EAI Endorsed Transactions
on Scalable Information Systems
Research Article EAI.EU

Scalable Dynamic Trust Evolution Framework for Large-Scale IoT Information Systems with Asymmetric Evidence Weighting

Tao Sun[1,*]

[1] Guangzhou Academy of Fine Arts, Guangzhou, China

Abstract

INTRODUCTION: The growth of Internet-of-Things (IoT) infrastructure being built pushes the envelope to giant scale, heterogeneous systems where autonomous devices keep communicating amongst themselves with less and less human intervention. Static or transient security mechanisms based on pure authentication fall short in this case, as every device that has nominally been put in a non-trust domain can push bad from there. OBJECTIVES: To guard against, we present in this paper a Scalable Dynamic Trust Evolution (SDTE) framework for large-scale IoT information systems. METHODS: We model trust as a dynamically changing latent state dependent on multiple sources of evidence, such as direct interaction, neighbour recommendation, context condition, and historical behaviour. A temporal update mechanism with exponential forget rate (λ) allows fast adaptation to changing behaviour, while asynchronous weighting ($\beta^- > \beta^+$) indicates negative actions have larger weighting on trust than positive ones. An uncertainty-aware fusion of heterogeneous evidence sources mitigates conflicting observations. Overall, the framework is fully distributed and operates in lightweight computation ($O(d)$) without any need for sufficient computing resources, and can thus be deployed on low-resource edge devices. RESULTS: Our experimental results on publicly available IoT datasets (IoT-23 and Edge-IIoTset) show that SDTE achieves high detection performance (96.8% accuracy, 95.7% F1-score) across malicious ratio scenarios, good robustness against intermittent on–off attacks, and scaling as the network grows in size. CONCLUSION: The proposed SDTE framework provides an effective, lightweight, and scalable trust management solution for large-scale IoT information systems.

Keywords: Internet of Things, Trust Management, Scalable Systems, Dynamic Trust, Uncertainty Fusion, Distributed Security

Received on 15 February 2026, accepted on 25 April 2026, published on 28 July 2026

doi: 10.4108/eetsis.14117

1. Introduction

The Internet of Things (IoT) has progressed from small experiments to massive infrastructures linking tens of billions of heterogeneous devices in fields such as smart cities, industrial automation, healthcare, and transportation. Even more so than in more traditional environments, devices in these places are autonomous and continuously communicate with one another without human intervention, making long-term reliability a key concern in such places [1], [2]. Traditional security techniques that are based on static authentication assume that if a device passes testing, it will remain trustworthy for the rest of its working life. This is a mistaken assumption, as IoT devices can be left exposed, barely maintained, and even remotely taken over post-deployment [3].

While in principle a device may behave correctly, it may later yield incorrect data, deny service, or launch coordinated attacks—even with a valid credential. As a response, trust management became a supplementary way to assess how reliable entities are, from their behavior and interactions [4]. Unlike models of access control, trust mechanisms allow a dynamic evaluation of the condition, particularly in terms of state of uncertainty, as available information changes over the distributed environment. Although much work has been

*Corresponding author. Email: st@gzarts.edu.cn

done, existing trust management techniques suffer from not scaling well when transported to a large-scale IoT architecture. Many reputation models aggregate an entity's knowledge independently and do not adequately capture timing dynamics, and often do not discount evidence rapidly enough against suddenly changing behavior. Furthermore, evidence gathered from other intermediary sources, direct observation, recommendation from neighbor(s), context, and others, this evidence may be uncertain or conflicting, and " fusing" them without loss of meaningful information is a hard problem. Also, many of the above approaches are based on small, moderate networks and are thus hard to compact to deal with thousands of devices talking to each other in extreme situations of resource constraints [5].

Distributed power computing, edge cognition, and decentralized architectures do offer some hope but come with added headaches; some algorithms look towards more robust machine learning detection techniques, others towards the power of the blockchain or federated devices. While powerful, these respective systems often fall short due to computational overhead, communication cost, and implementation complexity overall/networking themselves, and are far from actual application [6].

To overcome these issues, in this paper, we propose a Scalable Dynamic Trust Evolution (SDTE) framework for large-scale IoT information systems. Rather than viewing trust as a static property, SDTE sees trust as a latent state that evolves based on observed interactions and the context in which those interactions occur. The model fuses multi-source evidence through an uncertainty-aware fusion and uses asymmetric weighting to take into account the more significant effect that negative behaviour has on trust. Critically, we account for the operational constraints of the IoT: trust information is updated locally, requires light computation, and is free from centralized coordination.

As key contributions of this work, we list here:

A dynamical model of trust evolution that can capture the changing behaviour of the device over time whilst remaining stable with respect to noisy observations.

An asymmetric weighting mechanism for melding evidence in a manner that helps to be more robust to intermittent malicious behaviour (on-off attacks).

An uncertainty-aware fusion of heterogeneous evidence that can mitigate the effects of those conflicts and unreliable evidence.

A lightweight distributed architecture that will allow scalability when deployed to many resource-constrained devices in large IoT networks, without centralised control.

Extensive experiments that lend credence to robustness, scalability, and practical applicability. The remainder of this paper is organised as follows: Section 2 surveys related work on IoT trust management. Section 3 describes the proposed SDTE architecture. Section 4 outlines the experiments undertaken and results. Section 5 addresses considerations for deployment, limitations, and further work. Section 6 concludes this work.

2. Related Work

2.1. Static Trust Models

Early trust management techniques were primarily based on static evaluation methods of averaging past interactions into a global reputation score. Reputation systems and simple context-based trust models, which provide reliability estimates based on aggregated history, e.g., [7], [8]. These approaches are computationally light and simple to deploy, making them appropriate for widespread resource-constrained devices.

Either extending reputation systems with physical attributes, e.g., location, channel quality, service quality, etc., or more sophisticated trust models provide context-bearing trust decisions. Borrowing information based on operational circumstances improved the fidelity of trust models over static methods. Static trust models also rely on the idea that past behavior indeed suggests future behavior, an assumption that can yield dangerous problems within dynamic IoT systems, where devices may change drastically, rendering them untrustworthy or available to attack. Devices may approach or obtain an aggregate reputation score that is too high, but they may be doing this for a long time with bad intentions, without being aware of it. If we rely on static aggregation, we are going to hide subtle anomalies, and we can ' t protect ourselves from intermittent attacks. This presumed static aggregation of trust models won't scale well because we need fast adaptations.

2.2. Dynamic Trust Models

To overcome the drawbacks of static methods, dynamic approaches leverage temporality in their models. Such techniques are based on continuously updating trust based on recent observations, through sliding windows, decay functions, or probabilistic transitions [9], [10]. By placing more importance on recent behaviour, a model can react faster to a change in device reliability.

Recent research has also focused on leveraging machine learning methods for dynamic trust estimation, such as neural networks and anomaly detection algorithms. Such approaches allow more complex behaviour to be considered, improving accuracy in heterogeneous environments.

However, dynamic approaches lead to new issues. Learning-based techniques often require huge amounts of training data and computational resources, often not available in distributed IoT scenarios. High model complexity may also lead to a lack of interpretability, making adoption difficult for safety-critical applications. Finally, dynamic models do not help to resolve whether several pieces of evidence are internally consistent. Recommendations from neighbouring nodes are unreliable and can be malicious, and aggregating them without proper caution can lead to expanding an error throughout the network.

2.3. Distributed and Decentralized Trust Frameworks

As large-scale IoT ecosystems start to appear, decentralized trust management approaches are gaining popularity. Blockchain-based approaches allow tamper-resistant storage of trust records as well as allowing reputation information to be shared transparently without the need for centralized authorities [11]–[14]. Federated learning approaches allow for collaborative evaluation while maintaining the privacy of data across administrative domains [15]–[18].

These mechanisms are then largely defense against manipulation of data on the one hand, and single points of failure, as in distributed systems on the other, and also allow for cooperation between autonomous subsystems that do not fully trust each other.

On the other hand, many decentralized methods come with considerable operational overhead. Consensus and persistent storage come with update latencies and high energy costs that will not be worth the trade-off for real-time decisions at the edge. Federated methods rely on stable and well-orchestrated communication that is likely to be extremely dynamic in highly transient networks. Moreover, decentralization does not help with the question of how to form and reshape trust in uncertain and even contradictory evidence. These systemic problems twist such methods around the form and end up failing both efficiency and flexibility.

2.4. Lightweight and Scalable Trust Approaches

While we are aware that models with many parameters will not generally perform "well" in rapidly evolving environments, recent work on "lightweight" trust evaluation models shows promise in allowing greater deployment of these systems in more constrained resource settings. Edge-oriented frameworks focus on decisions made locally, and thus limit communication, and the associated latency with each [19], [20]; adaptive models attempt to capture the short-term changes in behavior but do so with little additional computation cost. We note that detecting coordinated malicious behaviour in large networks [21], [22] points towards being able to utilise the structure of the relationships between nodes and the graph-based techniques possible for aiding detection capability. However, many lightweight approaches generally only weakly, sacrificing robustness with less considered techniques for efficiency, while often requiring global topology information or iterations, not feasible given the disadvantages of large-scale systems with intermittent connectivity. Recent works approach attempting to trade efficiency for robust accuracy, but remaining responsive and accepting of uncertainty, while scalable is difficult.

2.5. Research Gap and Motivation

Our analysis reveals an important weakness in the literature as a whole. Deploying effective trust solutions in large-scale information systems requires that we satisfy several criteria at once, notably: the ability to keep track of behavioural change over time; some resilience to uncertain and conflicting evidence; low computational and communication burden; and suitability for distributed use. Most proposed solutions trade off some of these criteria, usually optimising only a subset. Static models are very efficient, but too little responsive; dynamic models help to keep pace, but can be inflexible and unscalable, or at least hard to understand; decentralised approaches give some robustness, but can add operational complexity; lightweight systems can err too far towards minimalism and lose validity in the process. We aim to redress the balance through a Scalable Dynamic Trust Evolution (SDTE) that leverages temporal variations in evidence, asymmetric evidence weighting, combined with uncertainty-aware fusion.

3. Proposed Scalable Dynamic Trust Evolution Framework

3.1. Design Objectives

Large-scale IoT information systems are comprised of heterogeneous devices, plugged into dynamic and potentially hostile environments where nodes can join or leave the network regularly, conditions for reliable communication can be unstable, and devices can also change their behaviour, either due to faults and environmental effects, or malicious compromise. In these situations, trust management mechanisms need to fulfil several requirements simultaneously: to understand and act on changes in behaviour rapidly, to be resilient to unreliable or imprecise information about behaviour, to do the analysis with low computational cost, and to scale to thousands of nodes.

Many existing approaches address only a subset of these requirements, high accuracy with complex models and therefore long training times needs centralized processing and large amounts of training data, while light-weight and simple reputation-based schemes are easy to deploy, but neglect transient changes or targeted attacks, while evidence gathered from many sources may be uncertain, and indeed contradictory, making it difficult to trust trust estimation.

The Scalable Dynamic Trust Evolution (SDTE) proposed for sale with the aim of balancing, performance, accuracy and competing goals such as trustworthy trust estimation with a system model using temporal modeling with asymmetric evidence weightings and uncertainty-aware fused trust values without excessive computational overhead in a distributed framework based around the principle of practical deployability allowing executing indefinitely without central coordination on resource-constrained devices.

3.2. Framework Overview

Figure 1 illustrates the overall architecture of the SDTE framework. Each node independently evaluates the trustworthiness of its neighbors using locally available information and periodically updates trust values.

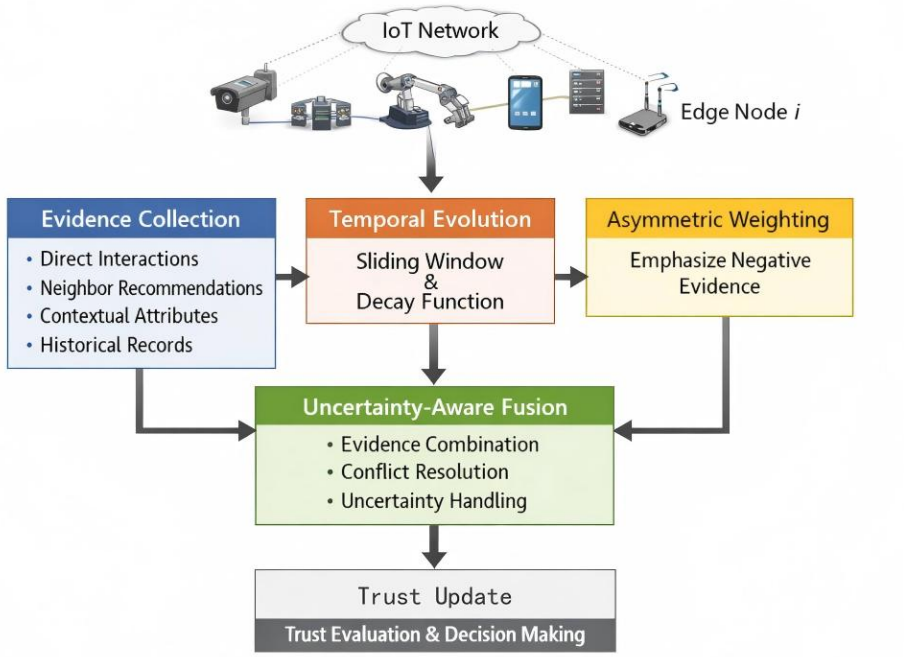

Figure 1. Overall architecture of the SDTE framework

The framework consists of four primary modules:

- This functionality is provided through the following modules:
- Evidence Collection Module—collects heterogeneous observations, raw interactions, neighbours' recommendations, context attributes, and past observations;
- Temporal Evolution Module—updates trust according to updated recent observations but respects past trends;
- Asymmetric Weighting Module—down-weighs evidence that has proved less effective in context and SocialNet.
- Uncertainty-Aware Fusion Module—takes in and fuses information while reducing conflicts and noise;
- The modular structure allows for flexible distribution and easy combination with existing network management tools.

3.3. Trust Representation

Trust between nodes is represented as a continuous value $T_{ij}(t) \in [0,1]$, indicating the perceived reliability of node$j$ by node i at time t. Direct manipulation of bounded values may lead to instability when evidence fluctuates. To address this issue, SDTE introduces a latent variable $z_{ij}(t)$ that captures the underlying reliability tendency.

Trust is obtained through a sigmoid mapping:

$$T_{ij}(t) = \sigma = \frac{1}{1 + e^{-z_{ij}(t)}}$$

Operating in the latent space allows additive updates and prevents abrupt oscillations in observable trust values. Small variations in evidence produce gradual changes in trust, improving stability in noisy environments.

3.4. Multi-Source Evidence Modeling

Trust evaluation in practical systems must consider diverse information sources. SDTE integrates four complementary components:

- Direct Behavioral Evidence (D_{ij}), derived from interactions between nodes;
- Indirect Recommendations (R_{ij}), provided by neighboring nodes;
- Contextual Factors (C_{ij}), describing environmental conditions or communication quality;
- Historical Memory (H_{ij}), representing accumulated past trust states.

The aggregated evidence is expressed as

$$E_{ij}(t) = w_D D_{ij}(t) + w_R R_{ij}(t) + w_C C_{ij}(t) + w_H H_{ij}(t)$$

where $w_D + w_R + w_C + w_H = 1$. Using adjustable weights allows the model to give greater or lesser weight to an information source depending on its use case. A multi-dimensional representation increases the reliability of the system because if an unreliable input is received from one source, then the same input can be compensated for from multiple sources.

3.5. Temporal Evolution Mechanism

Trust should be grounded on both recent interactions as well as long-term behaviour. In order to give recent observations greater importance, SDTE employs a sliding time window with exponential decay.
Let $\mathcal{W}(t)$ be an observation window. Each observation observed at time τ is given weight.

$$\omega(\tau) = e^{-\lambda(t-\tau)}$$

where λ controls the decay rate.
The latent trust state is updated as

$$z_{ij}(t+1) = \alpha z_{ij}(t) + \beta \sum_{\tau \in \mathcal{W}(t)} \omega(\tau) E_{ij}(\tau)$$

where α and β govern the degree to which memories fade. This formula allows the system to quickly identify consistent malicious behavior while reducing sensitivity to one-off anomalies.

3.6. Asymmetric Evidence Weighting

When performing reliability assessments, negative behavior typically has much more weight than positive behaviors. For example, one malicious action can negate many benign behaviors. SDTE accounts for this asymmetry by assigning much more influence to any negative evidence than to an equal amount of positive evidence.

$$E_{ij}^{*}(t) = \begin{cases} \beta^{+} E_{ij}(t), & E_{ij}(t) \geq 0, \\ \beta^{-} E_{ij}(t), & E_{ij}(t) < 0, \end{cases}$$

where $\beta^{-} > \beta^{+}$.
This mechanism prevents rapid trust recovery after malicious activity and improves resistance to intermittent strategies such as on–off attacks.

3.7. Uncertainty-Aware Evidence Fusion

Evidence from multiple sources may be incomplete, noisy, or contradictory: SDTE fuses them with a process inspired by evidence theory to explicitly model uncertainty.
Each piece of evidence contributes to a belief mass based on the value it provides and its confidence in that value. Conflicts between sources are reconciled through a process of normalization, preventing unreliable inputs from over-influencing the final result. This makes SDTE more robust to attack in adversarial environments where recommendations can be 'gamed'.

3.8. Distributed Implementation

The trust computation is performed locally by each node, which uses information from its interactions and information about its near neighbors. No single trusted authority or global knowledge is required.
The decentralized architecture shown in Figure 1 has the added benefits of reduced communication overhead and of not having a single-point-of-failure. As trust evaluation can continue when a part of the network is temporarily disconnected, our work is suitable for real IoT deployments.
Since our computations consist solely of simple arithmetic operations, and we use confined amounts of memory, our method can be executed on low-power devices like edge-gateways and embedded controllers.

3.9. Computational Complexity

Let d denote the average number of neighbors a node has. Updating trust for a single node is just O(d) since trust is computed based on local interactions. Unlike global propagation and consensus-based approaches, SDTE does not require operations to scale with the total number of nodes. Overall complexity grows linearly with growing network size, thus it makes the framework suitable for large scale deployments.

3.10. Summary

SDTE provides a distributed framework that combines temporal evolution, asymmetric weighting, and uncertainty-aware fusion, producing a lightweight distributed architecture that balances responsiveness, robustness, and efficiency to bring practical benefits to the trust management of large-scale IoT information systems. Exegesis of the framework by means of experimental evaluation is delegated to the following section.

4. Experimental Evaluation

4.1. Experimental Setup

To evaluate our SDTE framework, we performed experiments on scanning and DDoS datasets widely used in IoT security literature, such as IoT-23 [25] and Edge-IIoTset [26]. These data are those with benign and malicious traffic, along with activities like scanning, DDoSing, and data manipulation. They thus provide testing

scenarios for realistic IoT trust mechanisms in heterogeneous environments.
We simulate a distributed IoT formed of nodes that loosely interact with each other, with some services and recommendations. A configurable proportion of nodes act badly, forming false interactions or generating unreliable recommendations. Both long-term persistent malicious activity and intermittent on – off attack patterns are included. Experiments with varying-size networks are performed.
Trust values produced by SDTE are interpreted as an indication of reliability. Nodes whose trust goes beyond the pre-defined threshold are indicated by classifying them as malicious. This simple mechanism is reminiscent of practical applications. Trust scores could guide access control, routing, or other tasks.

4.2. Baseline Methods and Evaluation Metrics

SDTE was compared with representative trust management approaches from different categories:

- A static reputation model that aggregates historical interactions without temporal adaptation.
- A dynamic trust model based on sliding-window updates.
- A blockchain-based reputation framework emphasizing decentralized record keeping.

Anomaly detection using machine-learning techniques.
Using evaluation metrics such as detection accuracy, precision, recall, F1 score, and computation overhead, the evaluation metrics measure both the effectiveness of the solution from a security perspective and its operational viability in large-scale IoT environments.

4.3. Detection Performance under Varying Malicious Ratios

The accuracy versus proportion of the malicious nodes is shown in Fig 2. The SDTE shows consistent performance over many conditions, and thus demonstrates its robustness, even when a very high proportion of the nodes in the network are malicious.

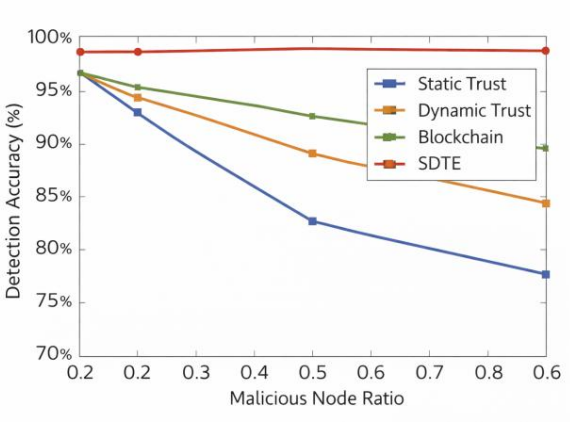

Figure 2. Detection accuracy versus malicious node ratio

Static models struggle with a higher ratio of malicious as they still rely on good values recommended by older and highly reputable nodes. Dynamic models without uncertainty detection are not immune to wrong values recommended by compromised nodes. Learning methods can perform with comparable accuracy, though at a greater cost.
All quantitative results across evaluation metrics are shown in Table 1.

Table 1. Performance comparison of trust management methods

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Avg. Update Time (ms)
Static Trust Model	86.7	84.5	82.3	83.4	3.2
Dynamic Trust Model	90.4	89.1	87.6	88.3	7.8
Blockchain-Based Framework	92.1	91.4	89.8	90.6	18.6
ML-Based Detection	93.3	92.5	91.7	92.1	21.4
SDTE (Proposed)	96.8	96.1	95.4	95.7	6.5

SDTE achieves the highest F1 score and overall accuracy among the evaluated methods, indicating balanced detection capability with reduced false positives.

4.4. Resilience to On–Off Attacks

Assaults that alternate rapidly and randomly. Malicious nodes alternate between acting normal and acting malicious to avoid being detected as a malicious node. The nodes were cycled between normal and malicious behavior

at various times to determine how susceptible we were to this attack method.
Figure 3 depicts the trust values in the same scenario.

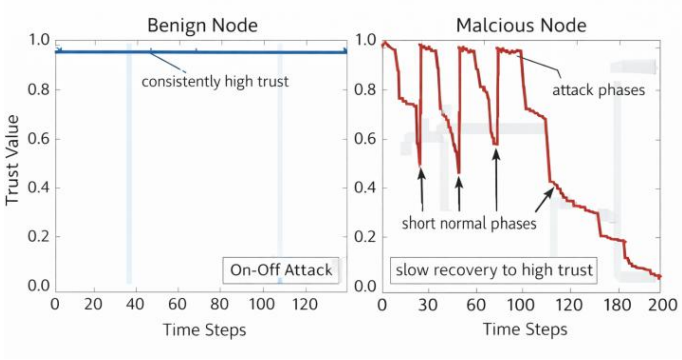

Figure 3. Trust evolution under on–off attack scenario

SDTE accelerates the decline of trust when things are malicious, but only allows slow recovery of trust during times that are non-malicious. Therefore, it prevents an attacker from regaining trust through the short time that they have a non-malicious act, which illustrates how effective asymmetric weights of evidence can be.

4.5. Scalability Analysis

Scalability is assessed by increasing the number of nodes while measuring computation time per trust update. Results are presented in Figure 4.

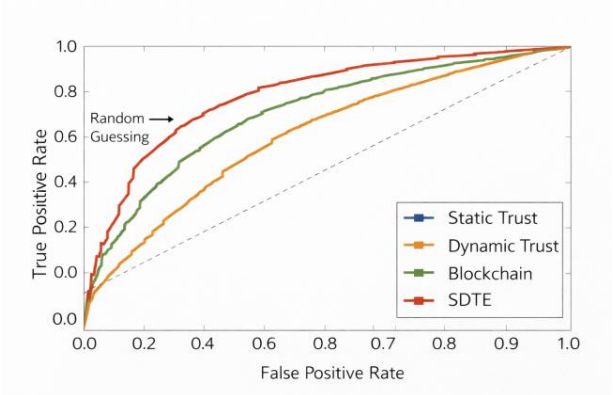

Figure 4. Scalability analysis with increasing network size

The growth in processing cost is approximately linear, which verifies that SDTE scales well due to its localized computations. In contrast, blockchain-based solutions have a higher latency due to consensus-related operations, while learning-based ones often require centralized processing.

In general, we conclude that SDTE is suitable for deployments with thousands of devices where resources for computation and communications bandwidth are limited.

4.6. Ablation Study

To evaluate the contribution of individual components, ablation experiments were performed by selectively disabling key mechanisms.

Table 2. Ablation study of SDTE components

Configuration	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
SDTE without Temporal Decay	92.4	91.6	90.2	90.9
SDTE without Asymmetric Weighting	90.7	89.8	88.5	89.1
SDTE without Uncertainty Fusion	91.2	90.3	89.1	89.7
SDTE without Indirect Recommendations	93.0	92.1	90.9	91.5
Full SDTE (Proposed)	96.8	96.1	95.4	95.7

Removing the aspect of asymmetric weighting significantly reduces the resistance of SDTE to intermittent attacks. Removing uncertainty-aware fusion increases the susceptibility of SDTE to unreliable recommendations, while the absence of temporal decay reduces the speed of adaptation to changes in behavior. Our results show that the effectiveness of SDTE is not due to one single component, but rather the joint influence of temporal modeling, asymmetric weighting, and evidence fusion.

4.7. Trust Evolution and Convergence Behavior

In addition to detection accuracy, the stability of trust values over time is critical for practical deployment. Figure 5 illustrates the evolution of trust for representative benign and malicious nodes.

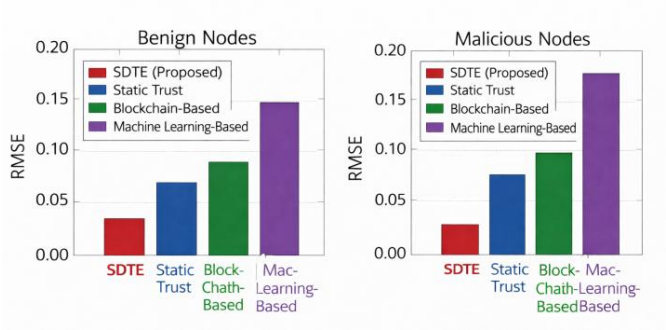

Figure 5. Convergence behavior of trust values

Trust values for a benign node approach high values incrementally over time after sufficient interaction, whilst malicious nodes have their value iteratively driven down. A decay that occurs exponentially leads to suitable stable convergence rather than oscillation, and shows that those techniques allow the appropriate trade-off between responsiveness and stability.

5. Discussion

5.1. Interpretation of Experimental Findings

Experimental results demonstrate that the SDTE framework is able to maintain a balanced detection performance in such evolving dynamic IoT environments. As illustrated in Figs. 2 and 3 and Table 1, SDTE maintains a high level of detection accuracy on varying malicious node ratios, showing robustness against large-scale adversarial presence. In contrast to static reputation models that respond only very slowly to changes in behaviour, SDTE is designed to adapt quickly because of its temporal evolution mechanisms. The trust trajectories in Figure 4 illustrate the effectiveness of our proposed asymmetric evidence weighting. During on – off attacks, trust of malicious nodes degrades rapidly and recovers only slowly in benign periods. This behaviour prevents attackers from regenerating high trust in a short space of time upon conducting short attacks and regenerating normal behaviour - a vulnerability exhibited by many of the symmetric trust models.

5.2. Deployment Feasibility

Scalability results shown in Figure 4 confirm that SDTE can operate efficiently in large networks. Since trust computation relies predominantly on local information and does not necessitate global coordination, the processing cost grows at most by a factor approximately linearly correlated with network size. This property is necessary for real deployments comprising thousands of heterogeneous devices.

The lightweight computational footprint also makes implementation viable on resource-constrained edge devices. Since SDTE does not depend on heavy learning/consensus methods, only basic arithmetic operations + bounded memory are necessary for trust evaluation to occur continuously without cloud connectivity or specialized hardware.

Furthermore, the distributed architecture improves resilience. Trust updates continue to be sent in the event of parts of the network becoming disconnected temporarily, thereby decreasing exposure to communication outages/infrastructure failures.

5.3. Applicability to Practical Scenarios

Continuous trust evaluation is most useful in contexts where the reliability of a device affects the performance of the evaluated systems, such as industrial monitoring systems, smart cities, or large-scale sensing networks, which may suffer from hardware degradation, software faults, or adversary compromise. The limit of convergence represented in Figure 5 suggests that SDTE is capable of maintaining stable estimates of trust over long periods of use. Benign nodes start to accumulate a considerable level of trust, while trust in malicious nodes drops considerably, which makes the information relevant for decision making, for instance, for access control, routing selection, or resource allocation.

5.4. Design Trade-offs

No single trust management mechanism can strike the optimal balance between all four attributes of accuracy, robustness, efficiency, and scalability. SDTE favours deployability and operational feasibility whilst retaining detection capability. Deep learning or global graph-based models may capture more challenging behaviour but require a centralised processing facility, loads of training data, and high compute. Conversely, overly simplified models get stupid quickly to the point of being useless at coping with changing targets. SDTE sits somewhere between the two, carefully targeting lightweight computation whilst fusing evidence in a principled fashion and projecting it over time. This may not always yield the highest absolute detection accuracy possible under every circumstance, but it represents a practical sweet spot for large distributed systems.

5.5. Limitations

While we certainly see many advantages, it is worth noting some limitations as well. To begin with, trust estimation depends on sufficient evidence from interactions. Nodes with only a limited communication history may not have reasonable trust values, particularly in cases of early deployment. Additional mechanisms may be needed for cold-starts.

Also, in this current version of the implementation, static parameters (like decay rates, evidence on actions, etc.) are

used. While parameters can be tuned for a particular environment taken into account less than optimal settings may degrade performance. Adaptive learning for parameters may provide more flexibility here.
Finally, the model presumes that the overwhelming majority of neighbors are "honest" nodes. If collusion is present on a large scale and neighbor recommendations may be manipulated in order to trip up the system, then trust estimates may be called into question. Cross-layer security, or complementary anomaly detection, may be needed for such cases.

5.6. Future Research Directions

Future work will focus on achieving greater adaptability and robustness in even more complicated environments. Some possibilities are updating parameters as the system conditions change over time, cooperating with learning-based anomaly detection methods, and validating these ideas in real operational deployments. There is also much to be gained in looking at its resilience to coordinated large-scale attacks and trust interoperability in cross-domain settings.

6. Conclusion

This paper proposed a Scalable Dynamic Trust Evolution (SDTE) framework for large-scale IoT information systems, which overcomes the shortcomings of traditional trust management that depend on static assumptions or central processing. By modeling trust as a dynamic latent state shaped by heterogeneous evidence, the framework offers an effective evaluation of device behavior under dynamic and uncertain conditions. The proposed method combines temporal evolution, asymmetric evidence weighting, and uncertainty-aware fusion in a lightweight distributed manner, enabling quick adaptation to changes in behavior while remaining stable in the presence of noise. Contrary to many existing solutions, SDTE does not require global coordination or complex computation, making it suitable for deployment in a multitude of systems consisting of resource-constrained devices.
Comprehensive tests on publicly available IoT datasets have shown that SDTE obtains good overall detection performance for varying malicious ratio percentages, regardless of the size of the network, remains robust to intermittent on–off attacks, and scales well. The results show that each of the design components contributes to the overall effectiveness of SDTE, hence illustrating that, when developing these models, combining temporal modelling with effective evidence fusion techniques is beneficial.
On the practical side, its decentralized nature and low computation requirements allow continuous trust assessments in environments where trust is essential, as the method can be applied on the fly on top of existing infrastructures to make decisions, such as access control, service selection, and anomaly mitigation.
While the experimental results are promising, a number of challenges remain. Trust estimation could be less accurate in environments with sparse interaction, and parameter settings need tuning for different deployment conditions. Future work will consider issues of adaptive parameter tuning, their integration with complementary security mechanisms, and validation on operational systems.
In summary, the SDTE framework provides a scalable implementation of a trust manager for the IoT, offering a practical trade-off among robustness, efficiency, and deployability.

Author Contribution

T. Sun performed all the tasks, including conceptualization, methodology, software, validation, formal analysis, investigation, resources, data curation, writing—original draft preparation, writing—review and editing, visualization, supervision, project administration, and funding acquisition. The author has read and agreed to the published version of the manuscript.

Data Availability Statement

The datasets supporting the findings of this study are publicly available: IoT-23 [25] (Zenodo, doi: 10.5281/zenodo.4743746) and Edge-IIoTset [26] (IEEE Dataport, doi: 10.21227/mbc1-1h68). No new data were generated in this study.

Acknowledgements

This research was funded by Guangzhou Academy of Fine Arts 2026 Research Project Program, grant number 26XSB01.

Ethics Statement

Not applicable

Conflict of interest statement

The authors have no relevant financial or non-financial interests to disclose.

References

[1] R. Molose and B. Isong, "A survey of multi-layer IoT security using SDN, blockchain, and machine learning," Electronics, vol. 15, no. 3, p. 494, 2026.
[2] A. M. Konsta, A. L. Lafuente and N. Dragoni, "A Survey of Trust Management for Internet of Things," in IEEE Access, vol. 11, pp. 122175-122204, 2023.
[3] G. D'Aniello and L. Fotia, "Blockchain and AI-based methods for trust management in IoT: a comprehensive survey," Internet of Things, Vol. 34, no. 101755, 2025.

[4] A. Rehman Khan, K. Ahmad Awan, F. F. Alruwaili, A. Ara, H. Herbert Song, and T. Saba, “Trust-enhanced lightweight security framework for resource-constrained intelligent IoT systems,” IEEE Internet of Things Journal, vol. 12, no. 8, pp. 10175–10182, 2025.
[5] Y. Wang, A. Mahmood, M. F. M. Sabri, and H. Zen, “Trust management in the Internet of Vehicles: A survey of the state-of-the-art,” IEEE Open Journal of Intelligent Transportation Systems, vol. 7, pp. 516-536, 2026.
[6] O. Kuznetsov, I. Lysenko, D. Prokopovych-Tkachenko, Y. Ulianovska, and V. Bushkov, “Dynamic trust evaluation and resilience assessment in edge computing networks,” International Journal of Computing, vol. 24, no. 2, pp. 223–232, 2025.
[7] D. Chen, G. Chang, D. Sun, J. Li, J. Jia, and X. Wang, “TRM-IoT: A trust management model based on fuzzy reputation for internet of things,” Computer Science and Information Systems, vol. 8, no. 4, pp. 1207–1228, 2011.
[8] Y. Wang, I. R. Chen, J. J. P. C. Rodrigues, D. C. C. Chang, and H. C. Chao, “CATrust: Context-aware trust management for service-oriented ad hoc networks,” IEEE Transactions on Services Computing, vol. 11, no. 6, pp. 908–921, 2018.
[9] Y. Alghofaili and M. A. Rassam, “A dynamic trust-related attack detection model for IoT devices and services based on the deep long short-term memory technique,” Sensors, vol. 23, no. 8, p. 3814, 2023.
[10] F. Jabeen, Z. U. R. Khan, Z. Hamid, R. Rehman, and A. Khan, “Adaptive and survivable trust management for Internet of Things systems,” IET Information Security, vol. 15, no. 5, pp. 375–394, 2021.
[11] Z. Tu, H. Zhou, K. Li, H. Song, and Y. Yang, “A blockchain-based trust and reputation model with dynamic evaluation mechanism for IoT,” Computer Networks, vol. 218, p. 109404, 2022.
[12] G. Fortino, F. Messina, D. Rosaci, and G. M. L. Sarné, “Using blockchain in a reputation-based model for grouping agents in the Internet of Things,” IEEE Transactions on Engineering Management, vol. 67, no. 4, pp. 1231–1243, 2020.
[13] E. Meybodian, S. Mostafavi, T. Dargahi, and V. Ranjbar Bafghi, “Secure and scalable trust management in IoT: A hierarchical blockchain-based approach,” Computers & Electrical Engineering, vol. 127, p. 110631, 2025.
[14] N. Khodjamov, S. Yang, K. Sharif, Y. Gao, F. Li, Y. Wang, S. Mamarasulov, and L. Zhu, “Blockchain-based secure trusted clusters for multi-tiered Social IoT environments in edge-cloud networks,” Computer Networks, vol. 275, p. 111880, 2026.
[15] K. Ahmad Awan, I. Ud Din, A. Almogren, Z. Han, and M. Guizani, “TrustAware-GNN: Graph-neural-network-based trust management for IoT anomaly detection,” IEEE Internet of Things Journal, vol. 12, no. 18, pp. 37670–37681, 2025.
[16] N. M. Al-Maslamani, M. Abdallah, and B. S. Ciftler, “Reputation-aware multi-agent DRL for secure hierarchical federated learning in IoT,” IEEE Open Journal of the Communications Society, vol. 4, pp. 1274–1284, 2023.
[17] M. Termos, Z. Ghalmane, M.-A. Brahmia, A. Fadlallah, A. Jaber, and M. Zghal, “ADAP-GNN: Adaptive property-aware graph neural network for intrusion detection in IoT networks,” Computers & Electrical Engineering, vol. 133, p. 111051, 2026.
[18] S. Chockalingam, S. Pirbhulal, S. Misra, P. Kvalvik, and H. Abie, “FedTrust: Modelling adaptive trust-risk for IoT-enabled federated decentralized systems,” in Proc. IEEE Vehicular Technology Conf. (VTC), Jun. 2025, pp. 1–6.
[19] R. Ul 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, 2025.
[20] H. Yang, L. Guo, T. Wang, and C. Lv, “A novel lightweight dynamic trust evaluation model for edge computing,” IEEE Transactions on Network and Service Management, vol. 22, no. 4, pp. 3542–3554, 2025.
[21] V. Padmavathi and R. Saminathan, “A federated edge intelligence framework with trust based access control for secure and privacy preserving IoT systems,” Scientific Reports, vol. 15, p. 35832, 2025.
[22] K. Herath, S. Mahangade, and S. Bagchi, “A lightweight reputation-based mechanism for incentivizing cooperation in decentralized federated learning,” in Proc. 55th Annual IEEE/IFIP Int. Conf. Dependable Systems and Networks Workshops (DSN-W), Naples, Italy, Jun. 23–26, 2025, pp. 298–304.
[23] D. Ferraris, C. Fernandez-Gago, Y. Assouyat, H. Labiod, and W. Haiguang, “Trust dynamicity for IoT: How do I trust your social IoT cluster?” Internet of Things, vol. 30, p. 101529, 2025.
[24] B. Hathout, P. Shepherd, T. Dagiuklas, K. Nagaty, A. Hamdy, and J. Rodriguez, “Adaptive trust management for data poisoning attacks in MEC-based FL infrastructures,” IEEE Open Journal of the Communications Society, vol. 6, pp. 3140–3160, 2025.
[25] Sebastian Garcia, Agustin Parmisano, & Maria Jose Erquiaga. IoT-23: A labeled dataset with malicious and benign IoT network traffic (Version 1.0.0) [Data set]. Zenodo, 2020. http://doi.org/10.5281/zenodo.4743746.
[26] Mohamed Amine Ferrag, Othmane Friha, Djallel Hamouda, Leandros Maglaras, Helge Janicke, "Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications: Centralized and Federated Learning", IEEE Dataport, January 18, 2022, doi:10.21227/mbc1-1h68
[27] Ma Z, Wei H, Jiang J, Wang B, Wang H, Di Z. A lightweight zero-trust authentication architecture for IoT via unified enhanced FAST-SM9 and dynamic re-authentication. PLoS One 20(10): e0332943, 2025.