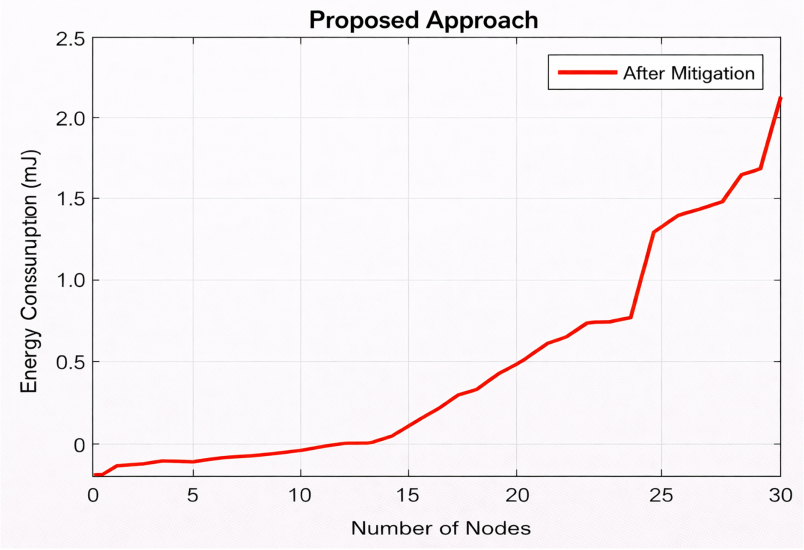

Figure 14: Energy consumption.

Fig. 15 presents the scalability analysis of the proposed DTEM framework by increasing the number of sensor nodes from 25 to 150. The detection accuracy at the baseline configuration of 30 nodes is 86%, which represents the primary experimental setup used in the proposed model. As the network size increases, a slight decrease in detection accuracy can be observed due to increased communication interactions, routing complexity, and trust computation overhead among a larger number of nodes. However, the decrease remains minimal, and the detection accuracy remains above 84% even at 150 nodes. This indicates that the proposed DTEM framework maintains stable malicious node detection performance as the network

size grows. The distributed trust computation mechanism and lightweight ECC-based communication help maintain efficient system performance, demonstrating that the proposed model is scalable and suitable for larger IoT-based wireless sensor network deployments.

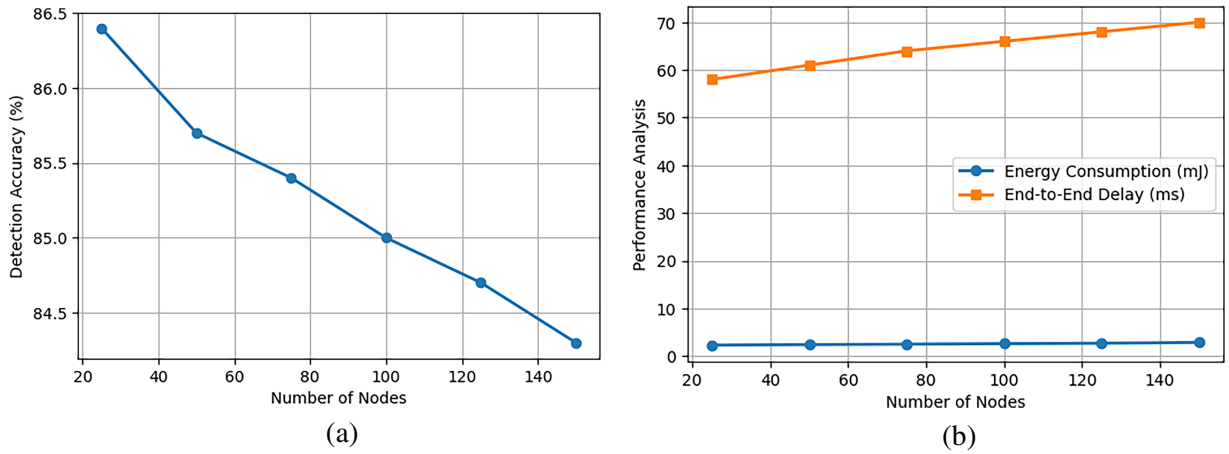

Figure 15: Network performance of the proposed DTEM model vs. number of nodes, (**a**) Detection accuracy (%) and (**b**) energy and delay.

A. Proposed Trust Model Evaluation

Different barriers or cells make up neural networks. The component stores information regarding network activity. The neural network maintains the latent state and the cell state. The three processes forget, access, and output, are handled by these two states. Surgery on these cells facilitates comprehension of the behaviour of the cell cycle and transmission of inputs aids the final cell. The MATLB nntraintool is used for data trained as shown in Fig. 16.

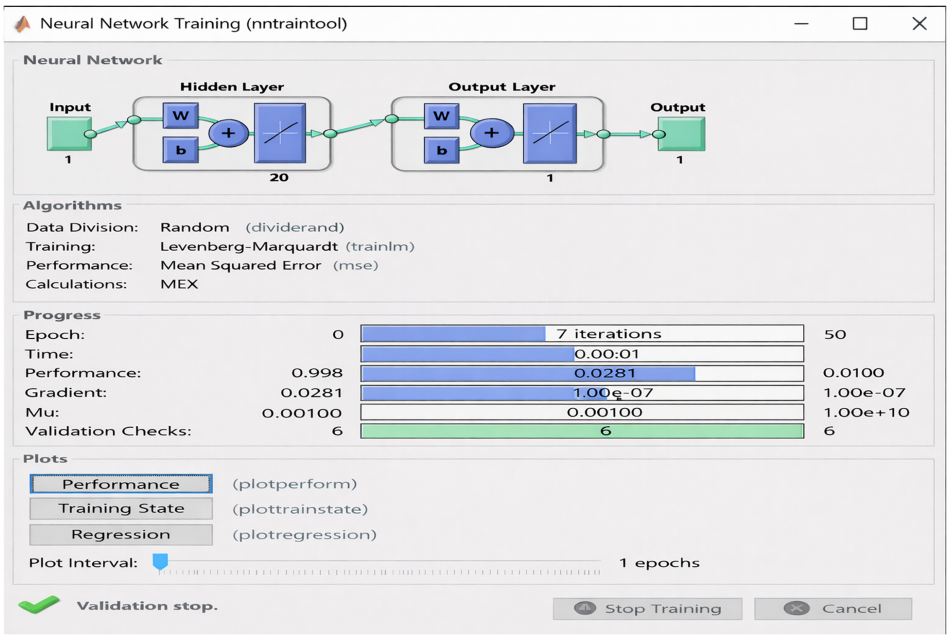

Figure 16: Neural network training.

SVM Classification: The SVM rank classifier uses local observations to establish an initial trustworthiness ranking in a ranked list. Because each node can only see its own local observations, they are then shared so that each node knows the behaviours of nodes beyond its radio range. This work makes two points. The first is to utilize a Support Vector Machine (SVM) to automatically determine how to penalize each misconduct and what each mobile node's dependability is based on context. Fig. 17 shows the classification model in the proposed trust model.

Figure 17: Proposed flow diagram of trust model.

Determining a node's trustworthiness is the goal of trust management methods. We proposed an automated management strategy that uses an SVM-based classifier to assess node trustworthiness.

The packet data rate and the time-domain packet drop rate are used to assess the reliability of neighbouring nodes. Using the Inter-Peer Trust (IPT) record and profile established and saved at each node, the module calculates the overall cumulative trust value for all nodes, including both indirect and direct trust values in Fig. 18. It includes both the time it takes for the sending node to send a packet and the time it takes for the receiving node to receive it. The network comprises several nodes, each with direct and indirect connections to the others. The direct trust of a node may be assessed by inspecting packets sent and received, the times at which they were sent and received, and the packet drop rates between nodes, whether they are the final destination or an intermediary node. Fig. 19 shows the confusion metric of trustworthy and untrustworthy data. The PS (Packet Sent) parameter counts the packets sent from the transmitter node, which could be the source or an intermediary node. The number of packets a node has received can be found by filling out the PR (Packet Received) section. The time it takes a transmitter node to transport or forward a packet to its intended destination is known as TPS (Time of Packet Send). When a receiving node receives a packet from a sending node, the TPR (Time of Packet Received) event occurs. The Packet Drop Rate (PDR) is the proportion of packets lost during transmission from a transmitter to a receiver, i.e., (Packet Data Rate). The number of packets transferred between two nodes on the same network over time.

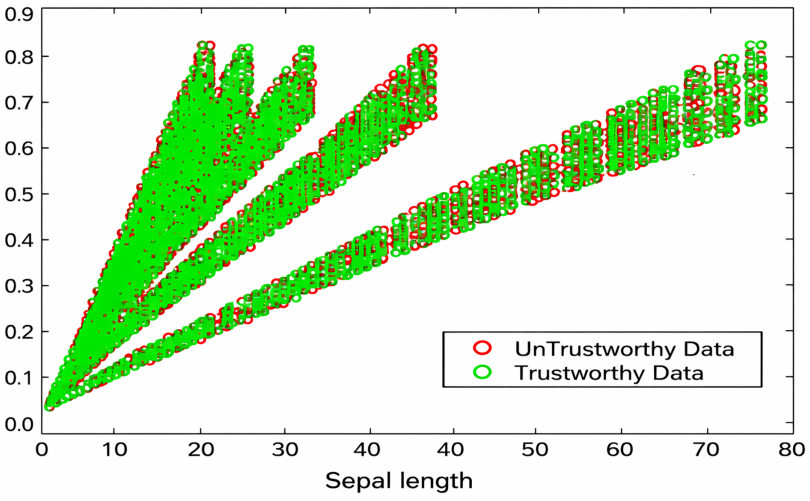

Figure 18: Classified untrustworthy and trustworthy data.

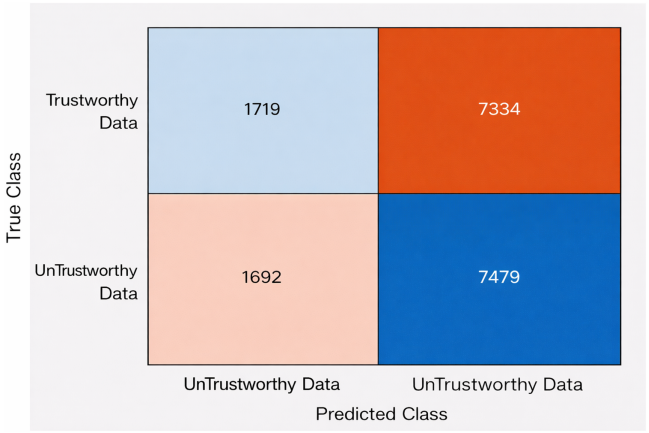

Figure 19: Predicted class of data.

The network's longevity influences. The time it takes for a node to run out of energy and stop the functioning is called the deadlock time. The Figs. 20 and 21 show the level of trustworthy and untrustworthy data vs. number of iteration. The error of choice the untrustworthy and trustworthy data with respect to the number of iteration is presented in the Fig. 22.

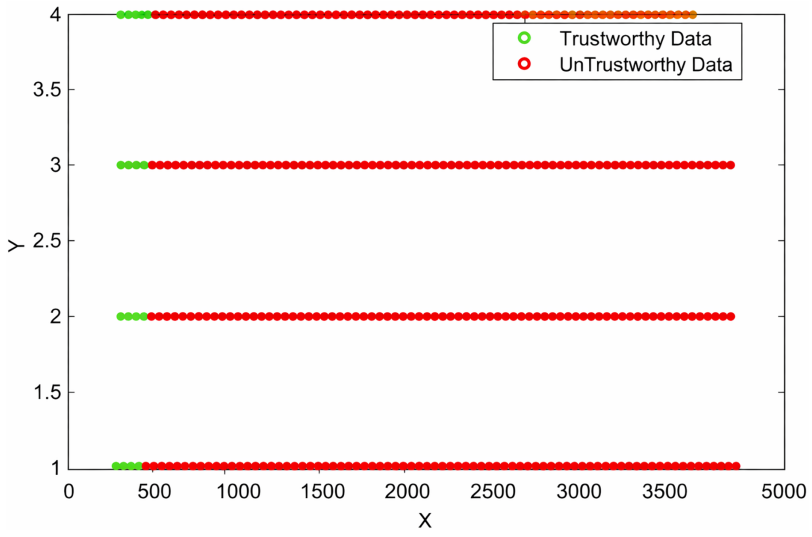

Figure 20: Level of untrustworthy and trustworthy.

B. Performance Evaluation

The CTBET mechanism's performance will be evaluated based on trustworthiness, detection accuracy and false-positive rate, average throughput, residual energy, and end-to-end delay. Examine how these stats are calculated. When analysing the recommended approach, the simulator considers the following performance factors. The degree of trustworthiness has an effect: Following the implementation of the proposed technique, this statistic displays the proportion of harmful nodes accurately recognised and the percentage of selfish nodes mistakenly reported or created.

Impact of Detection Rate: Instead of a percentage, this measure displays the proportion of malicious nodes discovered after using the suggested approach.

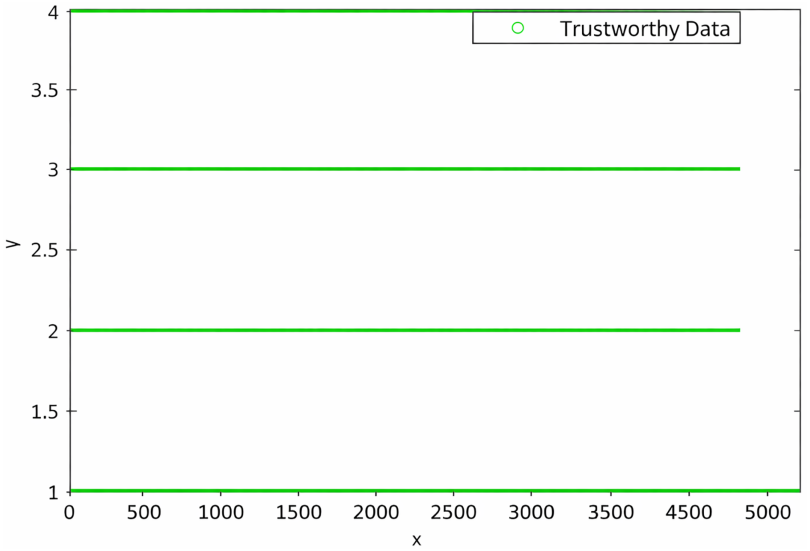

Figure 21: Level of trustworthy data.

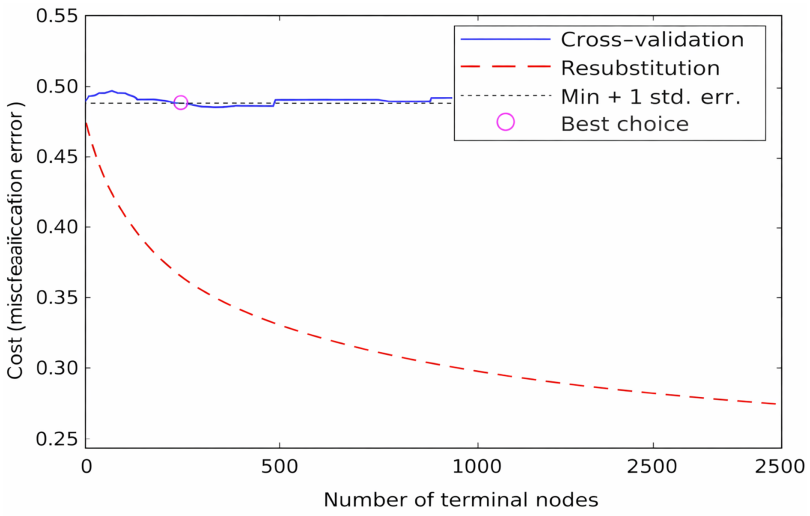

Figure 22: Level of untrustworthy and trustworthy data.

Impact of Detection Accuracy: After implementing the stated technique, this value shows the percentage of malicious nodes detected. The lowest number of false positive referrals is used to determine this ranking.

Detection of False Positives: Researchers can check the false-positive rate of various internal attacks using this option. To calculate the metric, divide the total number of false positives by the total number of false negatives.

Table 2 compares Energy consumption, End delay, Overhead consumption, Latency, and Number of requests per second.

Table 2: Comparison table.

Method	Energy Consumption M/J	End Delay (M/S)	Overhead Consumption	Latency	No. of Requests Per Second
With MITM Attack	6.5	80	3.5	6.5	5.5
After Mitigation	2.2	60	2.5	2.1	3.5

Although elliptic curve cryptography (ECC) is considered a lightweight public key cryptographic mechanism, it still introduces additional computational and communication overhead compared to non-secure communication. To analyse its impact, we evaluated the energy consumption and communication overhead associated with ECC-based authentication and secure key exchange in the proposed DTEM framework. ECC operations primarily occur during node registration, key generation, and authentication phases rather than during continuous packet transmission. Therefore, the overhead remains limited and does not significantly affect overall network performance. The ECC provides strong cryptographic security with 160–256 bits key sizes, which significantly reduces computational complexity and communication overhead. This makes ECC more suitable for resource-constrained IoT-based wireless sensor networks where energy efficiency and lightweight operations are essential.

The performance analysis shows that the trust evaluation module forms the core mechanism for malicious node detection in the proposed DTEM framework as shown in Table 3. Incorporating ECC-based secure communication improves system resilience against message manipulation and trust data tampering while reducing communication overhead. Furthermore, integrating machine learning classification enhances detection accuracy by analysing behavioural patterns that may not be captured through trust computation alone. Although the experimental evaluation focuses on the MITM attack scenario, the dynamic trust evaluation mechanism monitors node behaviour parameters such as packet forwarding reliability, packet drop rate, and interaction history, enabling the framework to identify other internal attacks including collusion, coordinated malicious behaviour, and selective forwarding. The MITM attack was selected as the primary evaluation scenario because it represents a common and critical security threat in IoT-based wireless sensor network communication.

Table 3: Performance analysis of DTEM.

Technique	Detection Accuracy (%)	Energy Consumption (mJ)	Communication Overhead
CTBET	61	–	–
SVM-based Detection	82	–	–
Trust Evaluation Only	74	3.8	3.1
Trust + ECC	78	3.2	2.8
Proposed DTEM (Trust + ECC + ML)	86	2.2	2.5

5 Conclusion

The study reveals several critical research directions for AI-based trust evaluation in its early stages. These avenues include exploring fine-grained trust assessment integrating subjectivity and dynamic aspects, aiming to align AI methodologies with conventional trust evaluation to achieve more realistic and nuanced

outcomes. Additionally, customising feature selection and estimation techniques using AI to enhance the efficacy and universality of trust appraisal methods is emphasised. Ensuring reliable, labelled data for supervised learning in trust assessment remains a significant challenge, underscoring the need for research on ethical labelling processes. Moreover, enhancing the security of AI-based trust evaluation against potential attacks by leveraging emerging technologies such as federated learning and differential security is proposed. Furthermore, adaptable trust evaluation frameworks that balance computational efficiency and real-world feasibility are suggested, with a focus on model adaptation and integration across diverse domains. Experimentation with various AI techniques, such as reinforcement learning, unsupervised learning, and semi-supervised learning, for trust evaluation is recommended, as each offers distinct advantages. Lastly, integrating AI methodologies with emerging technologies such as data fusion and association analysis could significantly improve trust evaluation by efficiently utilising diverse data sources and addressing zero data and cold start challenges to achieve more accurate assessments.

In edge computing-based IoT networks, distinguishing between genuine and malicious nodes is crucial to minimise data loss and network disruptions. While cryptography and authentication methods offer some security, they often fail to detect hostile nodes. Existing security approaches lack continuous re-evaluation, allowing malicious nodes to exploit vulnerabilities over time. To address this, a more robust strategy is needed to identify rogue nodes. Assessing node trustworthiness through direct and indirect trust evaluation becomes vital in detecting and mitigating the impact of malicious nodes, ensuring reliable data transfer and network integrity. Future work may extend the evaluation to include additional attack scenarios such as collusion attacks and coordinated multi-node attacks to further analyse the robustness of the proposed framework under more complex adversarial environments.

Acknowledgement: Not applicable.

Funding Statement: The authors received no specific funding for this study.

Author Contributions: Conceptualization: Anil Kumar, Abhay Bhatia, Amit Singh, Preeti Rani, Vincent Omollo Nyangaresi, Mahendihasan S. Heera. Software and Data Processing: Anil Kumar, Abhay Bhatia, Amit Singh, Preeti Rani. Writing—Original Draft: Anil Kumar, Abhay Bhatia, Preeti Rani. Writing—Review & Editing: Anil Kumar, Abhay Bhatia, Amit Singh, Preeti Rani, Vincent Omollo Nyangaresi. Heera. Supervision: Anil Kumar, Abhay Bhatia, Amit Singh, Preeti Rani, Vincent Omollo Nyangaresi, Mahendihasan S. Heera. All authors reviewed and approved the final version of the manuscript.

Availability of Data and Materials: Not applicable.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Kumar N, Rani P, Kumar V, Athawale SV, Koundal D. THWSN: enhanced energy-efficient clustering approach for three-tier heterogeneous wireless sensor networks. IEEE Sens J. 2022;22(20):20053–62. doi:10.1109/JSEN.2022.3200597.
2. Bansal H, Kohli S. Trust evaluation of websites: a comprehensive study. Int J Adv Intell Paradigms. 2019;13(1–2):101. doi:10.1504/ijaip.2019.099946.
3. Chen X, Yuan Y, Lu L, Yang J. A multidimensional trust evaluation framework for online social networks based on machine learning. IEEE Access. 2019;7:175499–513. doi:10.1109/ACCESS.2019.2957779.
4. Chen X, Yuan Y, Ali Orgun M. Using Bayesian networks with hidden variables for identifying trustworthy users in social networks. J Inf Sci. 2020;46(5):600–15. doi:10.1177/0165551519857590.

5. Feng R, Xu X, Zhou X, Wan J. A trust evaluation algorithm for wireless sensor networks based on node behaviors and D-S evidence theory. Sensors. 2011;11(2):1345–60. doi:10.3390/s110201345.
6. Li W, Song H. ART: an attack-resistant trust management scheme for securing vehicular *ad hoc* networks. IEEE Trans Intell Transp Syst. 2016;17(4):960–9. doi:10.1109/TITS.2015.2494017.
7. Khalid O, Khan SU, Madani SA, Hayat K, Khan MI, Min-Allah N, et al. Comparative study of trust and reputation systems for wireless sensor networks. Security Comm Networks. 2013;6(6):669–88. doi:10.1002/sec.597.
8. Singh A, Rani P, Venkata Naga Ramesh J, Athawale SV, Hussein Alkhayyat A, Aledaily AN, et al. Blockchain-based lightweight authentication protocol for next-generation trustworthy Internet of vehicles communication. IEEE Trans Consumer Electron. 2024;70(2):4898–907. doi:10.1109/tce.2024.3351221.
9. Pundir S, Wazid M, Singh DP, Das AK, Rodrigues JJPC, Park Y. Intrusion detection protocols in wireless sensor networks integrated to Internet of Things deployment: survey and future challenges. IEEE Access. 2020;8:3343–63. doi:10.1109/ACCESS.2019.2962829.
10. El-Sayed H, Ignatious HA, Kulkarni P, Bouktif S. Machine learning based trust management framework for vehicular networks. Veh Commun. 2020;25(6):100256. doi:10.1016/j.vehcom.2020.100256.
11. Guo J, Chen IR, Tsai JJP. A survey of trust computation models for service management in Internet of Things systems. Comput Commun. 2017;97:1–14. doi:10.1016/j.comcom.2016.10.012.
12. Hao F, Min G, Lin M, Luo C, Yang LT. MobiFuzzyTrust: an efficient fuzzy trust inference mechanism in mobile social networks. IEEE Trans Parallel Distrib Syst. 2014;25(11):2944–55. doi:10.1109/TPDS.2013.309.
13. Ullah F, Salam A, Amin F, Khan IA, Ahmed J, Zaib SA, et al. Deep trust: a novel framework for dynamic trust and reputation management in the Internet of Things (IoT)-based networks. IEEE Access. 2024;12:87407–19. doi:10.1109/ACCESS.2024.3409273.
14. Bahutair M, Bouguettaya A. An end-to-end trust management framework for crowdsourced iot services. ACM Trans Internet Technol. 2023;23(3):1–32. doi:10.1145/3600232.
15. Li X, Zhou F, Du J. LDTS: a lightweight and dependable trust system for clustered wireless sensor networks. IEEE Trans Inf Forensics Secur. 2013;8(6):924–35. doi:10.1109/TIFS.2013.2240299.
16. Zahariadis T, Leligou HC, Trakadas P, Voliotis S. Trust management in wireless sensor networks. Eur Trans Telecommun. 2010;21(4):386–95. doi:10.1002/ett.1413.
17. Yu Y, Li K, Zhou W, Li P. Trust mechanisms in wireless sensor networks: attack analysis and countermeasures. J Netw Comput Appl. 2012;35(3):867–80. doi:10.1016/j.jnca.2011.03.005.
18. Jiang J, Han G, Wang F, Shu L, Guizani M. An efficient distributed trust model for wireless sensor networks. IEEE Trans Parallel Distrib Syst. 2015;26(5):1228–37. doi:10.1109/TPDS.2014.2320505.
19. Han G, Jiang J, Shu L, Niu J, Chao HC. Management and applications of trust in wireless sensor networks: a survey. J Comput Syst Sci. 2014;80(3):602–17. doi:10.1016/j.jcss.2013.06.014.
20. Raoof A, Matrawy A, Lung CH. Routing attacks and mitigation methods for RPL-based Internet of Things. IEEE Commun Surv Tutor. 2019;21(2):1582–606. doi:10.1109/COMST.2018.2885894.
21. Bhola B, Kumar R, Rani P, Sharma R, Abed Mohammed M, Yadav K, et al. Quality-enabled decentralized dynamic IoT platform with scalable resources integration. IET Commun. 2025;19(1):e12514. doi:10.1049/cmu2.12514.
22. Shala B, Trick U, Lehmann A, Ghita B, Shiaeles S. Blockchain and trust for secure, end-user-based and decentralized IoT service provision. IEEE Access. 2020;8:119961–79. doi:10.1109/ACCESS.2020.3005541.
23. Nayak P, Devulapalli A. A fuzzy logic-based clustering algorithm for WSN to extend the network lifetime. IEEE Sens J. 2016;16(1):137–44. doi:10.1109/JSEN.2015.2472970.
24. Ahmad F, Adnane A, Kurugollu F, Hussain R. A comparative analysis of trust models for safety applications in IoT-enabled vehicular networks. In: 2019 Wireless Days (WD); 2019 Apr 24–26; Manchester, UK. p. 1–8. doi:10.1109/wd.2019.8734204.
25. Shaikh RA, Jameel H, d'Auriol BJ, Lee H, Lee S, Song YJ. Group-based trust management scheme for clustered wireless sensor networks. IEEE Trans Parallel Distrib Syst. 2009;20(11):1698–712. doi:10.1109/tpds.2008.258.
26. Goswami P, Khan T, Pathak V, Alabdultif A. Machine learning based dynamic trust estimation framework for Securing wireless sensor networks. Sci Rep. 2025;15(1):35821. doi:10.1038/s41598-025-19768-z.

27. Anwer RW, Abrar M, Salam A, Ullah F. TEAD: trust-enhanced anomaly detection framework for intrusion detection in IoT-enabled wireless sensor networks (WSNs). Wirel Netw. 2025;31(6):4179–97. doi:10.1007/s11276-025-03987-3.
28. Alshudukhi KS, Humayun M, Alsalem AO, Khan MF, Haseeb K. Edge driven trust aware threat detection for IoT enabled intelligent transportation systems. Sensors. 2026;26(4):1108. doi:10.3390/s26041108.
29. Alotaibi J. Energy-efficient trust management for secure IoT devices in information-centric wireless sensor networks. Peer Peer Netw Appl. 2026;19(2):43. doi:10.1007/s12083-025-02194-3.
30. Kumar A, Budhiraja I, Garg D, Garg S, Choi BJ, Alrashoud M. Advanced network security with an integrated trust-based intrusion detection system for routing protocol. Alex Eng J. 2025;120:378–90. doi:10.1016/j.aej.2025.01.087.
31. Selvarajan S, Manoharan H, Khadidos AO, Khadidos AO. Testing of emerging wireless sensor networks using radar signals with machine learning algorithms. IEEE J Sel Areas Sens. 2024;1:49–59. doi:10.1109/JSAS.2024.3395578.
32. Ishmanov F, Kim S, Nam S. A robust trust establishment scheme for wireless sensor networks. Sensors. 2015;15(3):7040–61. doi:10.3390/s150307040.
33. Zhang J, Shankaran R, Mehmet AO, Varadharajan V, Sattar A. A trust management architecture for hierarchical wireless sensor networks. In: IEEE Local Computer Network Conference; 2010 Oct 10—14; Denver, CO, USA. p. 264–7. doi:10.1109/LCN.2010.5735718.
34. Talbi S, Koudil M, Bouabdallah A, Benatchba K. Adaptive and dual data-communication trust scheme for clustered wireless sensor networks. Telecommun Syst. 2017;65(4):605–19. doi:10.1007/s11235-016-0254-3.
35. Alsaedi N, Hashim F, Sali A, Rokhani FZ. Detecting sybil attacks in clustered wireless sensor networks based on energy trust system (ETS). Comput Commun. 2017;110:75–82. doi:10.1016/j.comcom.2017.05.006.
36. Reddy VB, Negi A, Venkataraman S. Trust computation model using hysteresis curve for wireless sensor networks. In: 2018 IEEE SENSORS; 2018 Oct 28–31; New Delhi, India. p. 1–4. doi:10.1109/ICSENS.2018.8589697.
37. Zhang W, Zhu S, Tang J, Xiong N. A novel trust management scheme based on Dempster-Shafer evidence theory for malicious nodes detection in wireless sensor networks. J Supercomput. 2018;74(4):1779–801. doi:10.1007/s11227-017-2150-3.
38. Feng R, Han X, Liu Q, Yu N. A credible Bayesian-based trust management scheme for wireless sensor networks. Int J Distrib Sens Netw. 2015;11(11):678926. doi:10.1155/2015/678926.
39. Singh M, Sardar AR, Majumder K, Sarkar SK. A lightweight trust mechanism and overhead analysis for clustered WSN. IETE J Res. 2017;63(3):297–308. doi:10.1080/03772063.2017.1284613.
40. Freedman D. Statistical models: theory and practice. Cambridge, UK: Cambridge University Press; 2009.