

Collaborative trust computation model for social internet of things

Rashmi M R¹, C Vidya Raj¹, B R Vatsala¹, Bharathi Ramachandra², Mayura D. Tapkire¹

¹Department of Computer Science and Engineering, The National Institute of Engineering, Mysuru, India

²Department of Electronics and Communication Engineering, GSSS Institute of Engineering and Technology for Women, Mysuru, India

Article Info

Article history:

Received Oct 12, 2025

Revised Aug 13, 2026

Accepted Aug 20, 2026

Keywords:

Clustering

Cold start problem

Expectation-maximization

K-means

Social internet of things

ABSTRACT

Trust compromise is a major problem in social internet of things (SIoT). Existing trust management approaches often rely on predefined trust values, limited behavioral attributes, or historical interactions, making them less effective under dynamic and cold-start environments. This paper proposes a deep collaborative event trust model (DCETM) integrating collaborative event confidence modeling with graph neural networks (GNNs), long short-term memory (LSTM) networks, and multi-attribute trust evaluation to estimate device trustworthiness from spatial, temporal, and behavioral information. The proposed framework derives evidence-driven trust scores from collaborative event observations and integrates reliability, consistency, response behavior, and event confidence for robust malicious node detection. A preference-aware topology refinement mechanism further isolates malicious devices and promotes trustworthy interactions. Experimental evaluation on a SIoT benchmark dataset demonstrates that the proposed DCETM achieves 93.4% attacker detection accuracy, 0.90 F1-score, and reduces the misclassification rate by 25–30% compared with recent deep learning-based trust models. In-addition proposed DCETM maintains reliable trust estimation under cold-start conditions by avoiding default trust assignment through collaborative event validation, demonstrating its suitability for secure and scalable SIoT environments.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Rashmi M R

Department of Computer Science and Engineering, The National Institute of Engineering

Mysuru, Karnataka, India

Email: rashmi.mr7@nie.ac.in

1. INTRODUCTION

Internet of things (IoT) is a network of heterogeneous physical objects like sensors and devices with internet. Development and spread of IoT technology has enabled increased connectivity between humans and physical objects. With reduction in cost of computer chips and ubiquity of wireless networks, billions of devices are being connected to internet. Diverse objects in physical world like oven, cars, and house doors are getting connected to internet. With billions of devices on internet, the possibility of IoT objects establishing social relationships between them autonomously has resulted in a new paradigm called social internet of things (SIoT) [1].

The new paradigm allows smart objects and people to interact within a social structure of relationships. Similar to online social networks where people establish relationship between them based on many factors like social interests, real-life relations, background similarity etc. for sharing information, smart objects in SIoT establish relationship between them and share information. This relationship between smart objects allows better network navigation; discover various services and ability to perform number of tasks.

These functionalities make SIoT superior to IoT. But there is also a major security problem in establishment of relationship in SIoT environment. The data from these devices can be compromised, the devices can be manipulated, data can be tampered, risk of identity and information leakage. Protection from these wide varieties of security threats and vulnerabilities is a challenge. Controlling the social interaction between the devices based on trust is a solution to this problem [2], [3].

Online social network use conceptual trust based model. The trust is achieved in conceptual trust using harmonization. In harmonization, trust is learnt based on continuous observation between the two parties. The environmental conditions like threats/risks are observed during each interaction. From trust between two parties, trust between other parties is created using various relationships like transitive, co-location, co-work, and social relationship. But many of the trust models in online social network cannot be used in SIoT and especially when devices need to establish relationship in an autonomous manner [4], [5].

To enhance the robustness of trust estimation under complex and dynamic SIoT environments, this work proposes a deep collaborative event trust model (DCETM). The proposed solution combines event-centric trust modeling with deep learning for secure and scalable SIoT systems. The spatial and temporal characteristics are captured using graph neural networks (GNN) along with long short-term memory (LSTM). By this way DCETM learns latent trust representations from both structural and sequential data, enabling accurate detection of malicious nodes.

2. RELATED WORK

Lin and Dong [1] proposed a comprehensive trust model for SIoT. It is built on core concept of trustor, trustee and trust evaluation. Truong *et al.* [2] proposed a trust model using reputation scores. Trust model proposed in this work is based on three entities of reputation, recommendation and knowledge. Jayasinghe *et al.* [3] proposed a recommendations plus reputation based trust computational model (RpR). Objects can establish trustworthy association based on reputation. Chen *et al.* [4] proposed an adaptive trust model for SIoT. Social relationship dynamics of owners is used for trust establishment between devices. Nitti *et al.* [5] proposed trust management model based on subjective and objective assessment. Subjective assessment has a slower transitory response while dealing with dynamic node behavior. The same authors in [6] proposed a subjective model for trust management based on solutions available in P2P networks. Trust is calculated by each node based on its and its friends experience. Iqbal *et al.* [7] reviewed the trust models for social internet of vehicles. The work also reviewed how emerging technologies like block chain and fog computing can assist in developing a trust model. Xiao *et al.* [8] proposed a reputation model for SIoT. Bao *et al.* [9] proposed trust model for IoT environment with properties of scalability, adaptability. Block chain and machine learning is used in Wang *et al.* [10] for trust management in IoT networks. Block chain is used for identify management and certification of IoT transactions. Turkina and Ihnatiev [11] proposed a trust evaluation model which transforms subjective measurements to object interaction reputation.

Magdich *et al.* [12] proposed a trust metric for IoT. The metric considers dynamism in node behavior and to limit the influence of past reputation assessments. The trust metric is based on mutual evaluation of quality of service and security. Premarathne *et al.* [13] proposed a trust management system for IoT exploiting the operational conditions. The trust is based on predefined set of social relationships and residual energy content. The work identified multiple trust attributes in multiple categories of social relationship, communications, operation and indirect trust. A centralized server records the interactions between the nodes and calculates the trust. Artificial intelligence based deep chain framework is proposed by Kumar *et al.* [14] for calculating trust between the SIoT devices based on the social relationship between the owners in online social networks. Trust is evaluated in bilateral manner and then extended using transitivity calculations.

A holistic cross-domain trust management model for IoT is proposed by Awan *et al.* [15]. The nodes are divided into communities based on similarities and interests. A server is dedicated to calculate and manage trust in each community. The trust is computed for each community based on direct and indirect trust parameters. The calculated trust is used to ensure secure communications. Abderrahim *et al.* [16] proposed a scalable trust model for SIoT to provide a most trustworthy provider taking into account dynamic aspects like context, capacity and social relationship between objects. Atrey *et al.* [17] proposed a confidence building among correlated streams in multimedia surveillance systems, Jarman *et al.* [18] proposed a hierarchical cluster analysis of single linkage, complete linkage, average linkage and centroid linkage. The relationship between different components and SIoT objects is analyzed using decision trees. Jenifer and Preethika [19] proposed a self-adaptive trust management framework that dynamically adjusts trust evaluation parameters based on environmental changes and node behavior, improving scalability and responsiveness in large-scale

IoT systems. Moeinaddini *et al.* [20] leveraged GNN and recurrent architectures to learn spatial and temporal dependencies among devices, enabling more accurate trust prediction compared to traditional rule-based methods. Rexciya *et al.* [21] proposed an enhanced trust propagation mechanism for trust management in SIoT. This work focuses on trust propagation and does not jointly exploit collaborative event.

Mustafa *et al.* [22] proposed a light weight trust evaluation framework called MMTE. This work is based only on lightweight trust aggregation and does not exploit deep spatial-temporal learning or collaborative event validation. There are also studies on reinforcement learning-based trust management framework. This framework does not support capturing both neighborhood interactions and temporal trust evolution simultaneously [23]-[25].

3. PROPOSED DEEP COLLABORATIVE EVENT TRUST MODEL

The architecture of the proposed DCETM is given in Figure 1. DCETM aims to estimate trustworthiness of IoT devices in SIoT environment under dynamic and adversarial conditions. As shown in Figure 1, the proposed solution has following stages: i) event confidence modeling, ii) deep learning based trust estimation, iii) multi attribute trust computation, vi) malicious node detection, and v) topology refinement.

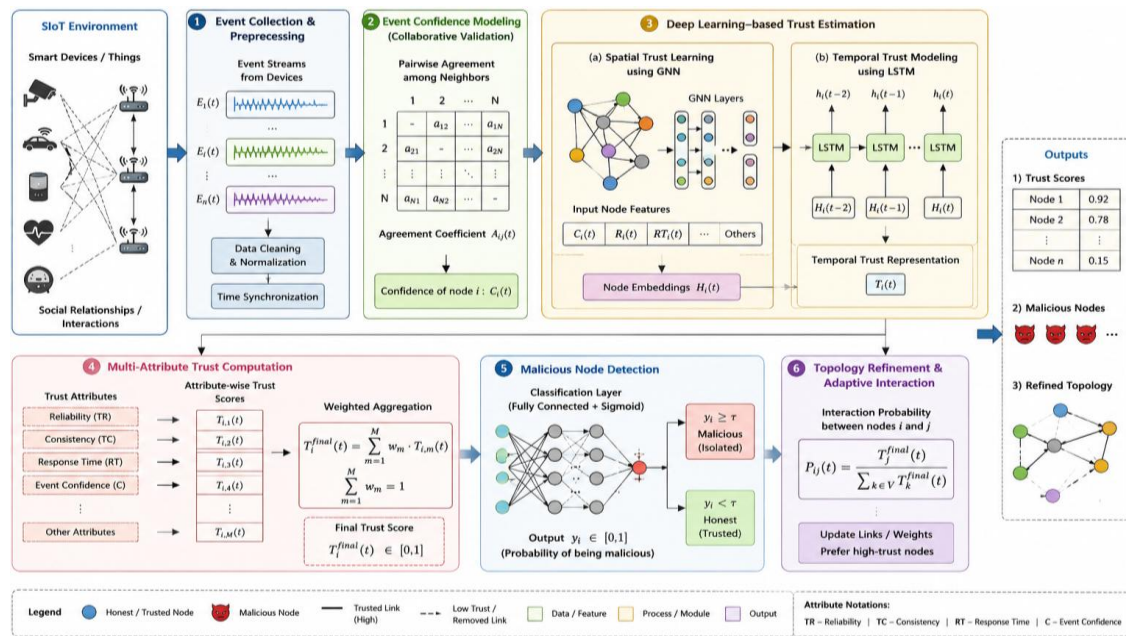


Figure 1. Architecture of proposed DCETM

3.1. Event confidence modeling

The event confidence model evaluates the reliability of events generated by multiple devices without the need for prior knowledge of the ground truth. Say an event is reported by a node i , the agreement with other nodes k is computed as (1):

$$A_{ik}(t) = \frac{1}{t} \sum_{\tau=1}^t \delta(E_i(\tau) E_k(\tau)) \quad (1)$$

where $\delta(\cdot)$ represents the agreement function between the event observations. The confidence of node i at time t is computed as (2):

$$C_i(t) = \frac{1}{|N_i|} \sum_{k \in N_i} A_{ik}(t) \quad (2)$$

where N_i are the neighbors of node i . Due to relying on multi source evidence is calculating confidence, the influence of isolated malicious nodes is avoided in the proposed work. Since the predicted confidence is

obtained from multiple independent event observations, the assigned trust reflects the current behavioral evidence rather than a fixed default value.

3.2. Deep learning based trust estimation

The SIoT network is viewed as a graph $G(V, E)$ where each node is a vertex and E represents the interaction link between the devices. To capture the complex interaction pattern between the devices, this work used GNN. The GNN captures spatial dependencies among SIoT devices by aggregating neighborhood information, enabling detection of collusion and structural anomalies in the interaction graph. In SIoT network, devices don't act in isolation. Honest nodes tend to connect with other honest nodes. Malicious nodes often demonstrate abnormal interaction patterns and collusive behaviors. GNN can learn these patterns effectively. Each node i in the graph G is associated with a feature vector consisting of confidence and multi attribute trust inputs as $X_i = [C_i(t), R_i(t), RT_i(t)]$ where $C_i(t)$ is event confidence, $C_i(t)$ is reliability reputation, $RT_i(t)$ is response time. Each node updates its representation by combining information from its neighbors as (3):

$$H_i^{(l+1)} = \sigma(\sum_{j \in N_i} W^{(l)} H_j^{(l)}) \quad (3)$$

where $H_i^{(l)}$ is the embedding of node at layer l . N_i is the neighbors of node i , $W^{(l)}$ learnable weights, σ is the activation function. After multiple layers, each node gets trust embedding as H_i^{final} which represents the node behavior, neighborhood influence and trustworthiness. The behavior of nodes can vary over a time period. To capture this temporal behavioral dynamics of node, LSTM is used in this work. The embedding of node are collected periodically at end of every window interval time and saved as sequence $H_i(1), H_i(2), \dots, H_i(t)$. This sequence captures trust evolution, behavior changes and event consistency over time. This sequence is processed by LSTM to provide the temporal trust representation.

$$T_i(t) = LSTM(H_i(1), H_i(2), \dots, H_i(t)) \quad (4)$$

3.3. Multi attribute trust computation

This work models trust as a multi-dimensional metric including multiple attributes like reliability, consistency, response time, and event confidence. Each attribute produces an individual score (as in subsection 3.2). From each individual score, the final trust score is calculated as (5):

$$T_i^{final(t)} = \sum_{m=1}^M w_m T_{i,m}(t), \sum_{m=1}^M w_m = 1 \quad (5)$$

where w_m is the importance of the attribute and $T_{i,m}(t)$ is the trust value for attribute m . Thus $T_i^{final(t)}$ aggregates reliability, consistency, response time, and event confidence using weighted scoring to produce an application-aware and robust trust estimate.

Different from existing trust models that rely on a single trust indicator (e.g., reputation or reliability), the proposed framework jointly evaluates multiple complementary trust attributes including reliability, consistency, response behavior, and collaborative event confidence.

3.4. Malicious node detection

A sigmoid-based classification layer is applied on the learned trust representations to identify malicious nodes, enabling robust detection of adversarial behavior in SIoT environments. The learned trust representations are processed as (6):

$$\hat{y}_i = \sigma(W_o \cdot T_i^{final(t)} + b_o) \quad (6)$$

where $\hat{y}_i \in [0,1]$ is the predicted probability of node being malicious. W_o, b_o are the learned parameters. σ is the sigmoid function.

From the $\hat{y}_i$, threshold is applied to detect node is malicious or not as (7):

$$Node\ i = \begin{cases} Malicious, & \hat{y}_i \geq \tau \\ Honest, & \hat{y}_i < \tau \end{cases} \quad (7)$$

3.5. Topology refinement

After identifying trustworthy and malicious nodes, the next step is to adapt the SIoT network structure so that future interactions preferentially occur among reliable devices. This stage dynamically refines the network topology to improve security, efficiency, and resilience.

The SIoT topology is dynamically refined by adjusting interaction probabilities based on computed trust scores, ensuring preferential communication among trustworthy nodes while isolating malicious entities. The interaction probabilities between node i and j is calculated as (8):

$$P_{ij}(t) = \frac{T_j^{final(t)}}{\sum_{k \in N_i} T_k^{final(t)}} \quad (8)$$

where $T_j^{final(t)}$ is the trust score of node j . The probability of node i to select node j for any application is controlled by $P_{ij}(t)$.

Malicious nodes are removed from neighbor list and assigned with zero interaction probability. It is also prevented from contributing to event aggregation. By this way, the effects of malicious entities like false information propagation, erroneous trust computation, and system performance degradation can be avoided. Dynamic topology update is implemented as follows. At each time step:

- Compute trust score,
- Identify malicious node,
- Update adjacency matrix $A(t)$ with adjacency between each node calculated as (9):

$$A_{ij}(t) = \begin{cases} P_{ij}(t), & \text{if } j \notin M \\ 0, & \text{if } j \in M \end{cases} \quad (9)$$

where M is the set of malicious nodes.

4. RESULTS

The performance of proposed collaborative event confidence model is simulated against IoT network dataset downloaded from SIoT/IoT Network Dataset – Net4U (<https://sites.unica.it/net4u/siot-iot-network-dataset/>). The dataset has a total of 16,216 devices. The dataset has both private and public devices. Devices like weather stations, street lights, and security equipment's are public devices. User's smartphone is an example of private device. In the dataset for dishonest rate from 5% to 30%, the devices are made as attacker. The simulation is done with following configuration given in Table 1.

Table 1. Simulation configuration

Parameter	Value
Total devices	1500
No of public devices	1000
No of private devices	500
Dishonest rate	5% to 25%
Simulation time	30 minutes
Models compared	Subjective trust [6], sustainable trust [11], SATM-SIoT [20], and DL trust [21]

The performance is evaluated in terms of detection accuracy, precision, recall, F1-score, misclassification rate, and detection latency. The experiments are repeated for 5 independent runs and results are reported in terms of mean± standard deviation (SD). The results for detection accuracy are given in Table 2.

Table 2. Comparison of detection accuracy

Dishonest rate (%)	Subjective [6]	Sustainable [11]	DL trust [21]	SATM-SIoT [20]	DCETM
5	85.2±1.8	86.1±1.6	89.3±1.4	88.7±1.5	93.4±1.2
10	81.4±2.1	82.2±1.9	87.1±1.7	85.6±1.8	91.2±1.5
15	77.6±2.3	79.1±2.0	85.0±1.9	83.2±2.1	89.3±1.6
20	73.8±2.5	76.3±2.2	82.4±2.1	80.5±2.3	87.1±1.8
25	72.1±2.7	73.5±2.4	80.2±2.3	78.4±2.5	85.0±2.0

The proposed DCETM achieves the highest attacker detection accuracy across all dishonest node ratios. Even as the proportion of malicious devices increases from 5% to 25%, the proposed model maintains an accuracy above 85%, whereas the competing methods exhibit a more pronounced degradation. The results for precision, recall and F1-score are given in Table 3.

Table 3. Precision, recall, and F1-score comparison

Model	Precision	Recall	F1-score
Subjective [6]	0.78±0.02	0.75±0.03	0.76±0.02
Sustainable [11]	0.80±0.02	0.77±0.02	0.78±0.02
DL trust [21]	0.86±0.015	0.83±0.02	0.84±0.018
SATM-SIoT [20]	0.84±0.017	0.81±0.02	0.82±0.019
DCETM	0.91±0.012	0.89±0.014	0.90±0.013

From Table 3 results it can be seen that proposed DCETM achieves the highest precision, recall, and F1-score among all compared approaches. The resulting F1-score of 0.90 confirms a balanced trade-off between false positives and false negatives. The results for misclassification rate are given in Table 4.

Table 4. Misclassification rate

Dishonest rate (%)	Subjective [6]	Sustainable [11]	DL trust [21]	SATM-SIoT [20]	DCETM
5	3.1±0.4	3.0±0.5	2.5±0.3	2.3±0.3	1.5±0.2
10	6.2±0.6	5.3±0.5	4.2±0.4	4.0±0.4	2.8±0.3
15	8.4±0.7	9.1±0.8	5.5±0.5	5.2±0.5	3.9±0.4
20	9.3±0.8	11.0±0.9	6.8±0.6	6.3±0.6	4.8±0.5
25	11.2±0.9	12.1±1.0	7.5±0.7	7.1±0.7	5.6±0.6

The results in Table 4 show that the proposed DCETM achieves the lowest misclassification rate under all attack intensities. A lower misclassification rate indicates that both malicious devices incorrectly accepted as trustworthy and legitimate devices incorrectly rejected are minimized. The detection latency is measured and results are presented in Table 5.

Table 5. Comparison of detection latency

Time (minutes)	Subjective [6]	DL trust [21]	SATM-SIoT [20]	DCETM
5	8.2±0.9	10.1±1.0	9.3±0.8	14.5±0.7
10	16.4±1.2	20.3±1.3	18.2±1.1	28.6±1.0
15	20.5±1.5	30.2±1.6	25.4±1.4	45.3±1.3
20	16.2±1.3	35.1±1.8	30.5±1.6	82.1±1.5
25	12.4±1.1	40.2±2.0	35.6±1.8	90.3±1.7

Detection latency determines how quickly malicious devices can be isolated after launching an attack. As shown in Table 5, the proposed DCETM identifies the majority of attackers within the early stages of network operation, enabling rapid trust updates and timely topology refinement.

The experimental results demonstrate that the proposed DCETM significantly outperforms existing trust models. The improvement is primarily due to: i) event-centric validation, which filters unreliable data before trust computation, ii) graph-based spatial learning, capturing complex interaction patterns, iii) temporal modeling, enabling detection of dynamic and stealthy attacks, and iv) the proposed multi-attribute trust mechanism contributes significantly to malicious node detection by combining complementary behavioral indicators instead of relying on a single trust metric. The results varying the GNN hidden dimension is given in Table 6.

Table 6. Results varying GNN hidden dimension

Hidden dimension	Accuracy (%)	F1-score	Training time
16	84.3±1.9	0.83±0.02	48
32	87.5±1.7	0.86±0.02	56
64	91.2±1.5	0.90±0.01	68
128	91.4±1.6	0.90±0.02	102

The accuracy increases with increase in GNN hidden dimension. But the performance gain beyond 64 is marginal and also the computation overhead in terms of training time increases significantly. The results varying LSTM hidden units are given in Table 7.

Table 7. Results varying LSTM hidden units

LSTM hidden units	Accuracy (%)	Recall	F1-score
16	85.1±1.8	0.83±0.02	0.84±0.02
32	88.4±1.6	0.86±0.02	0.87±0.02
64	91.2±1.5	0.89±0.01	0.90±0.01
128	91.5±1.7	0.89±0.02	0.90±0.02

The hyper parameter analysis demonstrates that increasing the model complexity beyond a hidden dimension of 64 or LSTM hidden units of 64 produces only marginal accuracy improvements while substantially increasing computational cost. Therefore, the selected configuration provides an effective balance between detection performance and computational efficiency, making it suitable for deployment on resource-constrained edge or fog nodes commonly used in SIIoT systems. The results varying the learning rate is given in Table 8. The DCETM model provides a stable convergence and high accuracy at learning rate of 0.001. The detection accuracy of solutions for various attacks are given in Table 9.

Table 8. Results varying learning rate

Learning rate	Accuracy (%)	Convergence epoch
0.1	78.3±2.5	Unstable
0.01	87.4±1.9	55
0.001	91.2±1.5	42
0.0001	88.2±1.7	95

Table 9. Detection accuracy for various attacks

Attack type	DL trust [21]	SATM-SIIoT [20]	DCETM
False data injection	84.2±1.8	82.1±2.0	91.5±1.4
On-off attack	79.4±2.2	77.8±2.4	89.1±1.6
Collusion attack	76.3±2.5	75.1±2.7	88.4±1.7
Sybil attack	81.5±2.1	79.6±2.3	90.2±1.5

The attack-wise evaluation results in Table 9 shows that the proposed DCETM consistently outperforms existing trust models across false data injection, on-off, collusion, and Sybil attacks. The largest improvement is observed for collusion attacks because the GNN captures abnormal neighborhood interaction patterns while collaborative event validation suppresses mutually reinforcing false observations. The proposed DCETM consistently achieves the highest detection accuracy across all evaluated cold-start levels.

5. CONCLUSION

A DCETM is proposed in this work. Different from existing trust models based on predefined expected outcomes or isolated pairwise evaluations, multisource event centric collaborative paradigm is proposed. The model integrates GNNs to capture spatial dependencies among interacting devices and LSTM networks to model temporal evolution of node behavior, enabling accurate detection of dynamic and stealthy adversarial patterns. In addition, a multi-attribute trust computation mechanism and trust-driven topology refinement strategy facilitate secure and reliable trust management in SIIoT networks. Though the proposed framework achieves better malicious node detection performance on the benchmark dataset, future work will emphasize extensive validation using multiple standardized trust datasets and real-world SIIoT test beds to further establish its generalizability, scalability, and practical applicability across diverse deployment scenarios.

FUNDING INFORMATION

No funding involved for the research work.

AUTHOR CONTRIBUTIONS STATEMENT

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

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Rashmi M R	✓	✓			✓	✓	✓			✓				
C Vidya Raj				✓		✓		✓		✓				
B R Vatsala			✓		✓	✓				✓				
Bharathi Ramachandra				✓	✓		✓	✓		✓				
Mayura D. Tapkire			✓			✓				✓				

C : **C**onceptualization

M : **M**ethodology

So : **S**oftware

Va : **V**alidation

Fo : **F**ormal analysis

I : **I**nterpretation

R : **R**esources

D : **D**ata Curation

O : Writing - **O**riginal Draft

E : Writing - Review & **E**dit

Vi : **V**isualization

Su : **S**upervision

P : **P**roject administration

Fu : **F**unding acquisition

CONFLICT OF INTEREST STATEMENT

There is no conflict of interest.

DATA AVAILABILITY

Data availability is on <https://sites.unica.it/net4u/siot-iot-network-dataset/>.

REFERENCES

- [1] Z. Lin and L. Dong, "Clarifying trust in social internet of things (extended abstract)," in *Proceedings - IEEE 34th International Conference on Data Engineering, ICDE 2018*, IEEE, Apr. 2018, pp. 1825–1826, doi: 10.1109/ICDE.2018.00270.
- [2] N. B. Truong, T.-W. Um, and G. M. Lee, "A reputation and knowledge based trust service platform for trustworthy social internet of things," in *Proceedings of the 19th International Conference on Innovations in Clouds*, 2016, pp. 104–111.
- [3] U. Jayasinghe, N. B. Truong, G. M. Lee, and T. W. Um, "RpR: a trust computation model for social internet of things," in *Proceedings - 13th IEEE International Conference on Ubiquitous Intelligence and Computing, 13th IEEE International Conference on Advanced and Trusted Computing, 16th IEEE International Conference on Scalable Computing and Communications, IEEE International Conference on Cloud and Big Data Computing, IEEE International Conference on Internet of People and IEEE Smart World Congress and Workshops, UIC-ATC-ScalCom-CBDCom-IoP-SmartWorld 2016*, IEEE, 2017, pp. 930–937, doi: 10.1109/UIC-ATC-ScalCom-CBDCom-IoP-SmartWorld.2016.0146.
- [4] I.-R. Chen, F. Bao, and J. Guo, "Trust-based service management for social internet of things systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 6, pp. 684–696, Nov. 2016, doi: 10.1109/TDSC.2015.2420552.
- [5] M. Nitti, R. Girau, and L. Atzori, "Trustworthiness management in the social internet of things," *IEEE Transactions on Knowledge and Data Engineering*, vol. 26, no. 5, pp. 1253–1266, May 2014, doi: 10.1109/TKDE.2013.105.
- [6] M. Nitti, R. Girau, L. Atzori, A. Iera, and G. Morabito, "A subjective model for trustworthiness evaluation in the social internet of things," in *2012 IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications - (PIMRC)*, IEEE, Sep. 2012, pp. 18–23, doi: 10.1109/PIMRC.2012.6362662.
- [7] R. Iqbal, T. A. Butt, M. Afzaal, and K. Salah, "Trust management in social internet of vehicles: factors, challenges, blockchain, and fog solutions," *International Journal of Distributed Sensor Networks*, vol. 15, no. 1, Jan. 2019, doi: 10.1177/1550147719825820.
- [8] H. Xiao, N. Sidhu, and B. Christianson, "Guarantor and reputation based trust model for social internet of things," in *IWCMC 2015 - 11th International Wireless Communications and Mobile Computing Conference*, IEEE, Aug. 2015, pp. 600–605, doi: 10.1109/IWCMC.2015.7289151.
- [9] F. Bao, I. R. Chen, and J. Guo, "Scalable, adaptive and survivable trust management for community of interest based internet of things systems," in *Proceedings - 2013 11th International Symposium on Autonomous Decentralized Systems, ISADS 2013*, IEEE, Mar. 2013, pp. 1–7, doi: 10.1109/ISADS.2013.6513398.
- [10] L. Wang, H. Zhu, J. Sun, R. Dai, Q. Ma, and X. Wei, "Trust assessment in internet of things using blockchain and machine learning," *Springer Science and Business Media LLC*, Nov. 19, 2020, doi: 10.21203/rs.3.rs-110210/v1.
- [11] V. Turkina and D. Ilnatiev, "Approach to sustainable trust and reputation evaluation in distributed mobile networks of the internet of things," in *Proceedings - 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies, DESSERT 2020*, IEEE, May 2020, pp. 117–121, doi: 10.1109/DESSERT50317.2020.9125015.
- [12] R. Magdich, H. Jemal, and M. B. Ayed, "Trust management model based on mutual evaluation method for the social internet of things," in *Lecture Notes in Business Information Processing*, vol. 381, pp. 361–375, 2020, doi: 10.1007/978-3-030-44322-1_27.
- [13] U. S. Premaratne, "Residual energy aware trust computation method for social internet of things," in *2019 IEEE 14th International Conference on Industrial and Information Systems: Engineering for Innovations for Industry 4.0, ICIIS 2019 - Proceedings*, IEEE, Dec. 2019, pp. 470–475, doi: 10.1109/ICIIS47346.2019.9063292.
- [14] J. S. Kumar, G. Sivasankar, and S. S. Nidhyananthan, "An artificial intelligence approach for enhancing trust between social iot devices in a network," in *Studies in Computational Intelligence*, vol. 846, Springer International Publishing, 2020, pp. 183–196, doi: 10.1007/978-3-030-24513-9_11.
- [15] K. A. Awan, I. U. Din, M. Zareei, M. Talha, M. Guizani, and S. U. Jadoon, "HoliTrust-a holistic cross-domain trust management

- mechanism for service-centric internet of things,” *IEEE Access*, vol. 7, pp. 52191–52201, 2019, doi: 10.1109/ACCESS.2019.2912469.
- [16] O. B. Abderrahim, M. H. Elhedhili, and L. Saidane, “CTMS-siot: a context-based trust management system for the social internet of things,” in *2017 13th International Wireless Communications and Mobile Computing Conference, IWCMC 2017*, IEEE, 2017, pp. 1903–1908, doi: 10.1109/IWCMC.2017.7986574.
- [17] P. K. Atrey, M. S. Kankanhalli, and A. El Saddik, “Confidence building among correlated streams in multimedia surveillance systems,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, Springer Berlin Heidelberg, vol. 4352, part 2, pp. 155–164, 2007, doi: 10.1007/978-3-540-69429-8_16.
- [18] A. M. Jarman, “Hierarchical cluster analysis: comparison of single linkage, complete linkage, average linkage and centroid linkage,” *International Journal of Georgia Southern University*, vol. 1, no. 1, pp. 1–13, 2020, doi: 10.13140/RG.2.2.11388.90240.
- [19] A. Jenifer and S. K. P. Preethika, “Deep learning models for trust management in social internet of things,” *Journal of Information Systems Engineering and Management*, vol. 10, no. 4s, pp. 226–232, Jan. 2025, doi: 10.52783/jisem.v10i4s.493.
- [20] E. Moenaddini, E. Nazemi, and A. Shahraki, “A new approach on self-adaptive trust management for social internet of things,” *Computer Networks*, vol. 263, p. 111187, May 2025, doi: 10.1016/j.comnet.2025.111187.
- [21] M. J. Rexciya, A. M. Kowshalya, M. Muthuchelvam, and R. Madhumathi, “Enhanced trust propagation mechanism for trust management in the social internet of things,” *IETE Journal of Research*, vol. 71, no. 6, pp. 1880–1896, May 2025, doi: 10.1080/03772063.2025.2504096.
- [22] R. U. Mustafa, A. McGibney, and S. Rea, “MMTE: micro-moment based lightweight trust evaluation model with trust spheres for scalable social iot,” *Technologies*, vol. 13, no. 12, p. 543, Nov. 2025, doi: 10.3390/technologies13120543.
- [23] S. Kumari and D. K. S. M., “An adaptive and resilient trust management model for social iot: a reinforcement approach,” *International Journal of Communication Systems*, vol. 39, no. 4, Jan. 2026, doi: 10.1002/dac.70391.
- [24] S. Somanath and U. B. Ajay, “Learning methodologies towards leveraging security resiliency in internet-of-things environment,” *IAES International Journal of Artificial Intelligence (IJ-AI)*, vol. 13, no. 3, pp. 2490–2497, Sep. 2024, doi: 10.11591/ijai.v13.i3.pp2490-2497.
- [25] S. A. Farooqi and F. Zafar, “Security and privacy challenges in the internet of medical things (iomt): A comprehensive review,” *International Journal of Social Sciences Bulletin*, vol. 2, no. 2, pp. 519–532, 2024.

BIOGRAPHIES OF AUTHORS



Rashmi M R    is an Associate Professor at the Department of Computer Science and Engineering, The National Institute of Engineering, Mysore, Karnataka, where she has been a faculty member since 2006. She graduated with a first-class honours B.Eng. degree in Information Science and Engineering from VTU, 2006, and M.Tech. in Computer Network Engineering from VTU, Belagavi in 2013. She completed her Ph.D. in Computer Science Engineering from VTU, Belagavi, Karnataka, in 2025. Her research interests are primarily in the area of social internet of things, machine learning, and artificial intelligence, where she is the author/co-author of over 20 research publications. She can be contacted at email: rashmi.mr7@nie.ac.in.



C Vidya Raj    is a professor in the Department of Computer Science and Engineering at The National Institute of Engineering, Mysore, Karnataka, India. Her research and teaching interests include quantum computing, software engineering, computer networks, wireless networks, storage area networks, and the internet of things. She has presented papers at various conferences and published research papers in reputed international journals. She is a life member of the Indian Society for Technical Education and a Fellow of the Institution of Engineers (India). She has received best paper awards for her research. She has guided and is currently guiding research scholars. She has also delivered several technical talks at various institutions. She can be contacted at email: vidyarajc@nie.ac.in.



B R Vatsala    is an Associate Professor in the Department of Computer Science and Engineering at The National Institute of Engineering, Mysore, Karnataka, India. His teaching and research interests include the internet of things, computer architecture, compiler design, microprocessors, embedded systems, and computer networks. He has presented papers at various conferences and published research papers in international journals. He was awarded an Elite Certificate with a gold medal for achieving a score of 90% in the NPTEL online course “Introduction to internet of things.” She can be contacted at email: vatsalabr@nie.ac.in.



Bharathi Ramachandra    received her Bachelor of Engineering degree in Electronics and Communication Engineering from SJCE in 2008. She received her Master's degree in Computer Network Engineering from The National Institute of Engineering (NIE), Mysuru, in 2013 and her Doctor of Philosophy degree from Visvesvaraya Technological University (VTU), Belagavi, in 2025. She is currently working as an Associate Professor in the Department of Electronics and Communication Engineering at GSSSIETW, Mysuru. Her research interests include wireless sensor networks (WSNs), attacks in WSNs, cryptography, internet of things (IoT), and communication systems. She can be contacted at email: bharathi@gsss.edu.in.



Mayura D. Tapkire    is currently working as an Associate Professor at the National Institute of Engineering (NIE) with over 13 years of teaching experience. She holds a Ph.D. in Computer Science and Engineering and was a University Rank holder in her B.E. degree. Her research lies in artificial intelligence and machine learning, with interests in deep learning, ai in healthcare, medical image analysis, and food-tech systems. She has published several research articles in reputed SCIE/WOS indexed journals, international conferences, book chapters, and patents. She can be contacted at email: mayura@nie.ac.in.