International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 2s
DOI: https://doi.org/10.17762/ijritcc.v10i2s.5907
***Article Received**: 14 October 2022 **Revised**: 09 November 2022 **Accepted**: 20 December 2022*

Intelligent Trust based Security Framework for Internet of Things

Kajol Rana[1], Dr. Ajay Vikram Singh[2], Dr. P. Vijaya[3]
[1]Kajolrana27@gmail.com [2]avsingh1@amity.edu [3]vijaya@waljat.net
[1]Amity University, [2]Amity University, [3]Waljat College of Applied Sciences

Abstract
Trust models have recently been proposed for Internet of Things (IoT) applications as a significant system of protection against external threats. This approach to IoT risk management is viable, trustworthy, and secure. At present, the trust security mechanism for immersion applications has not been specified for IoT systems. Several unfamiliar participants or machines share their resources through distributed systems to carry out a job or provide a service. One can have access to tools, network routes, connections, power processing, and storage space. This puts users of the IoT at much greater risk of, for example, anonymity, data leakage, and other safety violations. Trust measurement for new nodes has become crucial for unknown peer threats to be mitigated. Trust must be evaluated in the application sense using acceptable metrics based on the functional properties of nodes. The multifaceted confidence parameterization cannot be clarified explicitly by current stable models. In most current models, loss of confidence is inadequately modeled. Esteem ratings are frequently mis-weighted when previous confidence is taken into account, increasing the impact of harmful recommendations.

In this manuscript, a systematic method called Relationship History along with cumulative trust value (Distributed confidence management scheme model) has been proposed to evaluate interactive peers trust worthiness in a specific context. It includes estimating confidence decline, gathering & weighing trust parameters and calculating the cumulative trust value between nodes. Trust standards can rely on practical contextual resources, determining if a service provider is trustworthy or not and does it deliver effective service? The simulation results suggest that the proposed model outperforms other similar models in terms of security, routing and efficiency and further assesses its performance based on derived utility and trust precision, convergence, and longevity.

Keywords: IoT**,** Trust Model**,** Security**,** Privacy Protection

I. INTRODUCTION

The Internet-of-Things concept is becoming a reality as a global network for connecting devices, computers, routers, sensors, and any other type of entity that interacts directly or indirectly. It can be thought of as a collection of autonomous machines that run on their platform, relying on existing Internet infrastructure and utilising various technologies such as radio frequency identification (RFID) [39] and sensor networks to remotely detect, track, locate, and manage objects [20]. Furthermore, each smart entity has a unique identifier and specific simple computational skills, such as processing, networking, and service discovery. Current Internet of Things (IoT) research inherently involves large-scale cooperation and interoperability between multiple devices and networks. Consequently, system protection and data transmissions across these devices have become even more critical and challenging to handle due to the diverse characteristics of heterogeneous resources [16].

To overcome these problems, state-of-the-art techniques [4] and [14] have been used to protect the IoT platform and data exchange between these devices in a distributed architecture. [3] Still, it appears difficult to tolerate the comprehensive exploration of data from multiple categories and contexts. When many users and devices collaborate to pool resources and provide services, new lightweight, intelligent, and collaborative context-based distributed confidence management protection has proven to be a prominent and fascinating approach for collaborative IoT applications [25].

Today, the IoT comprises platforms and products offered by various emerging vendors, as they are not well acquainted with the remaining IoT customers. A confidence assessment method is required in these cases to determine whether an evolving customer's service is of high quality [37]. A more accurate method of calculating trust is to calculate the cumulative trust value by measuring the various nodes with the assistance of their peers, who connect to each other, resulting in the levying of numerous security threats. Confidence is abstract and multifaceted in the sense of the deployment of nodes. The Confidence Management Scheme offers steps and processes for determining the

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 2s
DOI: https://doi.org/10.17762/ijritcc.v10i2s.5907
***Article Received**: 14 October 2022 **Revised**: 09 November 2022 **Accepted**: 20 December 2022*

trustworthiness of virtual peers. The current built-in trust model computes trust value through recommendations and aggregations [31].

When trust fails, values decay. It affects the trust parameter collection, social interactions, and trust parameter weights among data communication or service consumption nodes. Trust parameters can be focused on contextual practical properties and timing characteristics to assess the service provider's efficiency. The developing model may provide a way to overcome the issues related to confidence mechanisms in the Dempster-Shafer theory [32]. Finally, the level of confidence and trust maturity are related to the extent to which an idea is adopted in social contexts, as well as the level of conviction that is used to weigh recommendations and the level of trust maturity for maintaining balance between the two nodes.

The remainder of the manuscript has been structured as follows: Section 2 points out the relevant studies on confidence modelling in IoT applications. Section 3 describes the proposed model based on "cumulated trust management for IoT applications." The simulation results for a specific case using the proposed model have been discussed in Section 4. In Section 5, we have figured out the conclusion and future scope of the presented manuscript.

II. RELATED WORK

This section has extensively studied the cutting-edge models listing the trust management system with appealing properties for IoT services. These are based on feedback and aggregation aspects to ensure secure peer interaction.

2.1 Trust management model based on fuzzy reputation for IoT

In this method, based on the fuzzy theory based on the IoT confidence [21, 27] and credibility model, node inactivity is identified by an interpretation of IoT services' unique features. A fuzzy approach has made it possible to trust the development of a feedback system focused on relationship mapping and forwarding action among neighbours [10]. The model presents a weighing factor for determining the relative value of the confidence-based advice and the end-to-end packet forwarding ratio. The important problems defined using other individuals' subjective opinions depict various issues in the collective IOT scenario. [34].

2.2 Using the recommendation function to compute trust

In the individual subjective opinions, the trust gap can be seen. Multi-level intermediary control could bridge the trust gap. In other words, without central intermediary control, trust is diffusely expressed. [9] Here, each node store sits on trusted values that have been previously defined and may also include partial suggestions from other nodes [17]. In partial trust, the degree of acceptance serves as a decision feature. This acceptability is seen as a change of view, modelled on social features. This work has been represented in tabular form in Table 1.

Table1: Notation Description of the Model Parameter

Symbols	Descriptions
tij	Trust Value of Node j Computed by Node I at current state and context
p	Trust Parameters of a node
$Bij \leftarrow k$	Trust Recommendation of Node j as per Node k given to Node I
w_i	Weight of the trust parameter for Node i
$T_{ij}(p)$	Trust Value of the Node i on the assessment of node j
t[C]	Trust over collaborating node

Assume that node i is in a node j connection session while also being in a session with another node k, each of which has certain assessments of the interacting node i. Node i will use the current partial trust value to initially change the partial trust scores of j before starting any further interactions. This is referred to as an "implied decision." In other words, it is the recommendation of node i given by node k to node j. [11] To put it another way, it is a recommendation on the creed function [6], which assesses the degree to which each node i accepts the recommendations of node k on node j. After node i is in direct connection with node j, k's indirect suggestions are easily rejected by node i. Node I's clear appraisal forms the foundation for the confidence ranking. In this case, trust decay will happen over a longer gap between interactions, as trust is a function of time. Similarly, in the concept of recommendation, belief in a high-trust node is high for the same subject.

Since trust is a dynamic concept, its value may change with each transmission. Belief function can measure the rate at which node i is able to embrace the advice of Node k for Node j. [38]

That is, the weight is allocated to the recommendation function as an implied assignment. The role of belief is given as in Eq.(1) where the Recommendation *B.jk* can be calculated.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 2s
DOI: https://doi.org/10.17762/ijritcc.v10i2s.5907
***Article Received**: 14 October 2022 **Revised**: 09 November 2022 **Accepted**: 20 December 2022*

$$B_{ij\leftarrow k} = 1 - \sum_{i=0}^{n}(T_{kj}(p) - T_{ij}(p)) \quad (1)$$

Thus, a malicious node has no hope of winning by giving bad advice or service to i, and its potential to influence (p) the decision is extremely restricted. It also offers successful protection against opportunistic or on-off attacks along with the trust-decay function [13, 40].

2.3 Trust computation using an aggregate function

The belief function, calculated using the recommendation function along with the confidence function (as an add-on function), defines how the cumulative trust value is applied to a node. [12] Furthermore, the function of a selected grouping is determined by the context of the relationship between the nodes. This manuscript employs a fully weighted approach [36]. Trust alerts are event-driven and only occur when nodes communicate with each other based on partial trust scores. This function implements a methodology for the calculation of multi-criteria confidence [35].

Trust over Collaborating Node is given by Eq.2:

$$t[C] = [t_{ij,}\ p, w, s, f, l] \forall_i\ j \in C \quad (2)$$

Where,

C represents the number of working nodes in the collaboration.

t_{ij} represents the Trust Score of node j computed by node i

prepresents set of parameters to access the trust such as p_1, p_2, p_3...p_n

w represents the weight on each parameter of node j such as $w_i(p_1)$, $w_i(p_2)$, $w_i(p_3)$...w_ip_n

s represents the set of trust value on each parameter such as $s_{ij}(p_1)$, $s_{ij}(p_2)$,$s_{ij}(p_3)$...$s_{ij}(p_n)$

f represents the function used for calculating cumulative trust value for each node f(w,s)[19]

2.4 Trust computation using cumulated Trust value

Cumulated trust is calculated in the preceding section by adding the value of trust to be given to each interconnected node. This combination is organised as a matrix, with the number of rows and columns equal to the number of nodes connected in a communication channel. [28] For example, suppose we have four nodes, N1, N2, N3, and N4, each with a different value relative to the others. The matrix will be developed as the matrix in Table 2, where Sum Col represents the sum of all the columns separately. As we can see in the table, node N2 has the highest value of trust. Because all nodes in the network inspect it, the node with the highest cumulative value of trust is chosen for data transmission. Since this method points out the most trusted node, it helps in the removal of confusion for selecting nodes for secure transmission [12].

In the event of a tie, the total of all scores is determined separately. The two tied nodes are now sum col there and sum rowicked, and the node with the highest trust value is chosen. A selected node is used as a transmitting node for packet forwarding. The matrix will be developed as shown in Table 3.

As it can be seen in Table 2, there is a tie in Sum Col between N2 and N4. So, the summation of all the rows is done separately and depicted by Sum Row, where Node N4 has the highest value of trust. Therefore, node N4 is selected for the task of forwarding the packets [33].

If there is still a tie, the system will choose one of the two people with the highest accumulated trust value at random [5].

Table 2: Matrix for cumulated Trust

Nodes	N_1	N_2	N_3	N_4
N_1	0	0.2	0.3	0.4
N_2	0.1	0	0.1	0.2
N_3	0.4	0.5	0	0.6
N_4	0.6	0.7	0.5	0
Sumcol	1.1	1.4	0.9	1.2

Table3: Matrix for Cumulated Trust for Tie Breaking

Nodes	N_1	N_2	N_3	N_4	SumRow
N_1	0	0.2	0.3	0.2	0.7
N_2	0.1	0	0.1	0	0.2
N_3	0.4	0.5	0	0.5	1.4
N_4	0.6	0.7	0.5	0.7	2.5
Sumcol	1.1	1.4	0.9	1.4	

III. PROPOSED MODEL

In this section, the comprehensive method referred to as a trust management model for the IoT is defined with the help of the cumulative trust value of nodes and a belief function to determine the trustworthiness of interactive peers. In other words, it uses the different rust values on the nodes to route packets to their destinations.

3.1 Definitions of Trust Entities

Trust Decay: It is a test of confidence in the operation of a temporal type in the past and present periods. Previous faith-based qualities in the facilities have eroded gracefully over time. The role of confidence decay should be provided by the decision-making mechanism [1].

Trust Composition: The management process should

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 2s
DOI: https://doi.org/10.17762/ijritcc.v10i2s.5907
***Article Received**: 14 October 2022 **Revised**: 09 November 2022 **Accepted**: 20 December 2022*

incorporate or assemble the trustee's objective properties (service quality, QoS, and security) and subjective properties (social and local) as trust conditions so that the trustee or decision-making process may make a well-informed decision [26].

Trust Convergence: The trust value t_{ik}, which the node I contains for node k. This value will be used as trust recommendation by node j for node i. This is a complex process in which a node with a higher trust value is also trusted by other nodes [2].

Trust Resilience: It is a measure of the willingness of the decision-making process to respond to moral changes in organisations or service improvement characteristics. It includes improving the relationship between malicious and supportive partners. In these circumstances, the confidence principles determined by the decision-making process remain correct and are rapidly convergent with the new realities on the ground [8].

Trust Score: Esteem can consist of one or more mutual confidence measures. Each confidence criterion can be assessed using either the quality of service (QoS) or the social contextual [15] assessment methods. The parameter used in the evaluation of an ODE is called partial confidence. Any confidence parameter can be applied by a trustee. Each trustee parameter has values that reflect its relative importance. Before being aggregated with other trust scores, half of the trust scores are weighted [24].

3.2 Trust Parameter

A trustee shall make a judgement based on several factors. The criteria may be either factual or subjective. Parameters shall be deemed objective (e.g., "These assets include contract pace, performance, job rate, proximity, service cost, partnering, et cetera. Subjective parameters (Eq. 4) [30] the trustee is assumed to value qualities such as dependability, cooperation, and friendliness. The confidence value of each peer would not yield the same outcomes for the trustee, even though they are all evaluated at the same time. It shall be granted as follows:

3.2.1Condition for Objective parameter

If (p is an objective parameter)

$$\text{Node } J \in C$$
$$S_{ij}(p_1) = S_{ij}(p_2) = S_{ij}(p_1) \quad (3)$$

3.2.2 Condition for Subjective parameter

If (p is a Subjective parameter)

$$\text{Node } J \in C$$
$$s_{ij}(p_1)=s_{ij}(p_2)=s_{ij}(p_3)=.....=s_{ij}(p_n) \quad (4)$$

Therefore, due to its improved robustness and latitude of application, the confidence model implicitly encompasses both QoS and social trust parameters. In this work, the choice of which parameters should be determined at the time of the calculation of C depends on the relationship context.

3.3 Trust Weight Computation

Trust weight calculation is done using the metric system. Metric weight determines the parameter value for trust's core calculation. Targeted metrics, such as working rates or network speed, are well defined and equally calculated by C, whereas the computational scale for subjective parameters is as good as node-to-node interaction. Node-to-node interaction. Based on subjective view points, the weight of each parameter is decided by each node interacting in an IO ecosystem. Confidence The standardisation method for determining trust scores depends on four variables:

– Value of past direct interactions.
– Value of past indirect interactions
– Value of Current direct interaction.
– Value of Current indirect interaction

The weights can be changed dynamically by the node under evaluation at any point during the session's stretch. Nodes may vary according to their set W record at any point, depending on their interpretation of each parameter's relative value. Because of the complexity, trust modelling can be done more effectively. The relative values of the trust factors that determine the extent to which a service or resource is trusted will differ significantly over time. Trust weight computation is given in Eq.5:

Trust weight computation is given as

$$w_i(p) \varepsilon [0,1] \forall i \in C, p \text{ and } \sum w_i=1 \quad (5)$$

Where,

Parameter under Consideration is Assigned $p_n = 1$

Parameter under Elimination is Assigned $p_n = 0$

Similarly, the relative importance of coordination requirements for each node will vary from session to session. The trust aggregation mechanism decides the score for each parameter to be aggregated. The computation of the trust score incorporates both the trustee's objective and arbitrary properties. Furthermore, the trust model renders the aggregation function unidentified until a relationship history is established and expressed as = (w, T). Weighted cumulative feature = w

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 2s
DOI: https://doi.org/10.17762/ijritcc.v10i2s.5907
***Article Received**: 14 October 2022 **Revised**: 09 November 2022 **Accepted**: 20 December 2022*

Trust Score using weighted sum function is given by Eq.6

$$T_{ij}=\sum_{x=1}^{n} w_i(p_x)*T_{ij}(p_x)\forall i,j\in C,px\in P \quad (6)$$

For the measurement of a trust value, a weighted score product or more complex characteristics such as the inference of Bayes [7, 22] or regression analysis [23] can be involved.

3.4 Trust Decay

The relationship between the nodes deteriorates gradually over time as a result of the confidence ranking; Tij, Nodei, and Nodej engagement tends to store, evaluate, and improve the trust relationship. The trust value depends on each trust parameter. Trust decay has been applied to each parameter separately. Trust is almost always eroded. For determining Node's behavior, it is dependent on the administrator's faith as well as the duration or number of contacts he has. In the absence of touch, the value of trust decays exponentially as trust decreases. The longer the protein's activity period, the higher its decay rate. New encounters shape the new views of the trustee. The trustee's confidence will always depend on new commitments. The previous meaning would no longer apply to confidence-based computing after new experiences.

The decay function follows an exponential pattern and is defined in the following mathematical equations (Eq. 7) based on this assumption.

$$(T_{ij}(p))_{0t\to t}=(T_{ij}(p))_0 * e^{-\lambda t} \quad (7)$$

where ((p)) 0t b is the current value of (vij(p))0 after time t for interactions between Nodes i and j, and t is the decomposition constant. The successful proportion of (p) that determines Tij (p) in the current session would be 0 after an appropriate number of contacts in an open session. At this point in the session, confidence has reached maturity.

3.5 Trust Maturity

Trust maturity is a conditional State that is achieved at a joint meeting in order to evaluate the trust scores of each node correctly, direct evaluations of relationships between the two nodes are sufficient. It is now believed that past node confidence has decayed completely and that suggestions are not used to measure the trust scores of each node. The node's interplay received direct assessment criteria. Maturity of trust is used to evaluate the future node session. At the beginning of a new *i-j* Node link session, the initial value of (*p*)=0.5 is. The key point between absolute mistrust (i.e. 0) and full confidence (i.e. 1) is considered. A neutral confidence attribute is presumed without information. It is also the default value for a node with no previous experience to calculate confidence scores. Models of trust computing are graded by secrecy, distribution, accumulation, changes and growth.

3.6 Cumulative Trust Based IoT Framework

The trust aggregate function employs the Dempster-Shafer theory. The stability of the node is evaluated by using some parameters. Dempster-Shafer theory [29] uses probability theory and weight computation on resultant values.

The architecture of the proposed framework is presented in Fig. 1. Algorithm 2 calculates the accumulated trust value for this selection of forwarding nodes.

On the belief computation, the trust value ranges between [0, 1]. In my opinion, the feature depends on the speed of uploading, the efficiency of effectively completing workloads, and the degree of safety and danger associated with teamwork on these parameters.

Effective completion rate, bandwidth use, and risk index are the metrics for determining confidence in the IoT system on the basis of context. In either scenario, it must be determined which practical requirements should act as trust parameters.

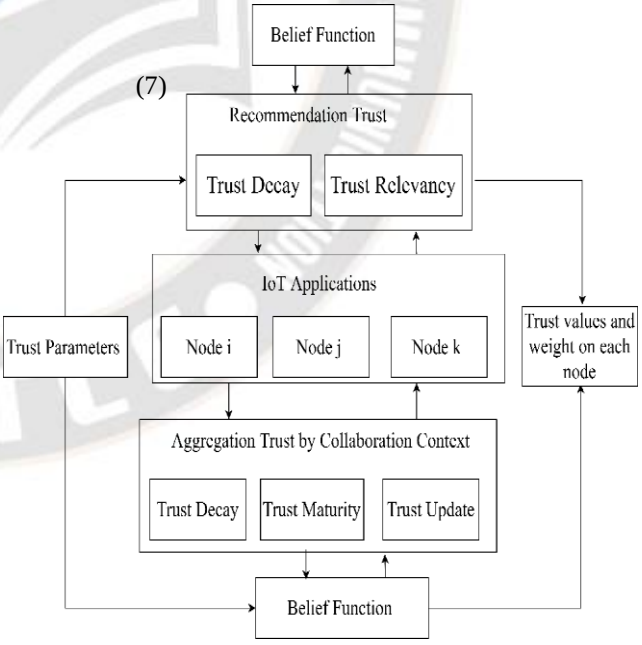

Fig.1: Architecture Diagram of the Proposed Architecture

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 2s
DOI: https://doi.org/10.17762/ijritcc.v10i2s.5907
***Article Received**: 14 October 2022 **Revised**: 09 November 2022 **Accepted**: 20 December 2022*

Algorithm 1 Trust Value Computation

1: **procedure** (Node, Trust Value)
2: Input: Node i, Node j, Node k, Successful Completion Rate, Risk Index, Bandwidth Usage
3: Output: Trust Value of Node j assessed by node i
4: Process
5: Compute Probability of node be trust on Past state
6: Probability of the node according to trust is given as
7: $p(S(t))=p(S(t)S(t-1),s(t-2),s(t-3),.....)$
8: Where $p(S(t)$ is Considered a set of propositions as a whole
9: As sign a set of proposition san interval [believe, plausibility] to constraint the degree of belief for each individual propositions in the set.
10: The belief measure be l is in **[**0,1**]**
11: 0–no support evidence for a set of propositions
12: 1–full support evidence for a set of propositions
13: The plausibility of p is pl (p)=1$bel(not(p))$
14: Range is a l so in**[**0,1**]**
15: Reflect how evidence of not (p) relates to the possibility for belief in p
16: *Bel* **(***not***(***p***))**=1: full support for not(p),no possibility for p
17: *Bel* **(***not***(***p***))**=0: no support fo not(p), full possibility for p

Algorithm2 Cumulated Trust Value Computation and selection of highest Trust value

1: **procedure** (Node, Trust Value)
2: Input: tij, number of nodes
3: Output: Trust Value of Node j assessed by node i
4: Process
5: Declare and initialize a multi-dimensional matrix a.
6: The number of rows and columns present in the array are equal to the number of nodes i.e.$i=j$
7: **for**<i=1ton>**do**
8: **for**<i=1ton>**do**
9: <do$C_{ij}=t_{ij}$>
10: Manage a variable sum Col to store the sum of elements in the specific column.
11: **for** <calculation of the sum of trust values in each column>**do**
12: < do Calculate the sum by adding elements present in a column>
13: Displays um Col
14: Repeat this for each column
15: Select the column with the highest value of Sum col, this value is the cumulated trust value
16: store the value in High sum col
17: Warding Packet Is Created On The node Sumcol is stored in High sumcol
18: In case of tie,
19: Calculate the sum by adding elements present in a row.
20: Display sum Row.
21: Repeat this for each row
22: Select the column with the highest value of Sum Row, this value is the cumulated trust value
23: store the value in High sumrow
24: Packet forwarding is done on the node whose SumRow is stored in High sumrow
25: **if** Case of tie still exists **then**
26: Transmitter can select node randomly from the nodes between which tie had occurred when considering SumRow.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 2s
DOI: https://doi.org/10.17762/ijritcc.v10i2s.5907
***Article Received**: 14 October 2022 **Revised**: 09 November 2022 **Accepted**: 20 December 2022*

3.7 Trust Architecture for Internet of Things framework

The downloading context application, which gradually evolves into the Internet of Things framework, has used the trust architecture generated in this section. Node's belief function is computed to enable trust among nodes in the IoT framework. It enables reliable data collection and mining of the data.

For an authorization protocol to work, a trusted infrastructure needs physical institutions, computing resources, and complex networking capabilities to send and receive data. Fig. 2 displays the architecture of the model. Trusted computing consists of near-by node details and formalised processing. It predicts that network traffic and controllers have been enabled with different roles, such as flows, scheduling, usability management, and separate applications. Finally, the data extraction is accomplished through a variety of credibility mechanisms.

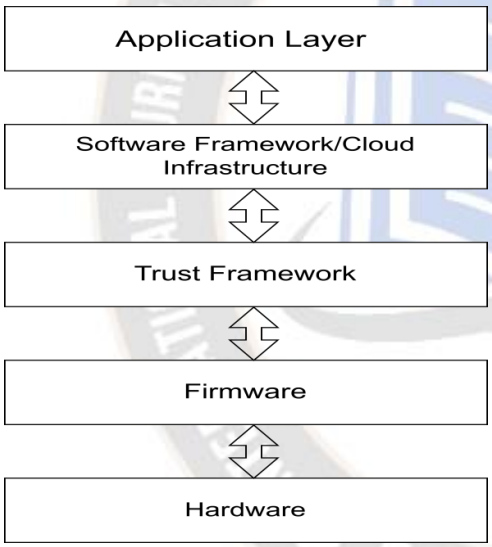

Fig.2: Trust Architecture for IoT framework

IV. SIMULATION RESULTS

We have tested our proposed algorithm with 100 nodes. The NS2 simulator has Algorithm 1, which has been used to validate the IoT nodes and their communication. Thurce and the destination nodes are fixed by us. The first algorithm addressed trust value initialization and hashing. Trust is based on the actual knowledge of the identified destination node. Node information from the trace file is collected and reviewed for confidentiality assessment. Conversely, for the same set of nodes, the trust value is calculated but randomly chosen. Node initiators have limited potential for discriminating the confidence threshold based on their preferences because, regardless of their trust scores, they can delete only 30% or less of available nodes. As a consequence, the effect of the trust model falls on acceleration. For each loop, it calculates new values. This mode is more sensitive and flexible to changes in node behaviour during the session. The model's trust results were compared to some real-world IoT system statuses [18]. The trust rate based on arbitrary nodal characteristics is used to determine the ground truth status. The truth's forward meaning is that the trustee is well aware of its behavior.

The proposed model accommodates changes in neurodegenerative behavior. The past of this interaction gives every contact a timeline. As a result, a relatively large number of interactions are needed to reliably determine trust values. As shown in Fig. 3, the reliability of the new confidence management software was calculated based on the current fuzzy system.

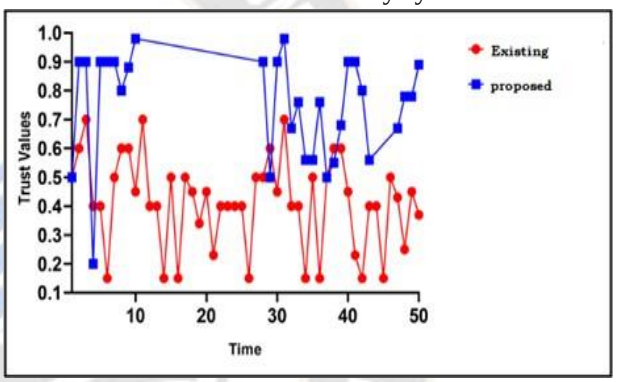

Fig.3: Performance analysis of the Trust Values

Nevertheless, the confidence value converges back to the field truth if the characteristic stays the same. The model's resilience is its ability to adapt to changes in these conditions while remaining highly efficient.

These three key factors are a lack of feedback from other nodes, a disparity in network behavior, and an increase in the group's violent node. Recommendations are only used at the beginning of a new contact session.

Table 4 reveals the utility analysis for trust values for the node relationship. The results show that without the confidence feature of degradation, it takes much longer to begin to converge and that the truth can be revealed again.

However, the new truth value is reached after some 250 experiences with the confidence-declining variable, keeping the confidence maturity index in the sense of cooperation constant.

Based on the results, when we create a matrix of all the trust values of various nodes among themselves in the real-world scenario, the system becomes more complex; the number of devices will be in the thousands or millions, depending on the area. So, In that case, the use of the cumulative trust

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 2s
DOI: https://doi.org/10.17762/ijritcc.v10i2s.5907
***Article Received**: 14 October 2022 **Revised**: 09 November 2022 **Accepted**: 20 December 2022*

value becomes highly useful for the forwarding of the data packet. The data packet is routed to the node with the highest cumulative trust value. Because we know that the trust value of soft nodes is inversely proportional to security over heads, the cumulative trust method is also useful. As a result, the higher the trust value, the lower the security, and vice versa. As a result, the method of cumulative trust is useful in defining a secure and efficient path for data transmission.

Table 4: Performance Comparison of Trust value on Varying Time Period

Time Period	Trust value of Fuzzy System Existing	Trust value of theory-Proposed
0	0.5	0.5
10	0.7	0.9
20	0.2	1
30	0.4	0.7
40	0.3	0.8

V. CONCLUSION

This manuscript deals with the new proposed algorithm for the calculation of the cumulative trust value to select the next node for communication. The more data flows through that path, the higher the cumulative trust value. To begin, we compute the trust value for each node in the other node. If the trust value for different nodes is the same, it will choose the path that follows the constraint. The confidence-safety trust-based framework was developed and simulated under various trust properties like trust maturity, trust decay, trust update, trust relevancy, and belief function. For the IoT System installation, the proposed model was examined. The analysis demonstrates that the model is effective, with high precision, dependability, and resilience in the confidence assessment and findings. Additionally, the maturity of confidence and the robust decreasing feature were modelled on aggregating confidence suggestions from nodes based on social interaction insights. The results of the simulation demonstrate the usefulness of the confidence equation over time. Further, the calculation of the cumulative trust value provides a path for forwarding the data in a secure and efficient way.

REFERENCES

[1]. Adewuyi, A. A., Cheng, H., Shi, Q., Cao, J., MacDermott, Á., & Wang, X. (2019). CTRUST: A dynamic trust model for collaborative applications in the Internet of Things. IEEE Internet of Things Journal, 6(3), 5432-5445.

[2]. Adewuyi, A. A., Cheng, H., Shi, Q., Cao, J., Wang, X., & Zhou, B. (2021). Sc-trust: a dynamic model for trustworthy service composition in the internet of things. *IEEE Internet of Things Journal*, *9*(5), 3298-3312.

[3]. Ahmed, E., Yaqoob, I., Gani, A., Imran, M., & Guizani, M. (2016). Internet-of-things-based smart environments: state of the art, taxonomy, and open research challenges. *IEEE Wireless Communications*, *23*(5), 10-16.

[4]. Alenezi, A., Atlam, H., Alsagri, R., Alassafi, M., & Wills, G. (2019). IoT forensics: A state-of-the-art review, callenges and future directions.

[5]. Arulanantham, D., & Palanisamy, C. (2021). Trusted cognitive sensor based dual routing network on Internet of things. *International Journal of Communication Systems*, *34*(10), e4836.

[6]. Asiri, S., & Miri, A. (2016, December). An IoT trust and reputation model based on recommender systems. In *2016 14th Annual Conference on Privacy, Security and Trust (PST)* (pp. 561-568). IEEE.

[7]. Awad, S., Malki, A., & Malki, M. (2021). Composing WoT services with uncertain and correlated data. *Computing*, *103*(7), 1501-1517.

[8]. Bao, F., & Chen, I. R. (2012, September). Dynamic trust management for internet of things applications. In *Proceedings of the 2012 international workshop on Self-aware internet of things* (pp. 1-6).

[9]. Beg, S., Anjum, A., Ahmad, M., Hussain, S., Ahmad, G., Khan, S., & Choo, K. K. R. (2021). A privacy-preserving protocol for continuous and dynamic data collection in IoT enabled mobile app recommendation system (MARS). *Journal of Network and Computer Applications*, *174*, 102874.

[10]. Chen, D., Chang, G., Sun, D., Li, J., Jia, J., & Wang, X. (2011). TRM-IoT: A trust management model based on fuzzy reputation for internet of things. *Computer Science and Information Systems*, *8*(4), 1207-1228.

[11]. Chen, G., Zeng, F., Zhang, J., Lu, T., Shen, J., & Shu, W. (2021). An adaptive trust model based on recommendation filtering algorithm for the Internet of Things systems. *Computer Networks*, *190*, 107952.

[12]. Chinnaswamy, S., & Annapurani, K. (2021). Trust aggregation authentication protocol using machine learning for IoT wireless sensor networks. *Computers & Electrical Engineering*, *91*, 107130.

[13]. Choudhury, S. S., Mohanty, S. N., & Jagadev, A. K. (2021). Multimodal trust based recommender system with machine learning approaches for movie recommendation. *International Journal of Information Technology*, *13*(2), 475-482.

[14]. Díaz, M., Martín, C., & Rubio, B. (2016). State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing. *Journal of Network and Computer applications*, *67*, 99-117.

[15]. Duan, R., Chen, X., Xing, T.: Aqos architecture for iot. In: 2011International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social

Computing, pp.717–720. IEEE (2011).

[16]. Ganeriwal, S., & Srivastava, M. B. (2004). Reputation-based model for High Integrity Sensor Networks. *proceedings of SASN04*.

[17]. Gessner, D., Olivereau, A., Segura, A. S., & Serbanati, A. (2012, June). Trustworthy infrastructure services for a secure and privacy-respecting internet of things. In *2012 IEEE 11th international conference on trust, security and privacy in computing and communications* (pp. 998-1003). IEEE.

[18]. Govindan, K., & Mohapatra, P. (2011). Trust computations and trust dynamics in mobile adhoc networks: A survey. *IEEE Communications Surveys & Tutorials*, *14*(2), 279-298.

[19]. Guo, J., Liu, A., Ota, K., Dong, M., Deng, X., & Xiong, N. N. (2021). ITCN: an intelligent trust collaboration network system in IoT. *IEEE transactions on network science and engineering*, *9*(1), 203-218.

[20]. 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.

[21]. Khan, S., Zafar, S., Iftekhar, N., Biswas, S., & Tripathi, G. (2021, March). Inculcating Dynamic Trust Management across Internet through avant-garde Approach. In *Proceedings of the 2nd International Conference on ICT for Digital, Smart, and Sustainable Development, ICIDSSD 2020, 27-28 February 2020, Jamia Hamdard, New Delhi, India*.

[22]. Kalnoor, G., & Gowrishankar, S. (2022). A model for intrusion detection system using hidden Markov and variational Bayesian model for IoT based wireless sensor network. *International Journal of Information Technology*, *14*(4), 2021-2033.

[23]. Kenchannavar, H. H., Pujar, P. M., Kulkarni, R. M., & Kulkarni, U. P. (2021). Evaluation and Analysis of Goodness of Fit for Water Quality Parameters using Linear Regression through the Internet of Things (IoT) based Water Quality Monitoring System. *IEEE Internet of Things Journal*.

[24]. Kil, H., & Nam, W. (2021). Automatic incremental recomposition algorithm for QoS-aware internet of things service composition. *International Journal of Web and Grid Services*, *17*(2), 118-137.

[25]. Kotis, K., Athanasakis, I., & Vouros, G. A. (2018). Semantically enabling IoT trust to ensure and secure deployment of IoT entities. *International Journal of Internet of Things and Cyber-Assurance*, *1*(1), 3-21.

[26]. Lin, Z., & Dong, L. (2017). Clarifying trust in social internet of things. *IEEE Transactions on Knowledge and Data Engineering*, *30*(2), 234-248.

[27]. Malchi, S. K., Kallam, S., Al-Turjman, F., & Patan, R. (2021). A trust-based fuzzy neural network for smart data fusion in internet of things. *Computers & Electrical Engineering*, *89*, 106901.

[28]. Mon, S., Winster, S. G., & Ramesh, R. (2021). Trust Model for IoT Using Cluster Analysis: A Centralized Approach. *Wireless Personal Communications*, 1-22.

[29]. Musen, M. A. (2015). The protégé project: a look back and a look forward. *AI matters*, *1*(4), 4-12.

[30]. Patel, M., Bhattacharyya, S., & Alfageeh, A. (2019, October). Formal Trust Architecture For Assuring Trusted Interactions In the Internet of Things. In *2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)* (pp. 0033-0039). IEEE.

[31]. Riahi, A., Challal, Y., Natalizio, E., Chtourou, Z., & Bouabdallah, A. (2013, May). A systemic approach for IoT security. In *2013 IEEE international conference on distributed computing in sensor systems* (pp. 351-355). IEEE.

[32]. Ruan, Y., Durresi, A., Alfantoukh, L.: Trust management framework for internet of thing. In: 2016 IEEE 30th International Conference on Advanced Information Net-working and Applications (AINA), pp.1013–1019. IEEE(2016)

[33]. Sharma, D. K., Bhardwaj, K. K., Banyal, S., Gupta, R., Gupta, N., & Nkenyereye, L. (2021). An Opportunistic Approach for Cloud Service-Based IoT Routing Framework Administering Data, Transaction, and Identity Security. *IEEE Internet of Things Journal*, *9*(4), 2505-2512.

[34]. Soleymani, M., Abapour, N., Taghizadeh, E., Siadat, S., & Karkehabadi, R. (2021). Fuzzy Rule-Based Trust Management Model for the Security of Cloud Computing. *Mathematical Problems in Engineering*, *2021*.

[35]. Swathi, S. (2021). Trust Aware Data Aggregation mechanism for malicious node identification in WSN based IoT Environment. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(13), 2217-2224.

[36]. Tahta, U. E., Sen, S., & Can, A. B. (2015). GenTrust: A genetic trust management model for peer-to-peer systems. *Applied Soft Computing*, *34*, 693-704.

[37]. Theodorakopoulos, G., & Baras, J. S. (2006). On trust models and trust evaluation metrics for ad hoc networks. *IEEE Journal on selected areas in Communications*, *24*(2), 318-328.

[38]. Wang, Y., Yang, G., Li, T., Li, F., Tian, Y., & Yu, X. (2020). Belief and fairness: a secure two-party protocol toward the view of entropy for IoT devices. *Journal of Network and Computer Applications*, *161*, 102641.

[39]. Weinstein, R. (2005). RFID: a technical overview and its application to the enterprise. *IT professional*, *7*(3), 27-33.

[40]. Yi, S. K. M., Steyvers, M., Lee, M. D., & Dry, M. J. (2012). The wisdom of the crowd in combinatorial problems. *Cognitive science*, *36*(3), 452-470.