QUBAHAN ACADEMIC JOURNAL
VOL. 4, NO. 2, June 2024
https://doi.org/10.48161/qaj.v4n2a537

LTEM: Lightweight Trust Evaluation Model in IoT Environment

Somya Abdulkarim Alhandi [1], Hazalila Kamaludin [1*], Nayef Abdulwahab Mohammed Alduais [1*], Noor Zuraidin Mohd Safar [1] and Salama A. Mostafa [1]

[1] Faculty of Computer Science and Information Technology, University Tun Hussein Onn Malaysia, 86400, Batu Pahat, Johor, Malaysia.

Corresponding author: e-mail: hazalila@uthm.edu.my and nayef@uthm.edu.my.

ABSTRACT: In the domain of the Internet of Things (IoT), data reliability is important, particularly within critical sectors like healthcare, environmental surveillance, and smart grids. Nevertheless, data transfer from the physical domain to the digital layer is susceptible to trust-related challenges encompassing data integrity, genuineness, and credibility. Predominantly, prevailing models for trust assessment primarily concentrate on the conduct of nodes, thus disregarding the direct evaluation of data packets. This particular constraint results in an insufficient validation of data credibility, thereby failing to consider pivotal elements like timeliness and accuracy. Furthermore, utilizing cloud-based packet evaluation frameworks frequently leads to inaccuracies, unreliability, and energy inefficiencies owing to the transfer of untrusted data. The current study introduces a streamlined trust assessment framework called the lightweight trust evaluation model (LTEM), custom-built for IoT settings to combat these obstacles. LTEM meticulously examines node behavior and data packets via a multi-tiered approach encompassing nodes, cluster heads (CH), and base stations (BS). Moreover, the proposed model's architecture considers energy usage by averting the transmission of untrusted data. Simulation results showcase the supremacy of LTEM compared to existing models by achieving a detection rate of 99% for untrusted data packets, outperforming the detection rates ranging from 30% to 75% observed in other models. Moreover, LTEM enhances the operational efficiency of sensor nodes regarding energy consumption, achieving an average energy utilization of 1.33J out of 4J, resulting in savings of approximately 2.67J on average, thereby extending the lifespan of nodes.

Keywords: Internet of Things; Trust Evaluation; Trust Value; Trust Model; Holistic Trust Model

I. INTRODUCTION

The Internet of Things (IoT) has recently emerged as a significant area of focus in both the academic realm and the information technology industry [1]. The increasing popularity of the IoT has opened up avenues for a robust method of representing the physical world comprehensively and enabling significant interactions with the tangible environment [2, 3]. At present, a vast network of interconnected IoT devices, comprising physical entities embedded with sensor nodes possessing IP addresses for seamless Internet connectivity and inter-device communication, is demonstrating promising potential across a multitude of sectors [4-6]. These domains encompass a broad spectrum of applications, ranging from industrial sectors like monitoring oil wells, enhancing transportation systems for vehicles, and optimizing agriculture practices to more personal settings, including smart home technologies, wearable devices, healthcare solutions, automotive innovations, and efficient power grid systems [7]. Figure 1 shows the popularity of various IoT applications in 2024 according to the popularity index of interest and relative usage.

These instances merely scratch the surface of the myriad application areas where this groundbreaking paradigm is poised to gain considerable traction. As per [3], the IoT ecosystem hit a significant milestone in 2020 by surpassing 50 billion connected objects, and this figure is anticipated to triple by 2025, as illustrated in Figure 2. This impressive expansion not only underscores the far-reaching impact of the IoT but also underscores its enduring significance as a catalyst for technological advancement and ingenuity.

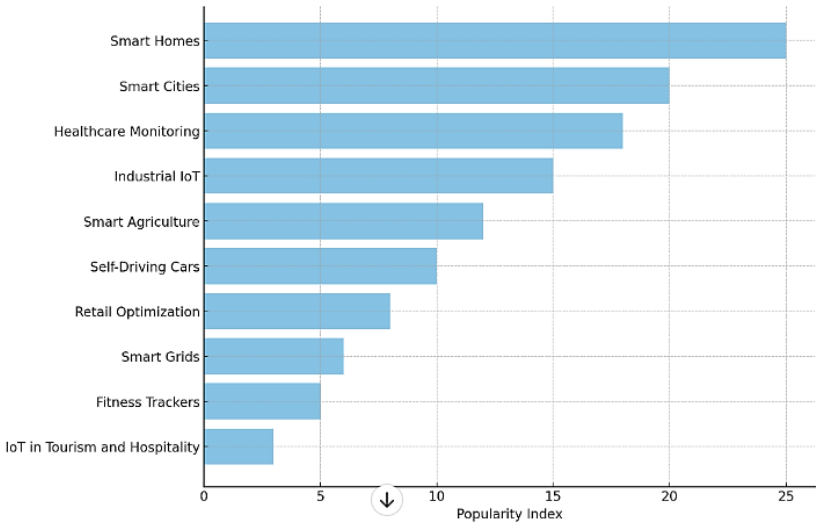

FIGURE 1. The popularity of the IoT applications in 2024

The advent of IoT has introduced new challenges to IoT services and devices due to its diverse data sharing, dynamic nature, and diversity of devices involved. These challenges are often addressed by addressing security issues rather than assessing specific risks across IoT entities and services [8, 9]. This approach could lead to serious harm and unforeseen danger if a malicious object exploits this information. Another issue related to the reliability of data collection is important in the field of IoT [10, 6]. When large amounts of data are collected from the physical sensing layer, and there is a lack of trustworthiness due to damaged sensors or malicious input, it can seriously affect the quality of IoT services. Even if network layer and application layer trust can be fully provided, the quality of IoT services will be greatly affected and difficult to accept by users [6, 11]. Therefore, trust in IoT is crucial to ensure reliable data and secure service provision among various IoT objects. Formerly, trust has become a fundamental requirement for strong security measures [9]. However, trust as a concept lacks a concrete definition, as it varies depending on the individuals involved and the specific situation and is influenced by both measurable and non-measurable factors [6, 7].

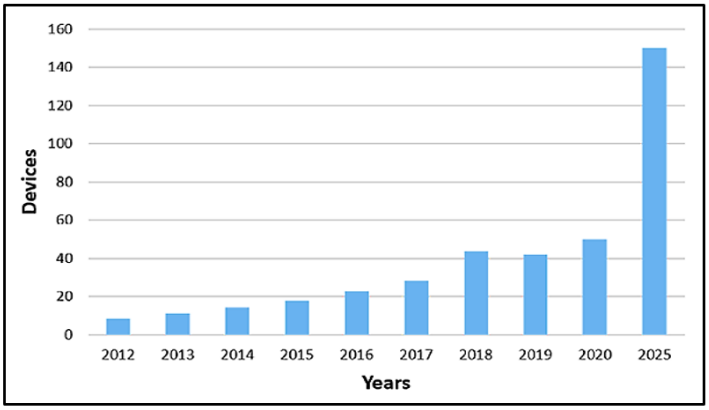

FIGURE 2. Growth of IoT Devices [1]

This complexity means that trust encompasses a variety of attributes, including an entity's capabilities, strength, goodness, reliability, availability, and other characteristics [8]. Consequently, trust poses a greater challenge than ensuring security, especially in emerging fields such as information technology in the IoT [9]. The idea of trust in IoT revolves around evaluating the behavior of connected devices within the same network. The level of trust between two devices significantly affects how they interact in the future [12]. When devices trust each other, they are more likely to collaborate by sharing data, services, and resources to a certain extent. The trust evaluation model

involves calculating and analyzing trust between devices, enabling informed decisions to establish efficient and reliable communication between devices.

The trust evaluation model is practical for solving trust-related issues in the context of IoT. These solutions have proven effective in enhancing security measures, aiding decision-making processes, identifying untrusted behavior, isolating untrusted entities, and rerouting functionality to trusted domains [10]. Researchers have devised various approaches, including those highlighted in references [10-22], as potential answers to trust-related challenges. However, these solutions still have certain limitations, including the inability to address trust issues comprehensively, difficulties handling large amounts of data and changing behavior, high energy consumption, quantifying the uncertainty associated with untrustworthy behavior, and selecting the most appropriate components. This work addresses the challenges of modeling trust and dealing with IoT's dynamic nature and heterogeneity [10].

Different trust evaluation models have been introduced by [10-22] to address the above challenges; however, some issues need to be considered, such as:

- Lack of consideration for data packet evaluation: Existing trust evaluation models mainly focus on node behavior without adequately considering the trustworthiness of data packets. This problem highlights the need for a trust model that can simultaneously assess both node behavior and data packet.
- Limitations of existing trust evaluation models: The research acknowledges that current trust evaluation models in the literature utilize a certain set of metrics to assess trustworthiness, primarily based on node behavior. However, these models may need to fully address the unique attributes of data, such as timeliness and validity, which are crucial for evaluating data trustworthiness.
- Energy consumption and transmission of untrusted packets: The transmission of untrusted data packets affects the system's accuracy and reliability and leads to energy wastage in the nodes. The research recognizes the importance of avoiding this to reduce energy consumption and extend the node's energy battery.

A lightweight trust evaluation (LTEM) in an IoT environment is proposed to solve the above trust issues in IoT applications. The significance of this model is summarized as follows:

- The proposed model considers three main factors, data packet, node behavior, and energy, that contribute to detecting most untrusted packets, unlike the other models that consider only one or two factors.
- The evaluation in the proposed model has been performed at three levels: node, CH, and BS. This helps improve the application's reliability as the packets will be evaluated at each level, node, CH, and BS. It also helps to reduce energy consumption because the untrusted packets are detected in the beginning at the node level. If it is untrusted, they are dropped before being transmitted to CH.
- The proposed model's accuracy is very high because each packet is evaluated individually. Furthermore, it considers all factors, including node data, node behavior, and energy factors. The proposed model evaluates node, CH, and BS packets at each level.
- The proposed model shows each node's confidence level/Trust Value, which helps the administrators know the node's status and take the necessary actions when the status is suspected or abnormal to avoid unexpected errors in the IoT application.

The rest of this paper is organized as follows: Section II investigates and discusses related work. Section III describes the proposed model. Section IV reports the experimental investigation, result analysis, and evaluation of the proposed model and the comparison results with existing models. Section V concludes the paper and suggests some future research directions.

II. RELATED WORK

The research of [13] introduces a trust evaluation model using the entropy method to identify potentially malicious nodes. The model measures direct and indirect trust values by examining the characteristics of relevant behavioral nodes and uses entropy methods to establish appropriate weight factors. It is worth noting that this method only detects malicious nodes based on their behavioral patterns without considering the content of the packets transmitted by these nodes.

The researchers in [3] introduced a trust management model specifically designed for IoT devices and services. The model utilizes Simple Multi-Attribute Scoring Technique (SMART) and Long Short-Term Memory (LSTM)

algorithms. SMART calculates trust values, while LSTM detects changes in behavior by comparing them with a predefined trust threshold. The model's main function is to pinpoint instances of untrustworthy behavior and isolate nodes exhibiting such behavior. However, the study did not cover trust-related data packets.

In [14], a trust management system model is introduced that aims to handle trust-related aspects in the context of inter-domain communication during the deployment of services in IoT networks. Their model mainly focuses on centrally controlling client service requests and managing the storage of trust values and certificate generation. However, more is needed to solve the problem of system scalability fully. Furthermore, the model does not consider objects with extensive social connections or clients vulnerable to various attacks, thus excluding them from its scope.

Another study [15] proposed a trust analysis method using information entropy to address trust-related challenges in IoT communication terminal power distribution. This approach involves establishing direct trust values based on exponentially distributed importance. Subsequently, the direct trust value is adjusted using the selected forgetting factor and sliding window. Furthermore, the unpredictability of direct trust values is evaluated, and indirect trust values are introduced to address potential errors in direct trust evaluation. In addition, a comprehensive analysis of indirect and direct trust values is performed to improve the accuracy of the assessment. Experimental results show that the technique effectively resists collisions and resist attacks. However, since this model relies on many parameters and complex calculations, some limitations exist in determining the weights and energy consumption.

The work in [12] proposed a unified calculation method based on models and fuzzy logic combined with a multi-criteria decision-making method. This method is used to evaluate trust weight. This study highlights the fuzzy mechanism's effectiveness in multi-criteria decision-making, demonstrating its superior ability to select reliable acquaintances in the Social Internet of Things (SIoT) context. It has also been suggested that this approach can be an important tool for uncovering trust-building properties in SIoT social objects.

The study in [5] proposed a benefit-centered model for organically establishing social connections between Social IoT nodes (SIoT) in a virtual community environment. This model efficiently computes trust between social nodes by considering user preferences related to shared interests. Furthermore, the authors introduce a system that employs recommendations based on similarities between service requesters and providers to improve service quality. Nonetheless, it is worth noting that these studies do not focus on the classification and prioritization of trust indicators or parameters when validating friendships in the context of SIoT.

In [16], a quantitative trust value model was introduced for identifying node behavior within Wireless Sensor Networks (WSN). The model involves the selection of various trust factors related to the behavior of sensor nodes. In order to ensure objectivity and reduce the impact of subjective settings, each trust factor is determined using the entropy method. Furthermore, the Dumpster-Shafer (D-S) theory is adopted to derive and consolidate trust, and statistical factors related to node behavior are introduced to refine the overall results. Notably, the model exhibits robustness against attacks and the ability to identify malicious nodes. The security of data packet forwarding is achieved through the combination of the entropy method and D-S theory. However, it is worth noting that the model's calculation process uses complex algorithms, resulting in increased energy consumption.

[17] introduces a trust model scheme rooted in the Dumpster-Shafer evidence theory. This scheme considers the spatiotemporal correlation of data collected by sensor nodes in nearby areas and approximates node credibility. Utilizing principles from D-S theory, this trust model is designed to assess the degree of interaction related to trust, uncertainty, or distrust. It can also be used as a tool to estimate direct and indirect trust values, using a flexible, comprehensive approach that allows the calculation of overall trust to classify potentially malicious nodes. Compared with traditional methods, this method has advantages in identifying malicious nodes and improving data fusion accuracy. However, there is a possibility for improvement in achieving a better balance between increasing energy efficiency, reducing redundant information, and ensuring impartiality in credibility assessments.

The research described in [2] proposes an adaptive trust management mechanism tailored for Wireless Sensor Networks. First, a node's trustworthiness is assessed based on its performance during interactions within its local information environment. Subsequently, an overall trustworthiness score is derived by merging the energy evaluation and trust endorsement metrics of other nodes with higher trust levels. In addition, node management and node reliability are constantly updated. Simulation and analysis results confirm that this method accurately and comprehensively depicts the credibility of nodes. However, it is worth noting that relying on the trust values

of other nodes (which may be compromised) in trust calculations may lead to incorrect recommendations and abnormal overall trust scores.

As described in [18], the Trust and Energy Aware Routing Protocol (TERP) routing protocol relies on a combination of trust, residual energy, and hop count parameters weighted accordingly to establish routes within Wireless Sensor Networks. Trust calculation in TERP involves a weighted average of direct and indirect trust, which is determined by recommendations from neighboring nodes. Additionally, nodes exchange information about their remaining energy levels. However, TERP's detection of malicious nodes is entirely based on evaluating communication trust.

In their research [19], a cluster-based centralized trust model was introduced as a solution to address the security issues and obstacles associated with IoT. The main goal of this research revolves around building a centralized trust framework tailored for IoT applications. To achieve this goal, the model employs intra- and inter-cluster analysis to determine the trustworthiness of node data and the presence of anomalous data. Within this framework, a node's data credibility is assessed by reviewing all node-sensing information's completeness, uniqueness, consistency, and accuracy.

In [20], a trust management model tailored for SIoT-based networks is introduced, aiming to evaluate the behavior of social entities. The assessment of node trustworthiness involves utilizing various trust metrics, including direct trust (based on first-hand information), indirect trust (based on second-hand recommendations), energy consumption, centrality, shared interests within the community, and service ratings. The proposed scheme implements regular synchronization of trust updates to enhance its effectiveness and reliability. Furthermore, the study includes an analysis of SIoT network performance and validates the reliability of the trust model even in the presence of selective forwarding attacks, especially ON/OFF attacks. However, there is still a need for improvement in detecting intruder patterns, especially when trust values are relatively low.

The basic function of WSN is to sense the environment and forward the sensed data to the BS. Malicious nodes may modify the data before forwarding it to the BS. MAC (Message Authentication Code) can protect data integrity, but MAC encryption may only be useful if the misleading data originates from the malicious node itself [21]. However, an effective data trust model may mitigate such attacks. This study [6] introduced a provenance-based trust management solution to establish trust among connected IoT devices. It provides a way to assess data reliability from a specific IoT device objectively. This model provides solutions to the data-related trust of IoT devices. Reliable solutions are needed to reduce resource pressure on space, response time, and manager performance.

In [22], a trust-based data fusion mechanism is introduced. It utilizes a trust evaluation model that computes trust values using the average weight of the comprehensive trust degree. This comprehensive trust degree considers three factors: data trust, behavior trust, and historical trust. Data trust is determined from sensor data processing; behavior trust is based on node behavior during data transmission, and historical trust begins with the maximum value and is updated with the comprehensive trust. The final trust value is recorded in a list and used for data fusion. This model effectively manages node status and prolongs node survival. Additionally, it exhibits superior anomaly detection compared to other models due to its consideration of data, behavior, and historical inertia.

In [23], it realizes dynamic trust evaluation through the dynamic adaptation of direct and indirect trust weights and the refinement of mechanism parameters. The calculation of direct trust considers energy trust, data trust, communication trust, and other factors and combines penalty factors and adjustment functions. Indirect trust, on the other hand, is endorsed and evaluated by an external third-party trust source. Furthermore, the comprehensive trust score is determined by dynamically assigning weights to direct and indirect trust and then combining them. In addition, the author proposes an update mechanism that utilizes sliding windows and adopts an ordered weighted average operator to enhance the system's flexibility.

In another study in [24], the Efficient Distributed Trust Model used the three key trust components: communication, data, and energy. Communication trust is derived from the evaluation of direct trust and indirect trust. Direct trust is determined by analyzing forwarding behavior using the beta distribution method, while indirect trust is established through the trust chain method. On the other hand, data trust is established by evaluating the differences between sensor data and average data from sensors within the same geographic area. Finally, energy trust relies on the node's remaining energy reserves. However, it is assumed that the node knows

the initial energy levels of its neighbors, which may only sometimes be feasible. Furthermore, methods that use averages to calculate data trust become ineffective in cases where malicious nodes transmit high outliers that significantly deviate from legitimate sensor data. The comparison of the proposed LTEM model to the previous works is tabulated in Table 1.

Table 1. Comparison of LTEM and the previous work

Ref. No	Behavior Node Trust	Data Node Trust	Energy Consumption Trust	Thing	Node	Cloud	Complexity	Lightweight
[2]	√	x	√	-	-	-	x	-
[3]	√	x	x	-	-	-	x	√
[6]	x	√	x	-	-	-	√	x
[13]	√	x	x	-	-	-	x	√
[14]	√	x	x	x	x	√	√	x
[15]	√	x	x	-	-	-	√	x
[12]	√	√	x	-	-	-	√	x
[16]	√	x	x	-	-	-	√	x
[17]	x	√	x	-	-	-	√	x
[18]	√	x	√	-	-	-	x	-
[19]	x	√	x	x	√	x	x	√
[20]	√	x	-	-	-	-	x	-
[21]	x	√	x	-	-	-	x	x
[22]	√	√	x	x	√	x	√	x
[23]	x	√	√	-	-	-	x	-
[24]	x	√	√	-	-	-	-	x
LTEM	√	√	√	√	√	√	x	√

nnotation: √ -Considered, x Not Considered, - Not Mentioned

III. THE LTEM MODEL

The general architecture of the LTEM is based on cluster architecture, as shown in Figure 3. The cluster architecture includes member nodes, CH, and BS. The nodes are distributed in a cluster, each with a Cluster Head. The node collects and transmits data from the environment to CH. The CH aggregates data from its member nodes and forwards it to the BS. The node in the LTEM contains a sensor and an RFID reader. The sensor is responsible for reading the body temperature of the object. Similarly, the reader is used to scan the RFID tag that is attached to the object. Therefore, the node transmits the sensor values and RFID tag data to CH. After that, the CH aggregates data from each member node and transmits it to the BS. Finally, the BS analyses the data and forwards it to the online cloud.

A lightweight trust-evaluation model in IoT applications is proposed to ensure the sensed data is trusted and transmitted to the cloud reliably. The evaluation of packets in the LTEM is carried out at three levels: at nodes, CH, and BS levels. The evaluation of packets in the LTEM includes three factors, as shown in Figure 3: data packet, node behavior, and energy factor. The trust metrics used in the LTEM are based on the flowing references [16, 23, 25, 26, 27, 28], which are:

- Timestamp (TS)
- Out-Range (Ran)
- Data Repetition (DR)
- Delay in transmitting a packet from Node to CH ($Delay\_N\_CH$)
- Energy consumed to a transmitted packet from Node to CH (EC_N_CH)
- Delay in transmitting a packet from CH to BS ($Delay\_CH\_BS$)
- Energy consumed to a transmitted packet from CH to BS (EC_CH_BS)
- Tag Validation (TV)

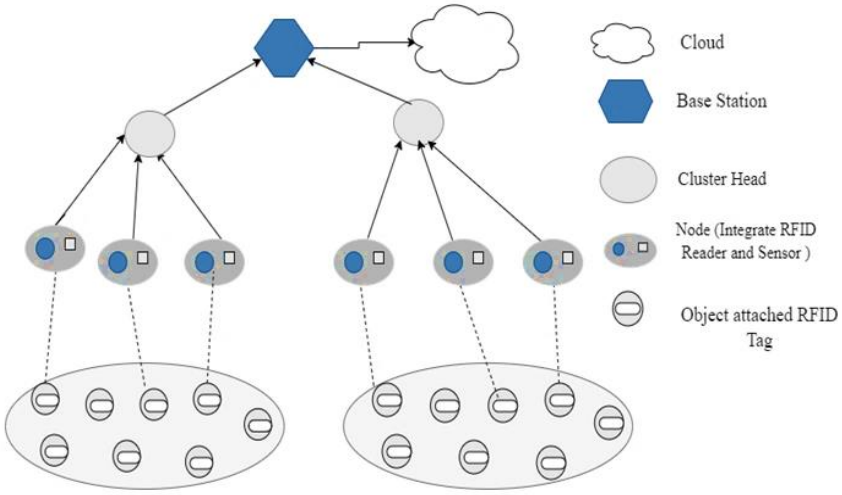

FIGURE 3. Cluster architecture of the LTEM

Some metrics are related to the data node, while others are related to the node behavior and node energy factor. Based on these trust metrics, the LTEM evaluates whether the packet is trustworthy or not. If the packet is trustworthy, it will be forwarded to the cloud; otherwise, it will be dropped, as shown in Figure 4.

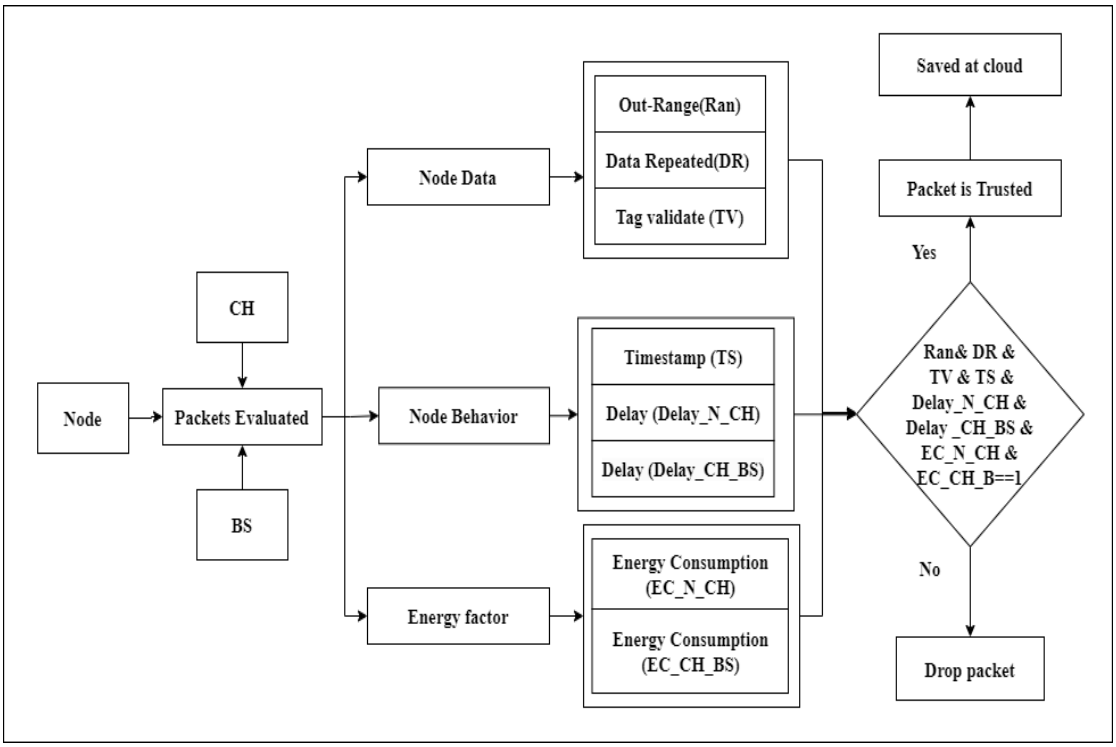

FIGURE 4. Trust metrics of the LTEM

Figure 5 shows the overall process of the trust evaluation model, which starts from the node (the node includes a temperature sensor and an RFID reader).

First, the node checks the body temperature of an object that has a range $Out - Range(Ran)$ (of 39°C – 43°C) [27]. The data packet is incorrect and discarded if the sensed data is greater than the maximum or less than the minimum range. However, if it is in range, it will be accepted, and the node will check the next metric, timestamp (TS), which is used to verify the tag ID. After the reader scans the RFID tag, the tag responds by sending a message

($Tag\_ID, object\_id$) and a timestamp (Tt) of the tag's current time. When the reader receives the message and Tt, it compares the reader's current time (Tr) with the tag's time and calculates the difference between them. If the result exceeds the time threshold ($\&T$), the authentication is denied, and the packet is dropped. Otherwise, the tag authentication is accepted. After that, the node checks the next metric, $Data\ Repeated$ (DR). Once the node scans the RFID tag and reads the body temperature of the object, the node compares them with the previous data packets. If they are similar, the packet is duplicated and will be dropped. Otherwise, it is valid, so the packet is trusted. Then, the node will send it to the Cluster Head. Once the object reaches the communication range, the sensor reads its body temperature, and the reader scans the tag ID. Nodes evaluate the sensed data and tag ID against TS, Ran, and DR. The packet evaluation Algorithm (1) at the node level is described in the following pseudocode.

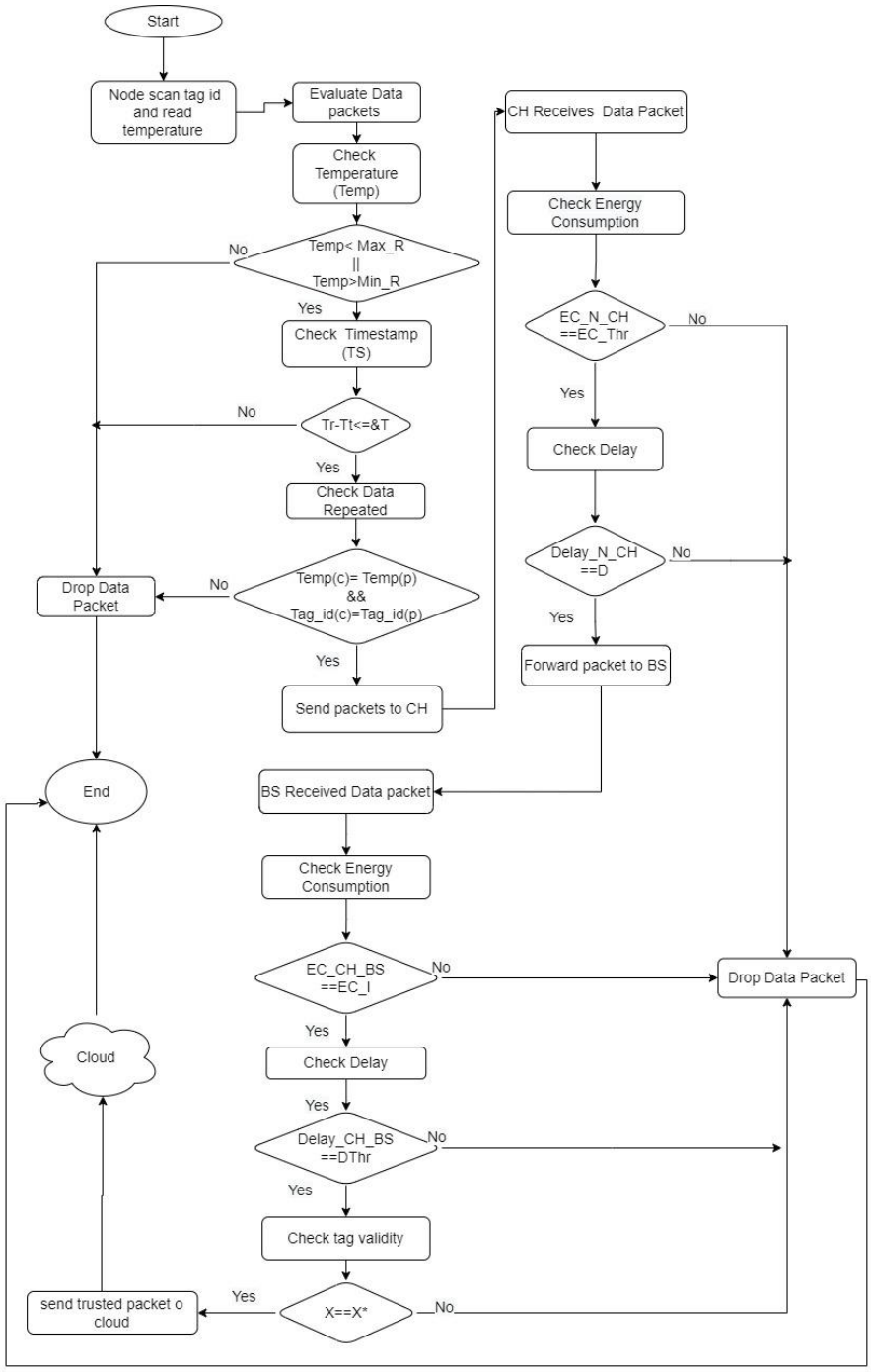

FIGURE 5. Packet evaluation process from node level to cloud level in LTEM

Algorithm (1) Evaluation at Node

```
Input:
   Temp (c), Temp (p), Tag_id(c), Tag_id(p), Tr, Tt , &T, Max_R, Min_R
Output:
    St either 1 Send packet or 0 remove packet.
Begin:
     Set Tag_id(p) previous reader  tag ID scanned by a reader
     Set Temp (p)  previous temperature value of the object read by the sensor
     Read Temp(c)  current  temperature value
    Read Tag_id(p) current tag ID scanned by a reader
     Set Tt  time sending tag  id
     Read Tr current time receive tag id by the reader
    If  (Tr – Tt  > &T)
       Set St = 0 //Remove packet
    Else if (Temp(c) >  Max_R|&&Temp(c) < Min_R)
        Set St = 0 //Remove packet
         If  (Temp(c) == Temp(p) &&  Tag_id(c) == Tag_id(p)
            Set St = 0 //Remove packet
        Else
             Set  St = 1  //Send packet to cluster head
   End  if
End Algorithm #
```

The packet evaluation Algorithm (2) at the cluster head level is described in the following pseudocode.

Algorithm (2) Evaluation at CH

```
Input:
   Temp(c),  Tag_id(c),  ST,  AT, D,  EC_Thr
Output:
    St either 1 or 0 //Send  or  packet to BS or  remove packet
Begin:
     The cluster head receives a packet
     Read   Temp(c) and  Tag_id(c)
     Set  ST   Packet send Time
    Read  AT   Packet Arrival Time
    If  (AT –  ST >  D)
          Set St = 0 //Remove packet
    Else
          Compute Energy Consumption(  EC_N_CH) as Eq. (3.7)
         If  (EC_N_CH ~ =  EC_Thr) //EC_Thr energy consumption at initial stage
             Set St = 0 //Remove packet
        Else
             Set St  = 1  //Send packet to BS
  End if
End Algorithm #
```

When the CH receives the packet, it will check the energy consumed in transmitting the packet from the node to itself (EC_N_CH). If the energy consumed in sending a packet is not equal to the energy consumed (EC_Thr) in the initial stage, it is considered abnormal, and the packet will be discarded. However, it is considered normal if the energy consumption is equal (EC_Thr). Thus, the CH then checks the next metric, which is the delay in the transmission from the node to CH. If the delay exceeds the threshold (D), the packet is rejected and dropped. Otherwise, the packet is accepted, and the status of the packet is trusted. Hence, the CH forwards the packet to the BS. The packet evaluation Algorithm (3) at the BS level is described in the following pseudocode.

Algorithm (3) Evaluation at BS:

```
Input:
  Temp(c), Tag_id(c), obj_id, ST_CH , AT_BS , DThr, EC_I Tag_id_S
Output:
   St either 1 or 0 //Send packet to BS or remove packet.
Begin:
   BS receive a packet from the Cluster Head
   Read Temp(c) and Tag_id(c)
   Set ST_CH Packet to send − time
   Read AT_BS Packet Arrival Time
 If (AT_BS – ST_CH > DThr)
        Set St = 0 //Remove packet
  Else
         Compute energy consumption EC_ CH_BS as Eq(3.11)
         If (EC_CH_BS~ = EC_I) // EC_I energy consumption at initial stage
            Set St = 0 //Remove packet
          Else
            Set X = Tag_id(c) // Tag_ID that is received from cluster head
             Read obj_id (Object Id)
             Read Tag _id_s from the server where the object id in the server equals the received object id.
             Set X* = (Tag_id_S ) //tag _id_s that is saved in the BS registration
           If (X ~ = X* )
                Set St = 0 //Remove packet
            Else
                Set St = 1 //Send packet cloud
   End if
End Algorithm #
```

Once the BS receives the packet, it checks the EC_N_CH. If the energy consumption of sending a packet from CH is not equal to the energy consumed in the initial stage (EC_I), the packet will be discarded. Otherwise, if the energy consumption is equal to EC_I, it is considered normal, and the BS will check the next metric, which is delay ($Delay\_CH\_BS$) in transmitting the packet from the CH to itself. If the delay exceeds the threshold ($DThr$) of 0.5s [29], the packet is unreliable and will be dropped. Otherwise, the packet will be authentic, and the BS will check the next metric, which is $Tag\ Validation$ (TV). The BS checks the RFID tag ID scanned by the reader received from the CH (X) against the tag ID stored in its database during the registration phase (*X). If they are the same, the tag authentication is accepted, and the packet is considered trusted and sent to the cloud. Otherwise, the tag will be rejected and will be dropped. Then, it will not be transmitted to the cloud because it is considered an untrusted packet. Table II describes the notations used in Figure 5.

IV. RESULT AND ANALYSIS

In this paper, we conducted our simulation on MATLAB, and multiple tests have been performed to validate the proposed model regarding the number of detected untrusted packets, energy efficiency, and accuracy. Simulation results show that the proposed model can detect untrusted packets and has higher detection accuracy than other models. In addition, the proposed model consumes less energy and saves more than existing models. Six scenarios were conducted to evaluate the performance of the LTEM. In the first scenario, LTEM is compared to the original model, which transmits packets directly to the cloud without detecting untrusted packets. In the second scenario, LTEM is evaluated based on the node, CH, or BS packet evaluation level in the third scenario. LTEM is compared with other models (DAME, EWMN, TMDF, and DTEM) according to the factors used to evaluate the packet. To evaluate the accuracy, the fourth scenario is applied in one node with different samples (500, 1000, 1500, and 2000 packets) injected with varying percentages of error. The fifth scenario is conducted in one cluster, with different nodes (N1, N2, N3, N4, N5, and N6) injected with different error percentages. The sixth scenario was carried out in all clusters, including all the nodes in the LTEM, which were injected with different percentages of errors. Table 2 shows the experimental parameters of the LTEM. Table 3 shows the scenario setup for the evaluation of LTEM.

Table 2. Parameters to develop LTEM

Parameters	Value
Number of Nodes	30 nodes
Node Distribute	randomly
Number of rounds	different round is used
Simulation Area	100m^2 x100m^2
Initial energy of node	0.5 j
Energy for Data Aggregation (EDA)	5nj/bit/signal
Transmitter Electronics and Receiver Electronics (Eelec)	50 nj/bit
Transmit Amplifier in free space (ξfs)	100 pi/bit/m2
Transmit Amplifier in free space (ξmp)	0.0013 pi/bit/m2
Message bits send per packet per node (L)	4000 bit
DT, $Dthr$	0.5s [31]
&T	100 MS
Internet Technology	Wi-Fi

Table 3. Scenarios setup used to evaluate LTEM

Scenario	Sample of size packets	Number of Nodes	Performance metrics	Error injected
Scenario 1	250, 230, 200, 190, 173, 150, and 145	7 nodes	Number of detected untrusted packets. Energy Consumption. Residual Energy	30%
Scenario 2	100 packets	1 node	Number of detected untrusted packets. Energy Consumption. Residual Energy	30%
Scenario 3	100 packets	1 node	Number of detected untrusted packets. Energy Consumption. Residual Energy	30%
Scenario 4	500, 1000, 1500, 2000 packets	1 node	Model accuracy	10% and 30%
Scenario 5	100 packets	6 nodes	Model accuracy	10%, 20% and 30%
Scenario 6	100 packets	30 nodes	Model accuracy	10%, 15%, 20%, 25%, and 30%

1. FIRST SCENARIO

Before adding the trust evaluation metric (BATEM), the model is compared to the proposed model LTEM. BATEM directly sends data packets from nodes to CH, from CH to BS, and then to the cloud without detecting untrusted data packets. The cloud then receives all trusted and untrusted packets. LTEM, on the other hand, evaluates packets at each level, node, CH, and BS, and only sends trusted packets to the cloud, while untrusted packets are discarded before being sent to the cloud. Simulation results show that BATEM sends approximately 95% of all trusted and untrusted packets to the cloud per node. Although LTEM transmits fewer packets than BATEM, each node transmits about 70% of the packets, as shown in Figure 6. As a result, 30% of packets avoid transmission to the cloud because they are not trusted and are dropped. Because LTEM detects untrusted packets and drops them before transmission, fewer packets are transmitted, reducing energy consumption and extending the system's life.

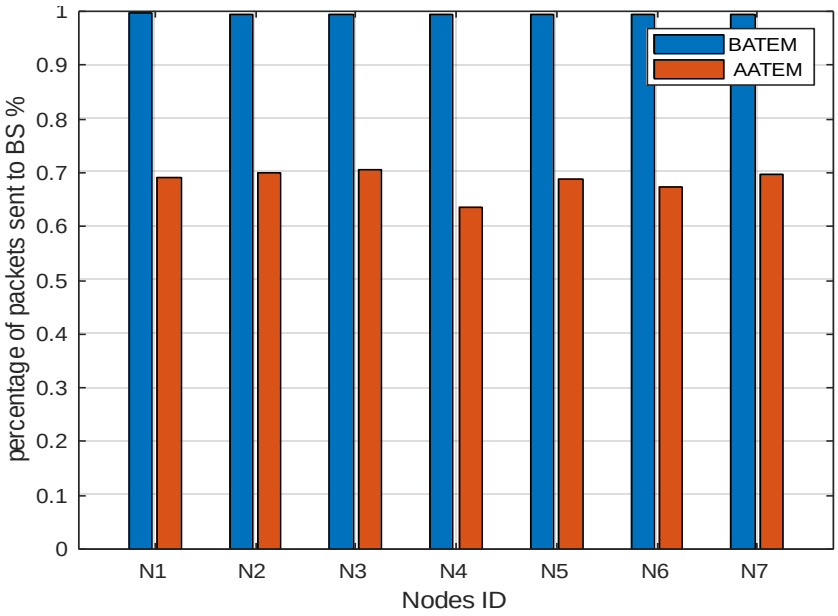

FIGURE 6. Packet transmission rate per node in BATEM and LTEM

Figure 7 shows the total energy consumption of all nodes in LTEM is 2.800J less than the 3.800J consumed by the BATEM model. Therefore, LTEM saves approximately 1.200J of energy compared to BATEM, which only saves 0.200J, as shown in Figure 8.

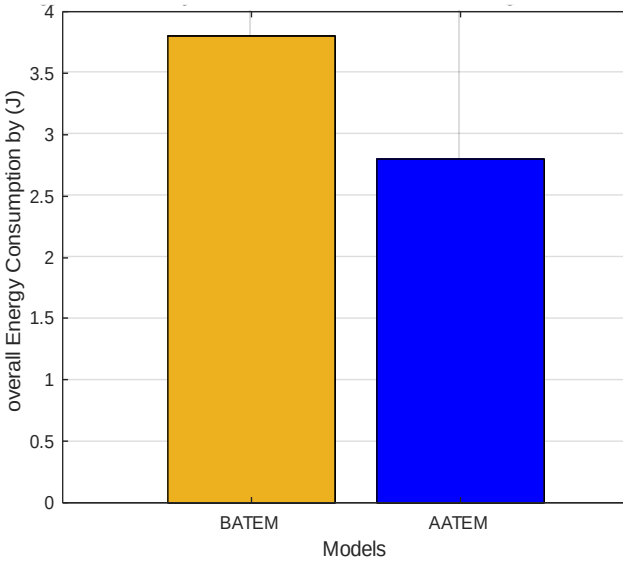

FIGURE 7. Total energy consumed by BATEM and LTEM

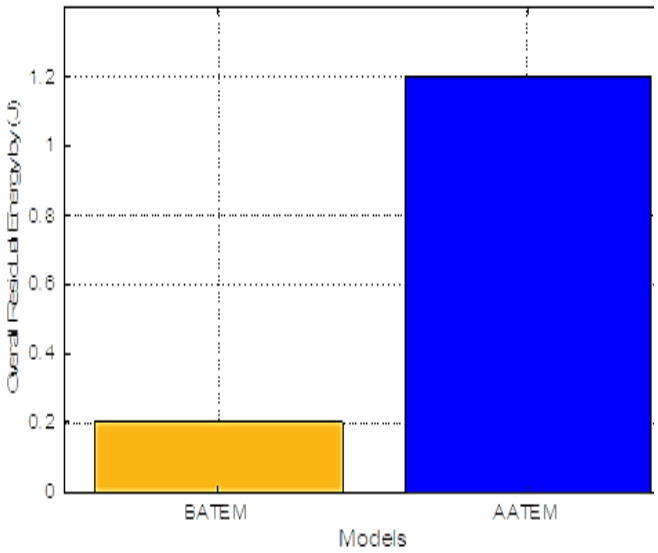

FIGURE 8. Total residual energy for BATEM and LTEM

2. SECOND SCENARIO

The LTEM is evaluated based on different BS, Cluster Head, and node levels in this scenario. The packet evaluation level impacts the node's energy consumption, as mentioned in [32]. To demonstrate that the LTEM first evaluated the data packet at BS (Eval_BS), then we evaluated the packet at the BS and CH (Eval _CH_ BS). Lastly, we evaluated the packets at node, CH, and BS (Eval_N_CH_BS). The simulation results show each model has an overall detection rate of 30% for untrusted packets, which is the same as that of injection errors, as shown in Figure 9. However, the difference was in energy consumption. The LTEM (Eval_N_CH_BS) consumes less energy

compared to other models, about 0.59J, while (Eval_CH_BS) and (Eval_BS) consumed about 0.63J and 0.71J, respectively, as shown in Figure 10.

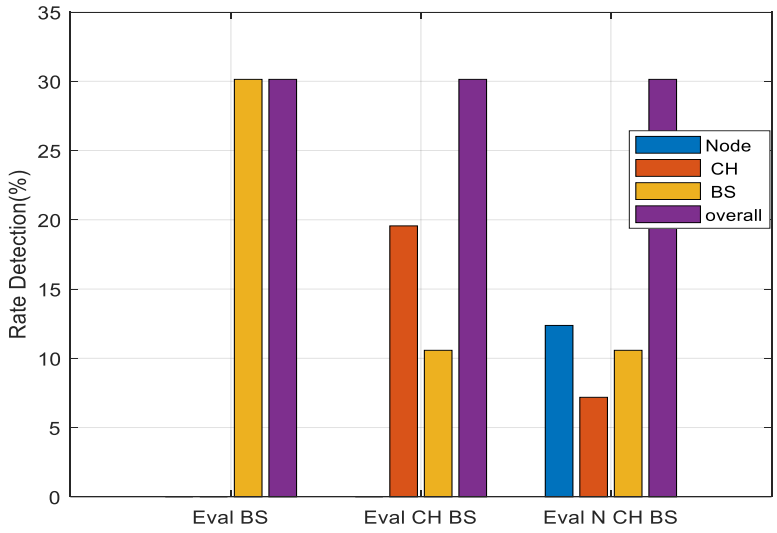

FIGURE 9. Percentage of untrusted packets detected by the LTEM at different levels of nodes, CH and BS

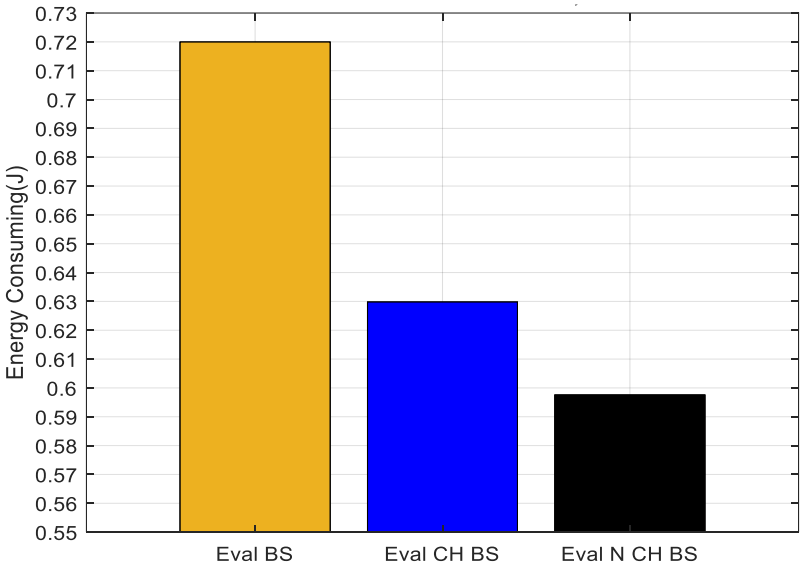

FIGURE 10. Total energy consumption of the LTEM to evaluate packets at different levels of nodes, CH and BS

This is because the LTEM (Eval_N_CH_BS) detects untrusted packets at the node level from the very beginning at the node level and avoids transmitting them to CH, which leads to reduced energy consumption. Therefore, the LTEM (Eval_N_CH_BS) saves more energy compared to other models by about 3.40J, while Eval_CH_BS and Eval_BS models consumed about 3.36J and 3.28J, respectively, as shown in Figure 11. Based on the above, Table 4 shows the results of the LTEM at different levels of nodes CH and BS.

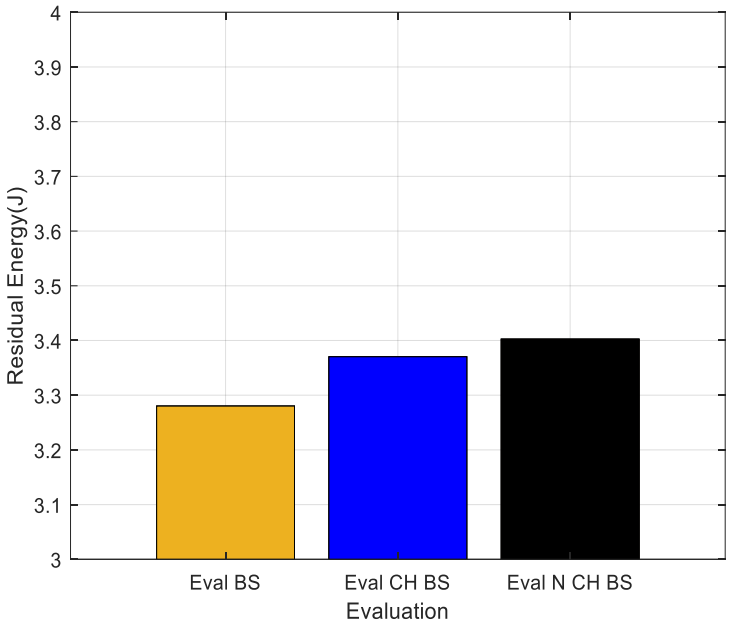

FIGURE 11. Residual energy of the LTEM at different levels of nodes, CH and BS

Table 4. Result of the LTEM at different levels of nodes CH and BS

Evaluate Models	Eval_ BS	Eval _CH _BS	Eval _N _CH _BS
Detect_at _N	0	0	62
Detect_at_CH	0	97	35
Detect_at_BS	150	53	53
Detect overall untrusted packets	150	150	150
Rate Detection	1	1	1
Energy Consuming	0.71849	0.63069	0.59846
Rate of Energy Consuming (%)	0.17962	0.15767	0.14961
Residual Energy	3.2815	3.3693	3.4015
Rate of Residual Energy (%)	0.82038	0.84233	0.85039

3. THIRD SCENARIO

Three main factors need to be considered in the evaluation process to perform a comprehensive evaluation: data packet, node behavior, and energy factor. Previous research [10-22] found that most of the existing trust evaluation models mainly focus on node behavior without adequately considering the trustworthiness of the data packet. However, the data evaluated is very important to ensure the data packet is trusted. Therefore, a trust model is needed to assess both node behavior and data packet simultaneously. In addition, most trust models do not consider energy in the evaluation processes shown in Table 5. Hence; the LTEM considers three factors: data packet, node behavior, and energy factor. The performance of the LTEM is compared with different models to evaluate its performance. The first model is the Data Aggregation Techniques of WSN using the External Mobile Elements (DAME) [33], the second model is the Trust-Evaluation Model with Entropy-Based Weight Assignment for Malicious Node Detection in Wireless Sensor Networks (EWMN) [25], the third model is Trust Model of Wireless Sensor Networks and Its Application in Data Fusion (TMDF) [22], and the last model is An Efficient Dynamic Trust-Evaluation Model for Wireless Sensor Networks (DTEM) [23]. Each of these models evaluated the packet and established the trust value based on some factors related to either the data packet, node behavior, or energy factor. As presented in Table 5, the evaluation in DAME is based on a data packet, while (EWMN) is based on node behavior. This model (TMDF) considers both data packet and node behavior but does not consider the energy factor. On the other hand, DTEM is evaluated based on node behavior and energy factors without considering the data packet. Hence, the LTEM considers data packets, node behavior, and energy factors.

Table 5. Comparison between the LTEM and other models

Models	Data of Node	Behavior of Node	Energy Factor
DAME	✓	×	×
EWMN	×	✓	×
TMDF	✓	✓	×
DTEM	×	✓	✓
LTEM	✓	✓	✓

The LTEM is evaluated with other models regarding untrusted-packet detection rate, energy consumption, and node-saving energy. The packets of 500 are selected from the dataset as samples, and 30% of them are randomly injected with different types of errors. The simulation results are shown in Figure 12. This shows that the LTEM has the highest detection rate (100%), while the detection rates of other models, DAME, EWMN, TMDF, and DTEM, are 42%, 31%, 73%, and 58% respectively. The reason is that during packet evaluation, the LTEM considers all factors: data packet, node behavior, and energy, while other models only consider one or two of them.

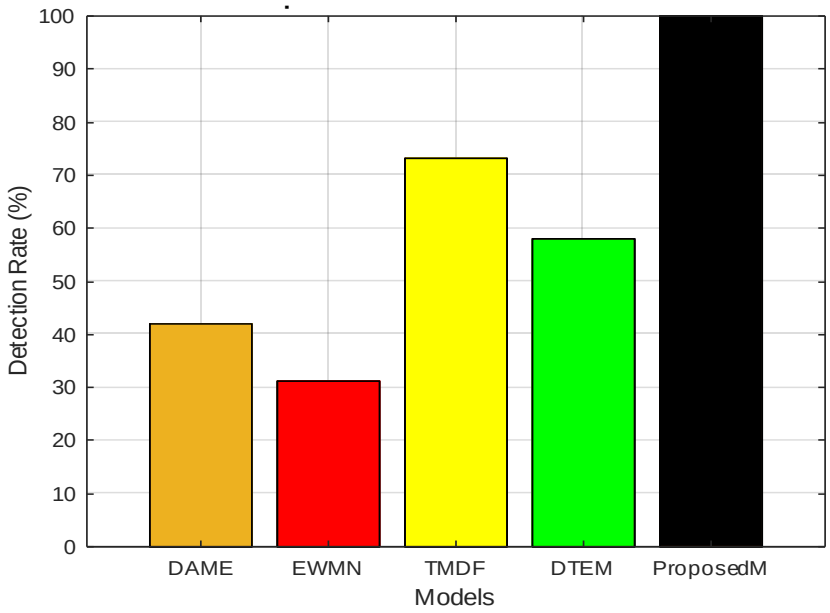

FIGURE 12. Detection rate of untrusted packets for the LTEM and other models DAME, EWMN, TMDF, and DTEM

Since most of the energy is consumed during packet transmission, about 80%, as mentioned in [10, 34, 35], then when the number of detected untrusted packets increases, the number of transmitted packets decreases. As a result, energy consumption decreases. Then, the LTEM detected untrusted packets the most. It consumed less energy, about 0.59J, compared to other models, namely DAME, EWMN, TMDF, and DTEM, which consumed about 0.65J, 0.67J, 0.61J, and 0.66J respectively, as shown in Figure 13. As a result, the energy saving rate for the LTEM is 3.40J higher than other models. In contrast, DAME, EWMN, TMDF, and DTEM models are 3.34J, 3.32J, 3.38J, and 3.33J, respectively, as illustrated in Figure 14. In general, the LTEM showed the best performance compared to other models in terms of untrusted packet detection, energy consumption, and saving energy.

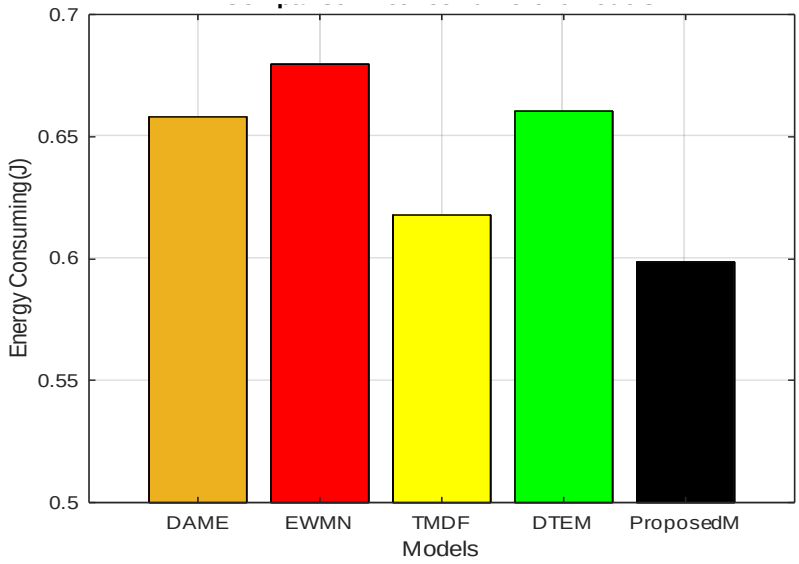

FIGURE 13. Total energy consumption of the LTEM and other models (unit in J)

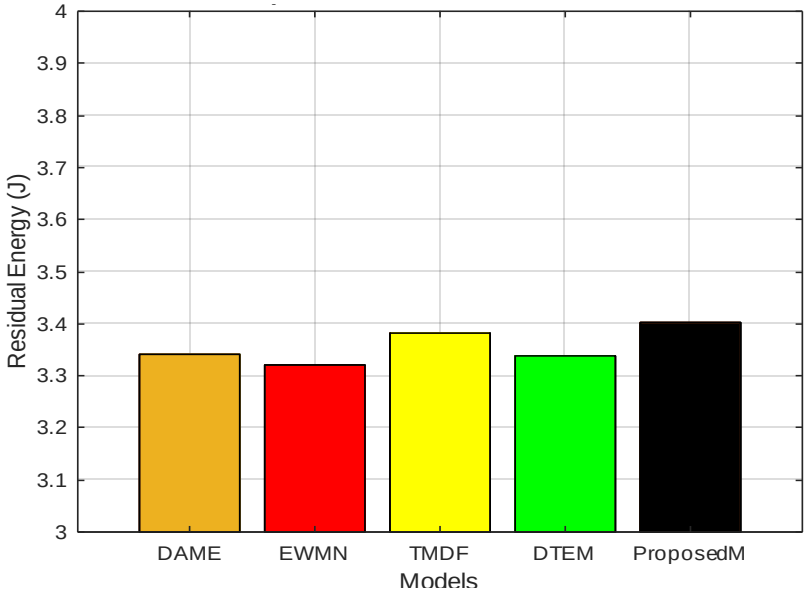

FIGURE 14. Residual energy of the LTEM and other models (unit in J)

4. FOURTH SCENARIO

Different cases are conducted to evaluate the accuracy of the detected untrusted packets of the LTEM and to test whether or not the LTEM can detect all untrusted packets. It was applied in one node with different samples (500, 1000, 1500, and 2000 packets) injected with varying error percentages to evaluate the accuracy. Table 6 summarizes the accuracy of the LTEMs in Case 1, Case 2, Case 3, Case 4, and Case 5. From the Table 6, the untrusted packets are detected in the same way as those injected in each case, which means the accuracy rate is 100%, except for Case 5. In this case, the accuracy rate is 99% due to the increase in the percentage of injected errors, which increases to 30%, as mentioned in [36]; when the percentage of error increases, the accuracy of detecting the malicious node decreases. However, even with the increased error percentage, the average accuracy of the LTEM is still as high as 99%. This result shows that the performance of the LTEM is outstanding.

Table 6. The average accuracy of the LTEM for several samples

Case	Sample	Injected Errors	Actual Detected Error	Accuracy
Case 1	500 packets	(10%) /50	50	100%
Case 2	1000 packets	(10%) /100	100	100%
Case 3	1500 packets	(10%) /150	150	100%
Case 4	2000 packets	(10%) /200	200	100%
Case 5	2000 packets	(30%) /600	599	99.8%
Avg				499.8/5=99%

5. FIFTH SCENARIO

In the fourth scenario, several samples were selected to evaluate the accuracy of the LTEM. However, in this scenario, several nodes (N1, N2, N3, N4, N5, and N6) were selected to evaluate the accuracy of the LTEM. The sample size per node is 100 packets injected with different error percentages. N1 and N2 are injected with 10% untrusted packets, N2 and N3 with 20% untrusted packets, and N5 and N6 with 30% untrusted packets). It can be seen from Table 7 the number of untrusted packets detected is the same as that of injected errors. 10% are detected by N1 and N2, 20% are detected by N3 and N4, and 30% are detected by N5 and N6. Therefore, the accuracy of the LTEM, in this scenario, is 100%.

Table 7. LTEM untrusted packet detection rates in N1 to N6

Node_ ID	Rate Detected
N1	10%
N2	10%
N3	20%
N4	20%
N5	30%
N6	30%

Table 8 summarizes the average accuracy of the LTEM for several nodes. It is clear from the Table 8 that the nodes N1, N2, N3, N4, N5, and N6 all injected errors. Therefore, the average accuracy of the LTEM, in this case, is 100%.

Table 8. The average accuracy of the LTEM for several nodes

Sample	Node ID	Percentage % of injected errors	Actual Detected Error	Accuracy
100 packets for each node	N1	10% errors (10 packets)	10	100%
	N2	10% errors (10 packets)	10	100%
	N3	20% errors (20 packets)	20	100%
	N4	20% errors (20 packets)	20	100%
	N5	30% errors (30 packets)	30	100%
	N6	30% errors (30 packets)	30	100%
Avg				600/6=100%

6. SIXTH SCENARIO

The LTEM is applied to one cluster in the fifth scenario to evaluate its accuracy. However, in this scenario, all nodes in the network, including Cluster 1, Cluster 2, Cluster 3, Cluster 4, and Cluster 5, are used to evaluate the accuracy of the LTEM. Table 9 shows the average accuracy of the LTEM for each cluster injected with different

percentages of errors: 10%, 15%, 20%, 25%, and 30% for Cluster 1, Cluster 2, Cluster 3, Cluster 4, and Cluster 5 respectively. The detection rate of the untrusted packets in Cluster 1, Cluster 2, Cluster 3, and Cluster 5 is the same as that of the injected rate. However, Cluster 4 was injected with a 25% error, and the actual detection was 24%. Therefore, the average accuracy of applying the LTEM to each cluster is 99%. Figure 15 shows the detection rate of the untrusted packets for Cluster 1, Cluster 2, Cluster 3, Cluster 4, and Cluster 5.

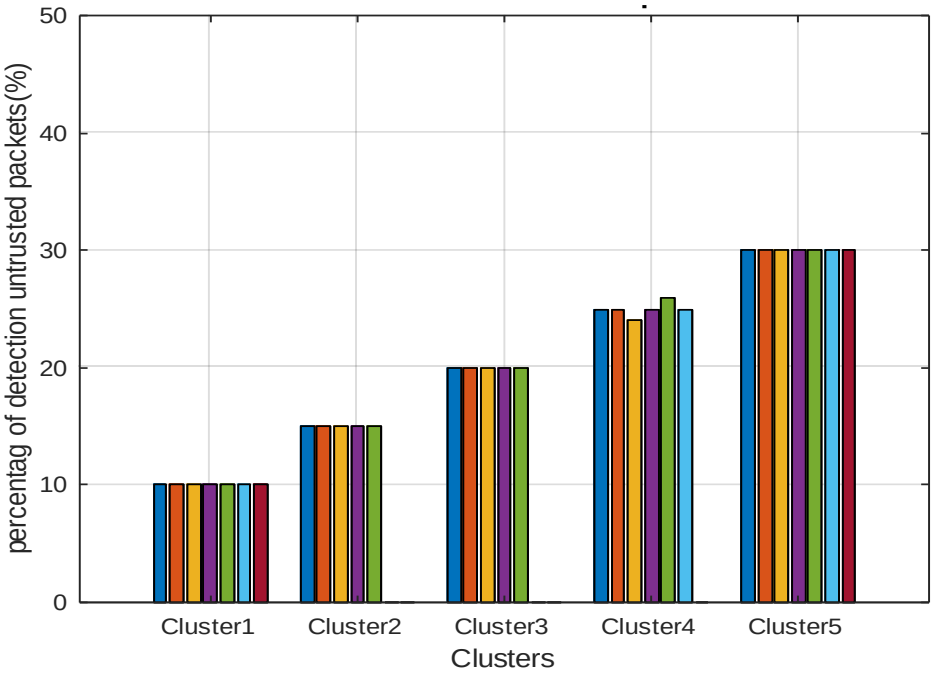

FIGURE 15. Detection rate of untrusted packets in each cluster

Table 9. Average accuracy of the LTEM for each cluster injected with different percentages of error nodes

Sample	Cluster	Injected Errors	Actual Detected Error	Accuracy
100 packets for each node	Cluster 1	10% errors	10%	100%
	Cluster 2	15% errors	15%	100%
	Cluster 3	20% errors	20%	100%
	Cluster 4	25% errors	24.8%	99%
	Cluster 5	30% errors	30%	100%
Avg				499/5=99.8%

7. COMPUTE CONFIDENCE LEVEL

Increasing the errors in the node indicates that the node may have faults. Therefore, the administrator should be careful about this node and take the necessary action to avoid unexpected errors, such as isolating or changing the faulty node. The LTEM evaluated the node based on the trust value to help the administrator know the node's status. Therefore, a cluster with multiple nodes (N1, N2, N3, N4, N5, N6, and N7) is selected to show the trust value for each node. The number of samples for each node is 100 packets, injected with different percentages of errors. Equation (1) calculates the nodes' trust value/confidence level [10]. The node has three statuses: either normal when ($TV == 1$), suspected when ($1 > TV >= 0.5$), or abnormal when ($TV < 0.5$) [10]. Figure 16 shows the trust value for each node, while Table 10 presents the status of each node.

Table 10. Status of nodes 1 to 7

Node_ID	Trust_Value	Status
N1	0.8	Suspected
N2	0.9	Suspected
N3	0.7	Suspected
N4	0.8	Suspected
N5	0.45	Abnormal
N6	0.55	Suspected
N7	1	Normal

As seen in Figure 16, the trust value for N7 = 1. Therefore, the status of this node is Normal. While N1, N2, N3, N4, and N6 have trust values between 1 and 0.5, the status for these nodes is suspected. Since the trust value for N5 is less than 0.5, the status of this node is abnormal. So, the administrator should care about this node and take necessary action, such as isolating or changing the abnormal node to avoid unexpected errors in the IoT application.

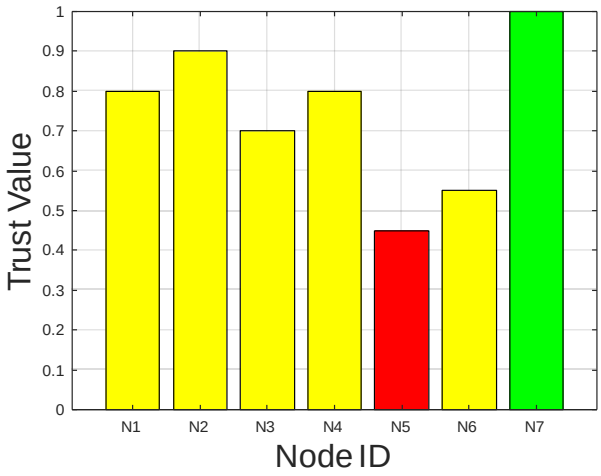

FIGURE 16. Trust values for node1 to node7

The Trust Value or Confidence Level is represented by Trust Value/ Confidence Level $= 1 - E\backslash E +$ Cquantifies the trustworthiness of a system based on the ratio of trusted to untrusted packets, where E is the number of untrusted packets and C is the number of trusted packets. This measure indicates a high trust value, close to 1, when untrusted packets are minimal compared to trusted ones, implying a reliable and secure system. Conversely, a low trust value, near 0, arises when untrusted packets are prevalent, signaling potential reliability issues. The formula subtracts the fraction of untrusted packets from 1 to yield the proportion of trusted packets, thereby providing a clear and straightforward metric for assessing the confidence level in various applications, such as network security, where the integrity of data transmission is critical.

V. CONCLUSION

IoT technology involves various tasks that achieve smart service goals, enabling devices to interact with the physical world. However, the continuous advancement of technology has led to more attack mechanisms that exploit the heterogeneity of IoT, raising trust issues. Trust assessment models are critical for identifying untrustworthy behaviors and objects and reducing uncertainty and potential risks. Most trust models focus on node behavior and ignore packet aspects that may affect the trustworthiness of an application. LTEM combines packet and node behavior evaluation to enhance application reliability. However, this approach affects energy consumption because IoT nodes have limited battery life. LTEM considers energy factors to reduce energy usage. The study employs eight trust metrics to determine the trustworthiness of a packet, covering packet, node

behavior, and energy factors. This comprehensive evaluation can detect many untrusted packets, thereby reducing energy consumption. LTEM evaluation occurs at three levels: node, cluster head (CH), and base station (BS). This multi-level evaluation enhances application reliability and reduces energy consumption by dropping untrusted packets before transmission to the CH and BS. Simulation results show that LTEM outperforms other models in detecting untrusted packets while consuming less energy. Its accuracy is exceptionally high, with an average accuracy of 99%. Future work aims to enhance the model using artificial intelligence (AI) and deep learning techniques.

`Notation	**Description**
Temp	Temperature Value Read by Sensor
Max_R	Maximum Range of the Temperature Sensor
Min_R	Minimum Range of the Temperature Sensor
Tr	Current Time of Receiving the Packet by the Reader
Tt	Current Time of Sending Tag ID
&T	Time Threshold
Temp(C)	Current Temperature Value Read by Sensor
Temp(p)	Previous Temperature Value Read by Sensor
Tag_Id(c)	Current Tag ID Scan by the Reader
Tag_Id(p)	Previous Tag ID Scan by the Reader
D_N_CH	Delay Between Node and Cluster Head
D_ CH_BS	Delay Between Cluster Head and BS
D_Thr	Delay Threshold
X	Tag ID that is Scanned by the Reader
X*	Tag ID that is Saved in the BS at the Registration Phase

Funding statement

This research was supported by Universiti Tun Hussein Onn Malaysia (UTHM) through Tier 1 (vot Q413), and Ministry of Higher Education of Malaysia (MOHE) through Fundamental Research Grant Scheme (FRGS) under Grant Vot K216 and Reference Code: FRGS/1/2019/ICT04/UTHM/03/2.

Author contribution

Somya, Hazalila, and Nayef Alduais contributed to the initial drafting of the paper. Hazalila and Nayef also reviewed and edited the manuscript. Noor Zuraidin and Salama provided critical review and feedback on the paper.

Conflict of Interest

The authors declare no conflict of interest.

Acknowledgements

This research was supported by Universiti Tun Hussein Onn Malaysia (UTHM) through Tier 1 (vot Q413), and Ministry of Higher Education of Malaysia (MOHE) through Fundamental Research Grant Scheme (FRGS) under Grant Vot K216 and Reference Code: FRGS/1/2019/ICT04/UTHM/03/2.

REFERENCES

1. Alghofaili, Y., & Rassam, M. A. (2023). A Dynamic Trust-Related Attack Detection Model for IoT Devices and Services Based on the Deep Long Short-Term Memory Technique. *Sensors*, *23*(8), 3814.
2. Zheng, G., Gong, B., & Zhang, Y. (2021). Dynamic network security mechanism based on trust management in wireless sensor networks. *Wireless Communications and Mobile Computing*, *2021*(1), 6667100.
3. Alghofaili, Y., & Rassam, M. A. (2022). A trust management model for IoT devices and services based on the multi-criteria decision-making approach and deep long short-term memory technique. *Sensors*, *22*(2), 634.

4. Lakhan, A., Mohammed, M. A., Zebari, D. A., Abdulkareem, K. H., Deveci, M., Marhoon, H. A., ... & Martinek, R. (2024). Augmented iot cooperative vehicular framework based on distributed deep blockchain networks. *IEEE Internet of Things Journal*.
5. Talbi, S., & Bouabdallah, A. (2020). Interest-based trust management scheme for social internet of things. *Journal of Ambient Intelligence and Humanized Computing*, *11*(3), 1129-1140.
6. Elkhodr, M., & Alsinglawi, B. (2020). Data provenance and trust establishment in the Internet of Things. *Security and Privacy*, *3*(3), e99.
7. Abdulrahman, S. M., Hani, A. A., Zeebaree, S. R., Asaad, R. R., Majeed, D. A., Sallow, A. B., & Ahmad, H. B. (2024). INTELLIGENT HOME IOT DEVICES: AN EXPLORATION OF MACHINE LEARNING-BASED NETWORKED TRAFFIC INVESTIGATION. *Jurnal Ilmiah Ilmu Terapan Universitas Jambi*, *8*(1), 1-10.
8. Abou-Nassar, E. M., Iliyasu, A. M., El-Kafrawy, P. M., Song, O. Y., Bashir, A. K., & Abd El-Latif, A. A. (2020). DITrust chain: towards blockchain-based trust models for sustainable healthcare IoT systems. *IEEE access*, *8*, 111223-111238.
9. Ahmed, A. I. A., Ab Hamid, S. H., Gani, A., & Khan, M. K. (2019). Trust and reputation for Internet of Things: Fundamentals, taxonomy, and open research challenges. *Journal of Network and Computer Applications*, *145*, 102409.
10. Alduais, N. A. M., Abdullah, J., & Jamil, A. (2019). RDCM: An efficient real-time data collection model for IoT/WSN edge with multivariate sensors. *IEEE Access*, *7*, 89063-89082.
11. Mohammed, Z. K., Mohammed, M. A., Abdulkareem, K. H., Zebari, D. A., Lakhan, A., Marhoon, H. A., ... & Martinek, R. (2024). A metaverse framework for IoT-based remote patient monitoring and virtual consultations using AES-256 encryption. *Applied Soft Computing*, *158*, 111588.
12. Rizwanullah, M., Singh, S., Kumar, R., Alrayes, F. S., Alharbi, A., Alnfiai, M. M., ... & Agrawal, A. (2022). Development of a model for trust management in the social internet of things. *Electronics*, *12*(1), 41.
13. Chen, R., & Guo, J. (2014, May). Dynamic hierarchical trust management of mobile groups and its application to misbehaving node detection. In *2014 IEEE 28th international conference on advanced information networking and applications* (pp. 49-56). IEEE.
14. Awan, K. A., Din, I. U., Zareei, M., Talha, M., Guizani, M., & Jadoon, S. U. (2019). Holitrust-a holistic cross-domain trust management mechanism for service-centric Internet of Things. *Ieee Access*, *7*, 52191-52201.
15. Lingda, K., Feng, Z., Yingjie, Z., Nan, Q., Dashuai, L., & Shaotang, C. (2021, February). Evaluation method of trust degree of distribution IoT terminal equipment based on information entropy. In *Journal of Physics: Conference Series* (Vol. 1754, No. 1, p. 012108). IOP Publishing.
16. Yu, Y., Jia, Z., Tao, W., Xue, B., & Lee, C. (2017). An efficient trust evaluation scheme for node behavior detection in the internet of things. *Wireless Personal Communications*, *93*, 571-587.
17. Zhang, W., Zhu, S., Tang, J., & Xiong, N. (2018). A novel trust management scheme based on Dempster–Shafer evidence theory for malicious nodes detection in wireless sensor networks. *The Journal of Supercomputing*, *74*, 1779-1801.
18. Ahmed, A., Bakar, K. A., Channa, M. I., Haseeb, K., & Khan, A. W. (2015). TERP: A trust and energy aware routing protocol for wireless sensor network. *IEEE Sensors Journal*, *15*(12), 6962-6972.
19. Mon, S. F. A., Winster, S. G., & Ramesh, R. (2022). Trust model for IoT using cluster analysis: A centralized approach. *Wireless Personal Communications*, *127*(1), 715-736.
20. Kowshalya, A. M., & Valarmathi, M. L. (2017). Trust management in the social internet of things. *Wireless Personal Communications*, *96*, 2681-2691.
21. Han, G., Jiang, J., Shu, L., Niu, J., & Chao, H. C. (2014). Management and applications of trust in Wireless Sensor Networks: A survey. *Journal of Computer and System Sciences*, *80*(3), 602-617.
22. Chen, Z., Tian, L., & Lin, C. (2017). Trust model of wireless sensor networks and its application in data fusion. *Sensors*, *17*(4), 703.
23. Ye, Z., Wen, T., Liu, Z., Song, X., & Fu, C. (2017). An efficient dynamic trust evaluation model for wireless sensor networks. *Journal of Sensors*, *2017*(1), 7864671.
24. Jiang, J., Han, G., Wang, F., Shu, L., & Guizani, M. (2014). An efficient distributed trust model for wireless sensor networks. *IEEE transactions on parallel and distributed systems*, *26*(5), 1228-1237.
25. Yin, X., & Li, S. (2019). Trust evaluation model with entropy-based weight assignment for malicious node's detection in wireless sensor networks. *EURASIP Journal on Wireless Communications and Networking*, *2019*, 1-10.
26. MOhammed Alduais, N. A. (2019). *An efficient real-time data collection model for multivariate sensors in internet of things (IOT) applications* (Doctoral dissertation, Universiti Tun Hussein Onn Malaysia).
27. Alqarni, A., Alabdulhafith, M., & Sampalli, S. (2014). A proposed RFID authentication protocol based on two stages of authentication. *Procedia Computer Science*, *37*, 503-510.
28. Mubarak, M. F., & Yahya, S. (2011, March). A critical review on RFID system towards security, trust, and privacy (STP). In *2011 IEEE 7th International Colloquium on Signal Processing and its Applications* (pp. 39-44). IEEE.
29. Ferrari, P., Flammini, A., Sisinni, E., Rinaldi, S., Brandão, D., & Rocha, M. S. (2018). Delay estimation of industrial IoT applications based on messaging protocols. *IEEE Transactions on Instrumentation and Measurement*, *67*(9), 2188-2199.
30. Feng, R., Che, S., Wang, X., & Yu, N. (2013). Trust management scheme based on DS evidence theory for wireless sensor networks. *International Journal of Distributed Sensor Networks*, *9*(6), 948641.
31. Ferrari, P., Flammini, A., Sisinni, E., Rinaldi, S., Brandão, D., & Rocha, M. S. (2018). Delay estimation of industrial IoT applications based on messaging protocols. *IEEE Transactions on Instrumentation and Measurement*, *67*(9), 2188-2199.
32. Feng, R., Xu, X., Zhou, X., & Wan, J. (2011). A trust evaluation algorithm for wireless sensor networks based on node behaviors and ds evidence theory. *Sensors*, *11*(2), 1345-1360.
33. Ali, B. A., Abdulsalam, H. M., & AlGhemlas, A. (2018). Trust based scheme for IoT enabled wireless sensor networks. *Wireless Personal Communications*, *99*, 1061-1080.
34. Bouguera, T., Diouris, J. F., Chaillout, J. J., Jaouadi, R., & Andrieux, G. (2018). Energy consumption model for sensor nodes based on LoRa and LoRaWAN. *Sensors*, *18*(7), 2104.
35. Alduais, N. A. M., Abdullah, J., Jamil, A., Audah, L., & Alias, R. (2017, March). Sensor node data validation techniques for realtime IoT/WSN application. In *2017 14th International Multi-Conference on Systems, Signals & Devices (SSD)* (pp. 760-765). IEEE.
36. Li, X., Zhou, F., & Du, J. (2013). LDTS: A lightweight and dependable trust system for clustered wireless sensor networks. *IEEE transactions on information forensics and security*, *8*(6), 924-93