Enhancing trust and privacy in iot ecosystems with the distributed trust and privacy consensus framework

Sushma Priyadarashini[1], Anuradha[2]
[1]Department of Computer Science and Engineering, CMR Engineering College, Telangana, India
[2]Department of Computer Science and Engineering, PDA college of Engineering, Gulbarga, India

Article Info

Article history:

Received May 25, 2024
Revised Apr 17, 2025
Accepted Jul 3, 2025

Keywords:

Data aggregation
DTPCF
IoT
Privacy
Wireless sensor network

ABSTRACT

In the contemporary digital landscape, the proliferation of wireless sensor networks (WSNs) and the internet of things (IoT) has revolutionized the way we interact with the physical world, offering unprecedented opportunities for automation and data-driven decision-making. However, this rapid expansion has also introduced significant challenges in terms of ensuring network security, maintaining user privacy, and establishing trust among devices. To address these critical issues, this paper introduces the distributed trust and privacy consensus framework (DTPCF), a novel methodology designed to strengthen trust and privacy within IoT ecosystems through a consensus-based approach. The DTPCF pioneers a distributed mechanism for trust management that evaluates and establishes the reliability of nodes democratically and transparently, thereby enhancing the robustness and scalability of IoT systems against malicious activities. Moreover, the framework integrates privacy preservation directly into the consensus process, employing state-of-the-art cryptographic techniques and protocols to protect sensitive data during transmission and decision-making phases. Through empirical analysis, the efficacy of the DTPCF is validated across various operational scenarios, demonstrating its effectiveness in enhancing network security, privacy, and trust. Performance metrics such as throughput, energy consumption, and node-level security are meticulously evaluated, providing comprehensive insights into the framework's capabilities and potential for real-world implementation.

Corresponding Author:

Sushma Priyadashini
Department of Computer Science and Engineering, CMR Engineering College
Telangana, India
Email: Sushma_priyadarashini@rediffmail.com

1. INTRODUCTION

These days, wireless sensor networks (WSN), or WSNs, are setting the standard for communication systems. They are used in many different sectors, smart home automation, environmental monitoring, and other areas as well. This technology has a large potential for real-time applications, which is mostly due to its small size, cheap cost, and straightforward implementation [1], [2]. The deployment conditions of wireless sensor networks (WSNs) might lead to variations in their designs. In the network architecture of energy-free applications, such as home and industrial automation, the delivery packets are essential. But in dangerous situations like mines, where batteries cannot be replaced or recharged, the primary goal of network design is to make sure the network lasts longer. Nonetheless, one of the most important aspects of the WSN architecture is the size of the distributed zone. Packets are sent straight from the sensory nodes to the base station or sink nodes in smaller areas. Nonetheless, in more expansive regions, packets traverse several intermediary nodes before arriving at the sink nodes [3]. Because of its many advantages, IoT-enabled devices have drawn the interest of a wide spectrum of technologists. Among these advantages is the capacity to link different "things" under one network, allowing for effective data exchange and communication [4], [5]. In the short term, internet of things (IoT) systems have a big influence on a lot of different industries, such as manufacturing, logistics, transportation, and healthcare. The sectors indicated above are critical in supplying the necessary infrastructure for the IoT [6]. Internet connectivity connects most of the intelligent control nodes in IoT technologies. The previously stated nodes serve as transmitters or sensors and can collect data from other systems and process it on their own. Numerous IoT applications have been used in the transportation, medical, and industrial management sectors, among other domains, as a result of the growing prevalence of the IoT [1, 2, and 3]. The goal of these apps is to raise the effectiveness and quality of the system. IoT technology is centered on addressing a variety of duties to fulfill the goals established by intelligent services. Because of their cognitive operations, the devices can interact with the actual world and provide clients with the services they need at any time and wherever. Figure 1 shows the integrated architecture of the wireless sensor network-internet of things (WSN-IoT). Several modules make up this design.

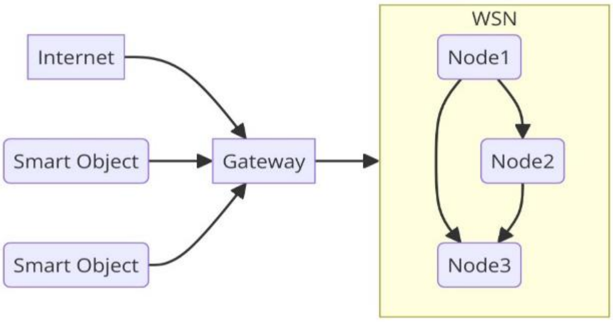

Figure 1. WSN and IoT Integration working

For effective transmission across the gateway, the wireless network system (WNS) acts as the core hub connecting various sensor networks. The other two blocks are smart devices made to send information to specific people. Several applications for heterogeneous devices and privacy threats provide difficulties in terms of recognition, access, and mitigation as a result of the growing complexity of design. On the other hand, a substantial amount of data is generated by the IoT devices' quickly increasing complexity. The regular exchange of private and sensitive data across networks has sparked worries about security and privacy in the core architecture of the internet of things [7]. Vulnerabilities in cyber systems may result in the possible compromise of large volumes of sensitive data, hence posing dangers to data integrity and privacy.

Significant technological improvements have led to a remarkable rise in both the number and type of assaults. Attackers frequently make use of the IoT intrinsic unpredictability to mishandle user confidence and control user behavior. They intend to mislead customers by raising questions about the validity of the sensors and the services they offer. In addition, serious problems with reliability, secrecy, and transparency make it difficult to deploy IoT effectively. These problems result from resource limitations as well as the diversity and complexity of IoT systems [5]. The approach of trust evaluation is employed to find instances of dishonest behavior by identifying and isolating untrustworthy objects. It also removes all chance of ambiguity and minimizes potential hazards while taking any action. By putting this solution into practice, unplanned events and service interruptions may be successfully reduced, allowing IoT devices to operate in a regulated setting. It is quite improbable that IoT systems would be deployed without a solid security framework. This technique ought to limit the influence of potentially dangerous models or at the very least prevent them from being created [6], [7]. Technologies for authentication and encryption are used in the realm of IoT security. Various security issues related to the internet of things may be efficiently addressed by using strong authentication and encryption solutions. Secure message transmission techniques between nodes, such as encryption and authentication, provide the first line of protection against external attacks [8], [9]. It is not possible for the defense mechanisms in place today to cope with insider threats or hostile network nodes. They can, nonetheless, recognize and stop outside assaults. Malicious insiders can successfully get around these security measures by obtaining the shared key and carrying out several attacks on the IoT network. To reduce internal attacks in the context of the IoT, trust must be established first. The issue of personal privacy has grown more subtle as information technology has developed. As a result, over time, there has been an increasing emphasis on creating techniques to protect privacy. However, several elements, including latency, location awareness, real-time communication and data interchange, and quality of service (QoS), have all decreased with the increasing use of edge computing and fog paradigms for IoT critical data [10], [11]. It has been established that IoT devices utilized for edge computing and storing private data are vulnerable to privacy issues [12]. The current methodology incorporates both conventional and cutting-edge deep learning algorithms and suggests many strategies [13] to guarantee anonymity. For crucial information solutions, the existing fog/edge computing-based deep learning algorithms require costly processing.

In the rapidly evolving landscape of WSNs and the IoT, this paper endeavors to address the forefront of innovation and security in these critical technologies. As WSNs become increasingly integral across diverse sectors such as smart home automation, environmental monitoring, and industrial management, the imperative for robust, real-time applications is unequivocally clear. The allure of WSNs and IoT devices lies in their compact size, cost-effectiveness, and straightforward deployment, promising an expansive horizon of possibilities for future applications. This work delves deep into the architectural intricacies and deployment challenges inherent in WSNs, highlighting the crucial role of energy-efficient design and the necessity for enduring network longevity in adverse conditions. Furthermore, it underscores the paramount importance of security and privacy within the IoT ecosystem, where the confluence of technological advancement and connectivity brings forth complex privacy issues and security vulnerabilities. Amid the increasing complexity and growing threats, this paper emerges as a cornerstone of innovation, proposing cutting-edge mechanisms for trust evaluation and privacy preservation. By advancing a comprehensive framework that ensures the integrity and reliability of IoT systems, this research not only contributes significantly to the academic discourse but also lays the groundwork for practical implementations that enhance system efficiency, safeguard data privacy, and fortify network security.

- Pioneering a distributed framework for trust management: the distributed trust and privacy consensus framework (DTPCF) introduces a novel distributed approach to trust management within WSNs and the IoT ecosystems. This framework employs a consensus mechanism for evaluating and establishing trust among nodes, effectively mitigating the risks associated with malicious or compromised devices.
- Integrating privacy preservation at the consensus level: a key innovation of the DTPCF is its unique integration of privacy-preserving mechanisms directly into the consensus process. This integration ensures that sensitive information is protected throughout the data exchange and decision-making processes, addressing one of the critical challenges in IoT environments.
- Framework efficacy: through rigorous empirical analysis, the DTPCF has been tested and validated under various operational scenarios and threat models. This contribution not only demonstrates the framework's effectiveness in enhancing trust and privacy within WSNs and IoT systems but also provides valuable insights into its performance metrics, such as throughput, energy consumption, and node-level security.

2. RELATED WORK

Zawaideh *et al.* [14], the neighbor weight trust detection (NWTD) mechanism's methodology is altered. With this change, the issue of secretly detecting rogue nodes in WSN is intended to be addressed. Using this method, the trust value is updated in parallel, guaranteeing that the nodes' trust degree is preserved and that the minimum peak value is set within a reasonable range. This approach's primary goal is to segregate malicious nodes in WSNs through their detection. The Dempster-Shafer (D-S) evidence theory is used by the trust approach suggested in [15] to assess the reliability of the network and the validity of the data packet. This approach takes into account third-party nodes' direct and indirect trust. Yaoxin *et al.* [16] and Prabha and Latha [17], a trust model was created to control the direct and indirect levels of trust in wireless sensor networks. This model considers both the internal attacks that these networks are vulnerable to in addition to estimating the degree of trust. This system's technology makes sure that the level of trust is updated frequently, which lowers the network's energy usage. It also creates a trust standard that helps to enable more efficient decision-making procedures. To preserve network security and dependability, the system can distinguish between malicious and old nodes. The traditional method of assessing trust is assessing the system's fairness, judgment accuracy, latency of nodes, and success rate of signals. These trust-building techniques are used to lower decision-making process uncertainty. To determine the overall trust value for every node, a multi-attribute trust model was created [18]. The result's accuracy was validated. We provide a new trust management system in this part, which is based on the D-S evidence theory [19]. Using the D-S theory, the spatiotemporal correlation of data gathered by neighboring sensor nodes was analyzed to create the trust model. As a result, a determination is made concerning which nodes are deemed malevolent. A unique methodology for identifying malicious nodes in modern WSNs is proposed in the study [15].

This approach tackles the shortcomings of the present malicious node detection technique as well as the problems with the single detection function. Its goal is to stop high-reputation nodes in WSNs from doing damaging and slanderous things. This model illustrated the implicit dependability of third-party nodes that have been shown, as well as the Beta Distribution's reputation distribution. The solution includes trust levels linked to various attack techniques and ensures accurate detection of rogue nodes. Miao *et al.* [20], a method is suggested for maintaining anonymity while ascertaining the truth, although at a considerable expense to the client. Li *et al.* [21] suggests using a two-layer strategy to satisfy the need to protect user privacy. The authors' work offers a creative and effective framework for protecting privacy while carrying out truth-finding. The goal of this system, which is explained in [22], is to produce two cloud platforms that don't function together. To guarantee safe calculations, the framework also includes a homomorphic cryptosystem. A brand-new data poisoning disguise attack (DDPA) is presented in the study [23] and is intended only for use with truth-finding techniques in private crowd-sensing systems. It is advised that a stealth strategy be used, in which the evil traits are hidden to evade the discovery of truth-finding methods. To solve optimization issues at the bi-level, a structured technique is implemented in addition to a stealth approach. After that, these problems are overcome by applying a different optimization method. In the context of online location sharing, the semantic-awareness information-theoretical Privacy (SEITP) technique is a revolutionary methodology that preserves both semantic and data privacy, as explained in [24], [25]. Semantic awareness of data is employed by SEITP to guarantee complete privacy preservation.

3. PROPOSED METHOD

The methodology designed presents a complex data handling process in a sensor network, beginning with the collection and transmission of data by sensor nodes. This data is structured within a directed graph, establishing targeted connections for data transfer. The process involves consensus validation by the functioning nodes and adapts based on the specific characteristics of data sensing, indicated by the term DECANE. The flowchart emphasizes the importance of reliability, verification, and privacy throughout the system, incorporating adaptive node engagement for data validation and transmission. Security is highlighted as a crucial aspect, with a specific focus on modeling and an event-based approach for triggering actions, all while maintaining and quantifying the system's privacy integrity. Figure 2 shows the proposed workflow.

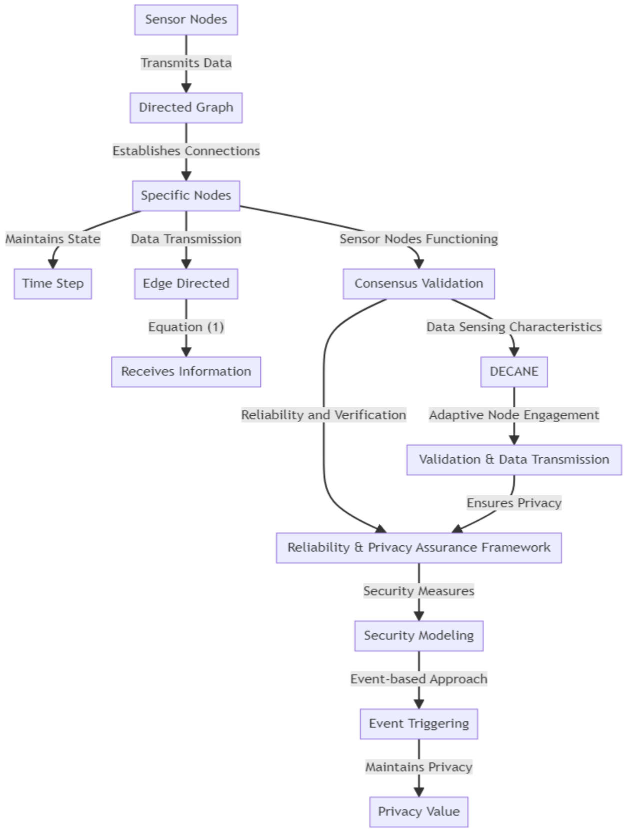

Figure 2. Proposed workflow

3.1. Problem statement

This section evaluates the mathematical formulation within the established sensor nodes within the WSN setup. Assuming the network framework $S(S \geq 2)$ which transmits data to nearby nodes, the data transmission is established via a designated directed graph. In the respective graph, $L_i = (A, J)$, where $A = [a_1, a_2, a_3, \ldots\ldots a_s]$ and s is the specific nodes with I as the edge. The time step $o \in E \geq 0$ wherein each node maintains its respective state. The edge directed between a_o and a_n is represented with the (1).

$$q_{no} \triangleq (a_o a_n) \in J \tag{1}$$

In (1) validates the sensor node a_o that receives information through c_q; this assumes the graph is implemented and connected wherein there exists a path between two distinctive nodes. However, the sensor nodes set which transmit the data to the node within the set of a_n represented by $S'_O = [a_n \in A|\ (a_o a_n) \in J]$, the nodes which act as the recipient receive the information from a_n within the parallel set represented by S''_o. The functioning of the sensor nodes within a network is discussed. By evaluating the connected graph as designed prior, each specific node consists of certain stages evaluated as $d_n[0]$, henceforth these nodes compute the equation that satisfies the criteria represented.

$$D' = s(\textstyle\sum_{q-1}^{s}\ d_q[q])^{-1} \tag{2}$$

The main goal of this work is to design a technique to ensure reliability and verification technique for nodes $a_m \in B_u/B_h$ by communicating with various other nodes. this problem is specifically designed to evaluate the D' as in equation (1). In the specified graph, data transfer is limited to nodes that are topologically parallel to each other. One potential scenario involves a particular node within set A that exhibits dishonest behavior. This node may make unauthorized attempts to gain access to the network to compromise confidentiality. Specifically, it may try to identify a specific state $d[0]$. The concealment of information by nodes and networks is commonly referred to as privacy. In line with this, the proposed model aims to safeguard privacy by concealing confidential information.

3.2. Consensus-driven sensory data validation mechanism

The proposed model is designed to consider the characteristics of data sensing in the WSN based IoT model. The model is designed to operate within a given time frame $\in D_{\geq 0}$, each node has attributes $d_o^x[p], e_o^x[n], e_o^x[p]$. However, v^x is denoted as another parameter designated for the output. It is denoted that each sensor node is aligned with parallel nodes and directly transfers the data, each node is allotted an outgoing edge r_{q_o}. Wherein $a_p \in S'_O$ which is the link (a_q, a_o) for node U_{p_o} denoted by U_{q_o}(where $\{U_{q_o}|a_q \in S'_o\} = \{0,1, \ldots\ldots, I'_o - 1\}$). The proposed framework establishes a consensus model for efficient data handling and transmission. After a specified number of steps, it produces v^x which represents the node's absolute average of its initial states. However, it is assumed that each sensor node within the network captures the initial states $d_o[0] \in E$. At each time the $a_o \in A$ retains the parameters $d_o[p] \in E$ and $e_o[p] \in E$ and state variables $d_o^x[p] \in E$ and $e_o^x[p] \in E$ and $v_p^x[p] = d_o^x[p]/e_o^x[p]$. In (3) and (4) $1_{on}[p]$ is zero when data transfer occurs at the node a_o from the neighbor a_n at iteration o, the following cases are encountered. This transmits $e_o^x[p+1]$, $e_o[p+1]$, to an adjacent $a_p \in S'_o$ and set the value $d_o[p+1]$=0 and $e_d[p+1] = 0$.

$$d_o[p+1] = d_o[p] + \textstyle\sum_{a_n \in S''_o}\ 1_{on}[p] d_n[o] \tag{3}$$

$$e_o[p+1] = e_o[p] + \textstyle\sum_{a_n \in S''_o}\ 1_{on}[p] e_n[p] \tag{4}$$

First step: $e_o[p+1] > e_o^x[p]$,
Second step: $e_o[p+1] > e_o^x[p]$ and $d_o[p+1] \geq\ d_o^x[p]$ is satisfied, the node z_d updates the state variables as,

$$\begin{gathered} e_o^x[p+1] = e_o[p+1], \\ d_o^x[p+1] = d_o[p+1] \\ v_o^x[p+1] =\ d_o^x[p+1](e_o[p+1])^{-1} \end{gathered} \tag{5}$$

3.3. Reliability and privacy assurance framework

This section implements a security measure aimed at safeguarding the information of the nodes and eliminating any unauthorized nodes attempting to gain access to the network for data retrieval purposes.

Moreover, the main objective of the algorithm is to evaluate the D'. The proposed model uses an event-based approach to security modeling, in which a breach causes an event to be triggered. The existing method of maintaining privacy makes use of the node's initial states $d'''[0] = d_o[0] + z_o$.hence for preserving privacy, the proposed model evaluates the negative variable z_o such that it ensures the consensus approach will be computed in a specific number of steps. However, each sensor node holds a privacy value $z_o[p]$, steps Q_O, the other variable and transmission counter variable h_o , the absolute value of the initial value, and the added variables Q_O is required to be larger than the parallel node a_o, upon initialization each node Q_O chooses the steps and parameter variable to satisfy the below condition.

Condition 1: the added steps within the variable of each node a_o is larger or equal in comparison with the a_o's degree such that the parallel node receives any data.

$$Q_{mO} \geq I'_O \tag{5}$$

Condition 2: In addition, the node a_om includes the accumulated variable in the computation to ensure that the node state can be calculated without any errors.

$$z_o = -\sum_{q_o}^{q_o} z_o[q_o] \tag{6}$$

Constraint 3: Every node in the network induces the variable $z_o[q_o]$ based on an event that must not be negative.

$$z_o[q_o] \geq 0, for\ all\ q_o \epsilon [0, q_o] \tag{7}$$

Constraint 4: Node z_o stops inducing variables such that states can be calculated as follows

$$z_o[q_o] = 0, for\ all\ q_o \notin [0, q_o] \tag{8}$$

The initial variable is negative and meets the aforementioned conditions since they show that it is induced in the network $w_l \geq I''_o$. While transmitting data further during the execution of a multi-stage process, every node is required to adhere to constraints 1 and 2. If these constraints are not met, it will hinder the computation of the average consensus. The proposed Algorithm 1 incorporates a value transfer process in which every node is associated with a connected digraph $J_f = (Z, A)$, this performs execution according to the set of event-triggering conditions. Wherein each node here shows $z_d \in Z_q$ to ensure privacy.

- On the counter basis q_o is set to zero sets the number of offset-added steps, Q_o like that as $Q_o \geq L'_o$ and the set of $(Q_o + 1)$ within a positive offset as $z_o[q_o] > 0$, wherein $q_o \in \{0,1,2 \ldots., Q_o\}$.Initially the negative offset value z_o disapproves the initial value $d_n[0]$ to $z_o = -\sum_{Q_o=0}^{Q_o} z_o[q_o]$.
- To choose the $a_q \in S'_o$ in this order U_{qo} that transmits $e_m[0]$ and $d'''[0] = d_o[0] + z_o + z_o[0]$ to the neighbor sets the value ${e'''}_o[0] = 0$, $e_o[0] = 0$, and $q_o = q_o + 1$. This algorithm is executed within each n step, the node a_o receives a set of parameters as ${d'''}_n[p]$ and $e_n[p]$ for each in-neighbor $a_n \in S'''_o$, this node updates the variables with ${d'''}_o[p]$ that checks if the condition holds; if true then $z_o[q_o]$ to $b_o[p + 1]$ which enhances the offset counter q_o by one. It sets this variable $d^x_o[p + 1]$ and $e^x_o[p + 1]$ irrespective of $d^v_o[p + 1]$ and $e^x_o[R + 1]$. It then communicates with the ${d'''}_o[p + 1]$ and $e_o[p + 1]$ in a pre-trained fashion. The message is not received from any of its neighbors, without transmission the variables retain the same result.

3.4. Distributed edge consensus through adaptive node engagement (DECANE)

Algorithm 1. Distributed edge consensus through adaptive node engagement algorithm

```
Input: graph $L_i = (A,J)$ with $s = |J|$ edges along with the initial state of $D_n[0] \in E$
Step 1: Allot a specific value $T_{q_n}$ in a given set $\{0,1, \ldots I''_o\}$ for each adjacent node $a_q \in S''_o$
Step 2: Setting up the counter $h_o = 0$ along with index(priority based) $j_o$ to $h_o$
Step 3: Setting up the counter $q_o = 0$, selects $Q_o \in E > 0$ where $Q_o \geq I''_o$
Step 4: Setting up $D'_o = D_o[0] + z_o$,
                                 $D_o[0] = 1, E^x_o[0] = 1 \;\&\; E^x_o[0] = D'_o[0]$
Step 5: Select the adjacent node $c_s \in U''_q$ such that $V_{sq} = j_o$ and communicate $E_O[0]$ and $E'_o + z_o[0]$ to
        a particular adjacent node. Furthermore, setting $D'_O[0] = 0$, $E'_o[0] = 0$, $p_o = p_o + 1$
Step 6: Setting $h_m = f_o + 1$ and $j_o = h_o\ mod\ Q''_O$
Step 7: Considering the iteration of $p = 0,1,2 \ldots.every\ node\ a_o$ carries out the following operation
Step 8: If it receives $D'_n[P], E_n[P]$ from adjacent node $a_o \in S'''_O$ and updation is carried out with
        Equation 1 and Equation 2
```

```
Step 9: If equation 1 and equation 2 hold then communicate the data about nodes to preserve
        privacy
Step 10: Output as $v_o^x[p]$ for each node $a_o \in A$
```

In the above algorithm, the first q_o to zero and select the total number of variables adding with Q_o steps such that $Q_o \geq I''_o$ and with $(Q_o + 1)$ positive variable $z_o[q_o] > 0$. Furthermore, considering $q_o \in S'_o$ following order U_{qo} and transmit $D'_o[0]$ and $D'_o[0]$. Furthermore, while executing of algorithm, at every step o, the node a_o obtain a set of requests for packet transmission from every neighboring node; the requests are verified by checking the conditions; if the verification is successful, the data packets are transferred and the node stays in the network; if not, it is ejected.

4. RESULTS

The results are evaluated in the form of a graph for this, a system setup with a 2 TB hard drive, 16 GB of RAM, and 2 GB of NVidia Cuda-powered graphics is used for the testing. This proposed approach assesses the detection of erroneous nodes that lead to network imbalance. The computation of the throughput for 30, 40, and 50 nodes, as well as the identification of the proper and incorrect nodes, are some of the features that are considered in this assessment. By contrasting it with the existing model, a comparison analysis is carried out to verify the security and efficacy of the suggested model. The findings show that when compared to the existing system, the proposed model performs better.

4.1. Energy utilization

Figure 3 depicts the value of energy consumed over a series of rounds, with three different categories identified by the number of nodes: 30, 40, and 50. It's observed that as the number of rounds increases, the energy utilization for all node categories decreases, suggesting a degradation or expenditure of energy over time. The nodes with the value '30' start with the highest energy utilization and maintain a lead throughout the observed rounds, while the '50' nodes consistently show the lowest energy usage. This trend could indicate that fewer nodes consume energy more efficiently or that their starting energy levels are higher. Conversely, more nodes might have higher overall energy consumption or start with lower energy levels. The graph shows a clear pattern of energy depletion, and a possible inference is that energy conservation measures become more critical as the number of rounds increases, regardless of the number of nodes.

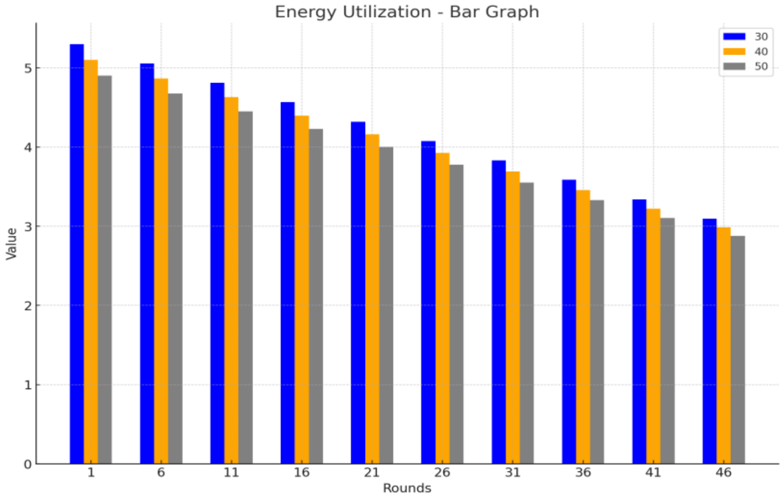

Figure 3 Energy utilization for different number of nodes

4.2. Packet level (correct node identification)

Figure 4 titled "Packet Level Classification," presents a comparative view of two different classifications, ES (Existing System) and PS (Proposed System), across varying percentages of deceptive nodes: 30%, 40%, and 50%. The data indicates that the value associated with PS is significantly higher than ES for all percentages of deceptive nodes. This could suggest that PS is more robust or prevalent in scenarios with a higher incidence of deception. Moreover, there doesn't seem to be a significant change in values for either classification as the percentage of deceptive nodes increases from 30% to 50%, indicating a stable relationship between the node deception percentage and the packet-level classification values. This stability might imply that the system’s ability to classify or handle deceptive nodes scales well with an increasing number of deceptive nodes, maintaining a consistent performance or that the classifications are not sensitive to the changes in the proportion of deceptive nodes.

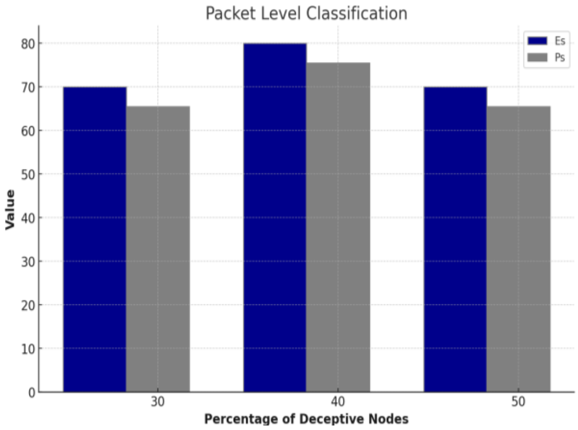

Figure 4. Packet-level classification for correct node identification

4.3. Wrong node identification

Figure 5 for wrong node identification illustrates the comparison between two classifications—ES and PS-across varying quantities of dishonest sensor nodes: 30, 40, and 50. In all categories, the ES classification identifies more erroneous nodes compared to the PS classification, suggesting a tendency towards higher false positives or a more conservative approach in labeling nodes as dishonest. The number of nodes incorrectly identified by ES peaks at 30, decreases at 40 and remains stable at 50. Meanwhile, the PS classification shows a gradual decrease in the count of misidentified nodes as the number of dishonest sensor nodes increases. This trend might suggest that the PS classification becomes more accurate or less sensitive as the number of dishonest nodes rises, which could be indicative of a system that adapts or becomes more discerning with greater exposure to dishonest behavior. The data implies that while ES is more aggressive in identifying dishonest nodes, PS might offer a more balanced approach, potentially reducing the incidence of false identifications in larger networks.

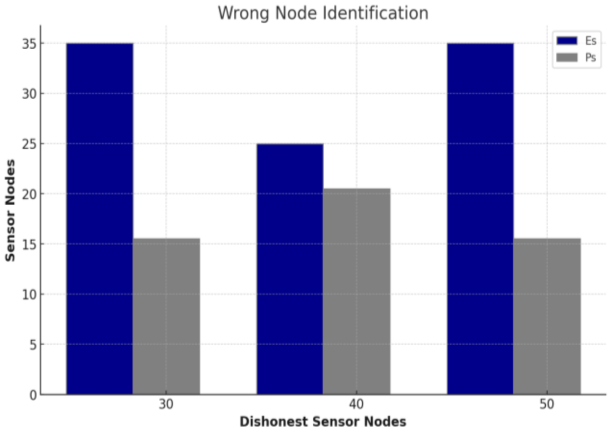

Figure 5 Wrong node identification comparison for various nodes

4.4. Throughput

The throughput parameter is evaluated at the packet and node levels in this section. Throughput is defined as the quantity of work done. Within a particular length of time and it highlights the efficiency of the models.

4.5. Throughput (Packet level comparison)

Figure 6 compares the packet value throughput across a network with different numbers of nodes: 30, 40, and 50, using two metrics, ES and PS. At 30 nodes, ES throughput is significantly lower than PS, which suggests that under these conditions, PS might be more efficient or possibly have a higher capacity for handling data packets. As the number of nodes increases to 40, ES throughput sees a substantial increase, surpassing PS, which could indicate that ES performs better in slightly larger networks or that its efficiency improves with more nodes. However, at 50 nodes, both ES and PS throughput values decrease, with ES experiencing a more pronounced reduction. This might suggest a scalability issue or network congestion that affects ES more severely than PS. The trend observed here points to a potential trade-off between the number of nodes and throughput efficiency for both ES and PS, with an optimal node count near 40 for ES and perhaps higher for PS.

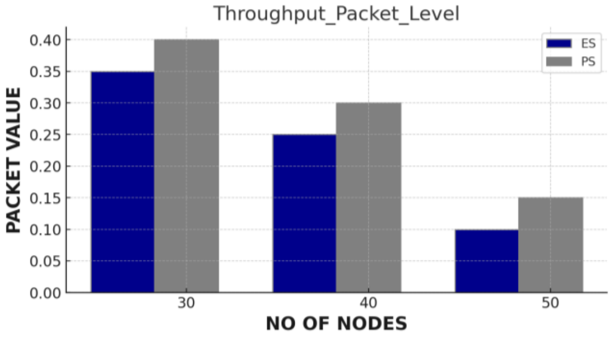

Figure 6. Throughput comparison at packet level

5. CONCLUSION

This paper presented the DTPCF, by leveraging a consensus-based approach for trust management coupled with robust privacy preservation mechanisms, the DTPCF addresses critical challenges inherent in the deployment and operation of IoT systems. The DTPCF's innovative integration of distributed trust evaluation and state-of-the-art privacy techniques offers a dual advantage: it not only enhances the resilience of IoT networks against malicious activities but also ensures the confidentiality of user data. The adaptability and scalability of the DTPCF suggest its applicability across a broad spectrum of IoT applications, from smart homes to industrial control systems, offering a solid foundation for its implementation in real-world settings, the development and validation of the distributed trust and privacy consensus framework represent a significant step forward in addressing the pressing need for secure, private, and trusted IoT and WSN architectures. As the digital landscape continues to evolve, the principles and methodologies underpinning the DTPCF will undoubtedly contribute to shaping a more secure and interconnected world, ensuring that trust and privacy are integral to the future of IoT innovation.

ACKNOWLEDGEMENT

I would like to express our sincere gratitude to all those who have supported and contributed to this research project. Primarily, I extend our heartfelt thanks to our guide for his unwavering guidance, invaluable insights, and encouragement throughout the research process.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Sushma Priyadarashini	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			✓	
Anuradha	✓	✓	✓		✓	✓		✓	✓	✓	✓	✓		

C	**C**onceptualization	I	**I**nvestigation	Vi	**Vi**sualization
M	**M**ethodology	R	**R**esources	Su	**Su**pervision
So	**So**ftware	D	**D**ata Curation	P	**P**roject administration
Va	**Va**lidation	O	Writing - **O**riginal Draft	Fu	**Fu**nding acquisition
Fo	**Fo**rmal analysis	E	Writing - Review & **E**diting		

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

No dataset is utilized in this research.

REFERENCE

[1] S. T. Mehedi, A. Anwar, Z. Rahman, K. Ahmed, and R. Islam, "Dependable intrusion detection system for IoT: a deep transfer learning based approach," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 1, pp. 1006–1017, Jan. 2023, doi: 10.1109/TII.2022.3164770.

[2] Y. Sei and A. Ohsuga, "Private true data mining: differential privacy featuring errors to manage internet-of-things data," *IEEE Access*, vol. 10, pp. 8738–8757, 2022, doi: 10.1109/ACCESS.2022.3143813.

[3] J. A. Onesimu, J. Karthikeyan, J. Eunice, M. Pomplun, and H. Dang, "Privacy preserving attribute-focused anonymization scheme for healthcare data publishing," *IEEE Access*, vol. 10, pp. 86979–86997, 2022, doi: 10.1109/ACCESS.2022.3199433.

[4] J. Andrew and J. Karthikeyan, "Privacy-preserving internet of things: techniques and applications," *International Journal of Engineering and Advanced Technology*, vol. 8, no. 6, pp. 3229–3234, Aug. 2019, doi: 10.35940/ijeat.F8830.088619.

[5] A. V. Dastjerdi and R. Buyya, "Fog computing: helping the internet of things realize its potential," *Computer*, vol. 49, no. 8, pp. 112–116, Aug. 2016, doi: 10.1109/MC.2016.245.

[6] I. Lee and K. Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises," *Business Horizons*, vol. 58, no. 4, pp. 431–440, Jul. 2015, doi: 10.1016/j.bushor.2015.03.008.

[7] N. Ma, H. Zhang, H. Hu, and Y. Qin, "ESCVAD: an energy-saving routing protocol based on voronoi adaptive clustering for wireless sensor networks," *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 9071–9085, Jun. 2022, doi: 10.1109/JIOT.2021.3120744.

[8] W. Zhou, Y. Jia, A. Peng, Y. Zhang, and P. Liu, "The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1606–1616, Apr. 2019, doi: 10.1109/JIOT.2018.2847733.

[9] H. Attaullah *et al.*, "Fuzzy-logic-based privacy-aware dynamic release of IoT-enabled healthcare data," *IEEE Internet of Things Journal*, vol. 9, no. 6, pp. 4411–4420, Mar. 2022, doi: 10.1109/JIOT.2021.3103939.

[10] M. A. Husnoo, A. Anwar, R. K. Chakrabortty, R. Doss, and M. J. Ryan, "Differential privacy for IoT-enabled critical infrastructure: a comprehensive survey," *IEEE Access*, vol. 9, pp. 153276–153304, 2021, doi: 10.1109/ACCESS.2021.3124309.

[11] P. Pujar, A. Kumar, and V. Kumar, "Plant leaf detection through machine learning based image classification approach," *IAES International Journal of Artificial Intelligence*, vol. 13, no. 1, pp. 1139–1148, Mar. 2024, doi: 10.11591/ijai.v13.i1.pp1139-1148.

[12] S. H. Sreedhara, V. Kumar, and S. Salma, "Efficient big data clustering using Adhoc fuzzy C means and auto-encoder CNN," in *Lecture Notes in Networks and Systems*, vol. 563, 2023, pp. 353–368.

[13] R. Lu, K. Heung, A. H. Lashkari, and A. A. Ghorbani, "A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT," *IEEE Access*, vol. 5, pp. 3302–3312, 2017, doi: 10.1109/ACCESS.2017.2677520.

[14] F. Zawaideh, M. Salamah, and H. Al-Bahadili, "A fair trust-based malicious node detection and isolation scheme for WSNs," in *Proceedings of 2nd International Conference on the Applications of Information Technology in Developing Renewable Energy Processes and Systems, IT-DREPS 2017*, Dec. 2017, vol. 2018-January, pp. 1–6, doi: 10.1109/IT-DREPS.2017.8277813.

[15] T. Khan, K. Singh, K. Ahmad, and K. A. Ahmad, "A secure and dependable trust assessment (SDTS) scheme for industrial communication networks," *Scientific Reports*, vol. 13, No. 1, 2023.

[16] S. Yaoxin, G. Xiufeng, and L. Yu, "Credibility based WSN trust model," *Electronics Optics & Control*, vol. 25, no. 3, p. 32, 2018, doi: 10.3969/j.issn.1671-637x.2018.03.008.

[17] V. Ram Prabha and P. Latha, "Fuzzy trust protocol for malicious node detection in wireless sensor networks," *Wireless Personal Communications*, vol. 94, no. 4, pp. 2549–2559, Jun. 2017, doi: 10.1007/s11277-016-3666-1.

[18] W. Zhang, S. Zhu, J. Tang, and N. Xiong, "A novel trust management scheme based on Dempster–Shafer evidence theory for malicious nodes detection in wireless sensor networks," *Journal of Supercomputing*, vol. 74, no. 4, pp. 1779–1801, Apr. 2018, doi: 10.1007/s11227-017-2150-3.

[19] G. Yang, G. S. Yin, W. Yang, and D. M. Zuo, "A reputation-based model for malicious node detection in WSNs," *Harbin Gongye Daxue Xuebao/Journal of Harbin Institute of Technology*, vol. 41, no. 10, pp. 158–162, 2009, doi: 10.367-6234(2009)10-0158-05.

[20] C. Miao *et al.*, "Privacy-preserving truth discovery in crowd sensing systems," *ACM Transactions on Sensor Networks*, vol. 15, no. 1, pp. 1–32, Feb. 2019, doi: 10.1145/3277505.

[21] Y. Li *et al.*, "An efficient two-layer mechanism for privacy-preserving truth discovery," in *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, Jul. 2018, pp. 1705–1714, doi: 10.1145/3219819.3219998.

[22] C. Miao, L. Su, W. Jiang, Y. Li, and M. Tian, "A lightweight privacy-preserving truth discovery framework for mobile crowd sensing systems," in *Proceedings - IEEE INFOCOM*, May 2017, pp. 1–9, doi: 10.1109/INFOCOM.2017.8057114.

[23] Z. Li, Z. Zheng, S. Guo, B. Guo, F. Xiao, and K. Ren, "Disguised as privacy: data poisoning attacks against differentially private crowdsensing systems," *IEEE Transactions on Mobile Computing*, vol. 22, no. 9, pp. 5155–5169, 2023, doi: 10.1109/TMC.2022.3173642.

[24] Z. Zheng, Z. Li, H. Jiang, L. Y. Zhang, and D. Tu, “Semantic-aware privacy-preserving online location trajectory data sharing,” *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 2256–2271, 2022, doi: 10.1109/TIFS.2022.3181855.

[25] J. N. Al-Karaki and G. A. Al-Mashaqbeh, “SENSORIA: a new simulation platform for wireless sensor networks,” in *2007 International Conference on Sensor Technologies and Applications, SENSORCOMM 2007, Proceedings*, Oct. 2007, pp. 424–429, doi: 10.1109/SENSORCOMM.2007.4394958.

BIOGRAPHIES OF AUTHORS

Sushma Priyadarashini working as Assistant Prof. in computer science and Engineering Department of KCTE college, Kalaburgi with experience of 19 years in Teaching and Ph.D. in the area of Wireless sensor network, and I had workshop, FDP area of interest in computer Networks and cloud computing. She can be contacted at this email: sushma_priyadarashini@rediffmail.com.

Dr. Anuradha got graduated in computer science Engineering in 2005 and completed posted graduation in 2007 computer Science and Engineering in 2018 she was awarded Ph.D. in computer science and engineering. She has published 40 papers in leading international journals and conference proceedings. She is presently working as associate professor PDA college of Engineering. She can be contacted at this email: anuradhat@pdaengg.com.