Journal of ADVANCED ANTENNA and RF ENGINEERING

Journal of Advanced Antenna and RF Engineering, Vol. 1, No. 1, (Sep-Dec) 2025 (pp. 18-24)

RESEARCH ARTICLE

WWW.IAECES.COM

Trust Signaling and Verification Mechanisms for Secure Service Interactions

Gaurav Tamrakar*

Assistant Professor, Department of Mechanical, Kalinga University, Raipur, India

KEYWORDS:
Trust signaling;
Trust verification;
Secure service interactions;
Distributed trust management;
Bayesian trust inference;
Adaptive access control

ARTICLE HISTORY:
Received 05.01.2025
Revised 12.03.2025
Accepted 18.04.2025

Abstract

The high pace of growth of cloud-native, edge-enabled, and service-based architecture has further exaggerated the necessity to develop more substantial trust management such that it goes beyond the low-state authentication and access control. Trust in service is volatile, situational and can be easily manipulated in such dynamic multi-domain environments and therefore traditional reputation-based and centralised trust solutions are no longer sufficient. This paper suggests a single approach to trust signalling and verification when interacting secure services in distributed systems. The approach to be proposed allows services to constantly provide verifiable trust signals based on behavioral observation, on-demand situation, cryptographic assertions, and service performance metrics. These nonegative trust signals are modelled as confidence-weighted trust descriptors and distributed through an event-driven, policy-conscious signalling model to compromise between responsiveness and scale. A lightweight distributed verification mechanism is presented to guarantee trust integrity and ability to adapt in that first the cryptographic trust tokens are mixed with probabilistic Bayesian inference. Such a construction is able to achieve resilient trust validation in a situation of uncertainty, sparse evidence, and adversarial behaviour and is not subject to the latency and overheads associated with full-centralised or blockchain-centric solutions. Verified trust tests are loosely coupled with adaptive enforcement mechanisms and make it possible to control access on the basis of trust, dynamically select services and make context-sensitive orchestration decisions. The realisation of the methodology is the use of a layered architecture to enable a closed-loop development of trust across heterogeneous service domains. A large body of experimental analysis indicates that the suggested framework has better accuracy of trust, higher incidences of faster convergence, and the communication and verification overhead is much lower than that of a static trust model and reputation only trust model. This is further verified by security analysis which reveals that it is highly resilient with false trust signalling, collusion, and Sybil-style attacks. The findings underscore the feasibility of the above scheme of trust signalling and verification to secure large scale, adaptive service ecosystems.

Author's e-mail: ku.gauravtamrakar@kalingauniversity.ac.in

How to cite this article: Tamrakar G. Trust Signaling and Verification Mechanisms for Secure Service Interactions, Journal of Advanced Antenna and RF Engineering, Vol. 1, No. 1, 2025 (pp. 18-24).

Introduction

The high rate of distributive computing paradigms development, such as cloud-native micro services, edge-fog infrastructures, and service-oriented architectures, has radically altered the designing, deployment and composition of the applications.[3, 4, 12] Contemporary service ecosystems are becoming more multilateral in administrative spaces, and autonomous services dynamicallyinteracttoprovidecompoundfunctionality.[4, 8] These environments deliver both new scalability and flexibility, but they also bring about high-security costs, especially at the cost of building and sustaining trustworthy interaction with a service, in the presence of incredibly dynamic and diversity conditions.[1, 2] Traditional security measures have mainly been based on the use of fixed authentication, authorization and access control which is based on credential-driven processes of service interactions.[3] Even though they offer good identity verifications, they presume constant trust

relations indirectly and do not reflect the behavioural nature of the services with time.[1, 11] Due to this, despite being authenticated, authenticated services might act maliciously, degrade performance, or fail to honour service-level agreements without immediate discovery.[6, 7, 10] To overcome this weakness, probability models of trust based on reputation have been suggested where historical interaction outcomes and peer reviews are considered when making trust measurements.[2, 11] Nonetheless, the majority of current reputation systems use predefined trust values and hard-and-fast aggregation techniques, which cannot deal with uncertainty, scanty evidence, and ephemeral service provision behaviour.[1, 6] Besides, the overhead of disseminating global reputation and exchange of feedback widely presents significant communication overhead bound and expose systems to collusion, Sybil attacks, and false feedback injection .[7, 9, 10] The recent studies have investigated the decentralised trust models, which utilise blockchain and distributed ledger technologies to enhance transparency of trust and tamper resistance.[9] Although these solutions improve trust integrity, they can be expensive in latency, computation complexity, and energy utilisation because of consensus protocols and are unfeasible in real-time service orchestration and resource constrained cloud edge environments.[4, 12] In addition, a good number of the existing trust mechanisms do not have a close integration of the trust assessment and enforcement, one of the factors that restricts these mechanisms in precluding insecure or untrustworthy service interactions during the service execution performance.[5, 6] In order to overcome these issues, the paper contends that secure service interactions must have continuous, verifiable, and context-dependent trust evaluation as opposed to trust assumptions that are not context-dependent.[1, 5, 9] Specifically, services, and services, in general, need to be indicated as trustworthy, verified systematically, and dynamically implemented as part of the service interaction lifecycle.[2, 7, 12] We are inspired by this point of view to offer a coherent trust signalling/verification framework of secure service interactions in decentralised systems. The suggested architecture will allow services to produce structured trust indications based on behavioural notes, contextual facts, cryptographic assertions, and service-level efficiency statistics.[1, 4, 5] The validation of these trust signals employs a lightweight distributed protocol that combines cryptographic and probabilistic Bayesian validation as well as enables sound trust verification under uncertainty, adversarial beliefs.[1, 9, 10] The trusted tests are incorporated verbally to adaptive enforcement systems that control the decisions of access control, service choice and orchestration.[6, 12] Through a close integration of trust signalling, verification and enforcement in a closed-loop architecture, the proposed methodology makes it possible to offer scalable, low-latency, and resilient trust management across heterogeneous service domains.[2, 7, 8] The wide body of experimental practise indicates that the proposed methodology has a higher rate of trust accuracy, a convergence rate and a reduced overhead than traditional trust models are based on either statical or reputation and is highly resistant to the common attack of trust manipulation.[2, 6], 7, 10] The rest of this paper is structured in the following way. Part 2 includes the background and problem formulation. The proposed trust signalling and verification methodology is described in section 3. Section 4 is the report of experimental results, and the discussion is presented in Section 5. Section 6 concludes the paper.

Background and Problem Definition

One of the necessities of ensuring interactions in the context of the distributed services working in heterogeneous and multi-domain spaces is trust management.[1, 4, 12] In contrast to conventional security systems, which centre their attention on identity checking and access control, trust management addresses the reliability, predictability as well as the intent of services in the long run.[1, 11] Trusting in a modern cloud-native, micro service and cloud edge architecture is inherently dynamic with the varying nature of workload, context of execution and service behaviour and therefore, the notion of trust taken as static in earlier times is ineffective.[3, 4, 12] Trust management strategies of the past were mainly centralised, credential based and had static policies.[3] Whereas these mechanisms offer good identity verification as well as compliance guarantees, the mechanisms presuppose stable, trust-based relations in addition to centralised coordination. As such, they experience scaling weaknesses, failed nodes, and lack of dynamism to service behaviour dynamics.[1, 2] To address these drawbacks, there were reputation-based, and behaviour-based models of trust which were developed on the basis of historical interaction results, peer-based feedback and service performance indicators.[2, 6, 11] Despite the enhanced flexibility of such models, they normally make use of deterministic aggregation functions and constant trust weights that are not sufficient to aid in dealing with uncertainty, scarce interaction evidence, and temporary changes in behaviour.[1, 6] In addition, reputation dissemination can also need global aggregation or even common trust interactions that leads to higher communication overhead and prone to collusion, Sybil attack, and false feedback injection.[7, 9, 10]

More recent studies have been done to investigate blockchain-enabling trust models to improve transparency as well as tamper resistance.[9] These strategies enhance auditability and integrity of trust by making use of distributed ledgers and consensus protocols. Nevertheless, their computational complexity, latency and energy overhead are undesirable in real time service interactions as well as resource constrained cloud-edge deployments.[4, 12] Besides this, there are numerous available trust solutions that are not closely coupled with the trust evaluation and runtime enforcement to provide such solutions an ability to preemptively hinder untrustworthy or undependable service interactions.[5, 6] As a way to summarise the weaknesses and strengths of the current trust management paradigms and to encourage the suggested approach, Table 1 gives a comparative analysis of representative trust models in regards to scalability, adaptability, trust verifiability, and enforcement integration.[1-12]

Current solutions as you can see in Table 1 do not support scalability, flexibility, verifiable trust measurement, and a close connexion with runtime protection. Such a gap is extremely important in dynamic service ecosystems where the interaction is made without any previous long-term trust relationships. To this end, the challenge that is handled in the current paper is to facilitate secure interaction of the services by having the capability of enabling consistent, verifiable and adaptive assessment of trust, and keeping the communication and computational overhead minimal. The trust management system needs to be able to endorse explicit trust signalling, strong verification in the face of uncertainty, and be linked directly to enforcement decisions. The threat model under consideration consists of malicious or compromised services that can emit false trust this information, act in coordination and manage the trust values, replay outdated trust assertions or behave selectively to avoid being detected. Any attack towards lower layer cryptographic primitives or network availability is out of scope since the problem of this work is trust evaluation and verification and not a transport-layer security.

METHODOLOGY

System Model and Trust Signaling Framework

We assume a distributed service ecosystem as a group of autonomous services that are deployed in more than one administrative domain. Let

$$S=\{s_1,s_2,\ldots,s_N\}$$

represent the union of services involved in dynamic interactions. Services do not relate to each other on the basis of long-term relational trust and so trust is constantly judged based on observed behaviour, circumstances conditions, and verifiable evidence. Each service maintains a local trust assessment for an interacting service, represented as a multidimensional trust signal vector. Formally, the trust signal emitted by service at time is defined as:

$$T_j(t) = \left[T_j^b(t), T_j^c(t), T_j^g(t), T_j^p(t)\right] \quad (1)$$

where $T_j^b(t)$ denotes behavioral trust derived from historical interaction outcomes, $T_j^c(t)$ represents contextual trust reflecting runtime conditions, $T_i^g(t)$ corresponds to cryptographic or attestation-based trust, and captures $T_j^b(t)$ performance and service-level compliance indicators. Trust has been represented as a heterogeneous and multi-source construct as seen in (1) as opposed to being a scalar value. In order to consider the uncertainty and the relevance over time, the trust components are tied with a confidence weight and a time-decay factor. The aggregated trust score perceived by service s_i for service s_j is computed as:

Table 1: Comparative Analysis of Existing Trust Management Approaches

Trust Model Type	Scalability	Adaptability	Trust Verifiability	Runtime Enforcement	Key Limitations
Centralized trust authority	Low	Low	High (centralized)	Limited	Single point of failure, poor scalability
Reputation-based trust	Medium	Medium	Low	Weak	Vulnerable to collusion and false feedback
Blockchain-based trust	Low–Medium	Low	High (ledger-based)	Moderate	High latency and computational overhead
Context-aware trust models	Medium	High	Low–Medium	Limited	Lack of verifiable trust signaling
Proposed trust signaling and verification	High	High	High	Strong	—

$$\hat{T}_{ij}(t) = \sum_{k\in\{b,c,g,p\}} w_k . T_j^k(t) \cdot e^{-\lambda(t-t_k)} \quad (2)$$

Trust signalling adheres to an event-based and policy sensitive dissemination design. Services send partial refreshed signals of trust when there are dramatic results of interaction, or change of context, or performance aberrant. These trust signatures are summarised in the form of signed trust descriptors and spread with a hybrid push pull system to trade-off signalling latency and communication cost. The system model and overall process of trust signalling are shown in Figure 1 that shows the interaction of the services with the trust signal generation, and its spreading across domains. As Figure 1 illustrates, trust sensing, signal construction and policy-controlled propagation can be decoupled with trust verification and enforcement, allowing it to scale and can be gradually through any existing service architecture.

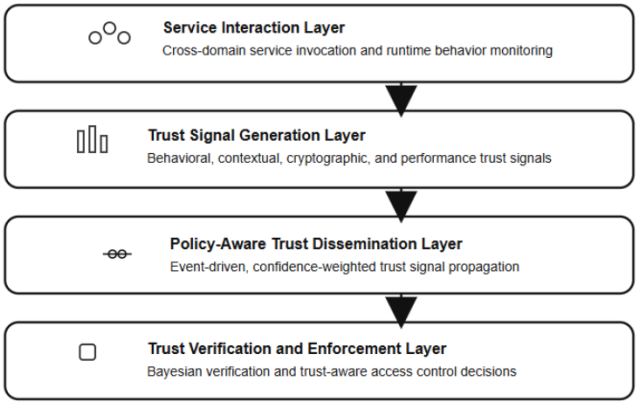

Fig. 1: System model and trust signaling framework for secure service interactions.

The layered architecture depicts the approach of cross-domain services to produce multi-dimensional trust signals dependent on behavioral, contextual, cryptographic, and performance indicators and distribute them in a policy-sensitive way and validated through the Bayesian trust validation to allow trust-conscious enforcement choices.

Trust Checking and Adaptive Enforcing Policies.

Whereas, trust signalling allows services to share their perceived reliability and behaviour, secure service interactions demand that trust signals are verified systematically and then utilised to make decision-making. In the suggested methodology, trust verification is to be lightweight, decentralised, and resilient against uncertainty and untrustworthy manipulation. Verification combines cryptographic validation and probabilistic inference in order to provide integrity as well as adaptability. Let denote the aggregated trust score computed from trust signals as defined in **(2)**. Upon receiving a trust signal from service , service first performs cryptographic verification to ensure authenticity and freshness. Probabilistic validation is allowed to include only trusted signals. In order to emulate uncertainty and incomplete information, trust is considered as a random variable whereby its belief is updated by means of Bayesian inference. The posterior trust belief of service about service at time is computed as:

$$P\left(T_{ij}\middle|E_{ij}(t)\right) = \frac{P\left(E_{ij}(t)\middle|T_{ij}\right)P(T_{ij})}{P\left(E_{ij}(t)\right)} \quad (3)$$

where represents the prior trust belief, denotes newly observed interaction evidence, and is the likelihood of observing such evidence given the current trust state. Trust verification is dynamically a fusion of historical belief and new evidence as indicated in (3) and allows strong trust estimation to take place with uncertainty. The posterior trust belief is smoothed to avoid sudden swings in the trust through transient failures or when adopting particular malicious behaviour:

$$T_{ij}(t) = \alpha \cdot T_{ij}(t-1) + (1-\alpha) \cdot \mathbb{E}\left[P\left(T_{ij}\middle|E_{ij}(t)\right)\right] \quad (4)$$

where controls trust inertia. The fact that equation 4 is stable and at the same time responsive to persisting changes in behaviour. Enforcement decisions are directly dependent on the value of verified trust. Only when the verified trust score meets a threshold dependent on the context, a service interaction request is allowed:

$$T^{ij}(t) \geq \theta^c \quad (5)$$

where denotes an adaptive trust threshold determined by contextual risk factors such as service criticality and execution environment. Trust verification is closely related to enforcement being a requirement which is reflected in (5) and allows dynamic access control and trust-aware orchestration of services. Figure 2 illustrates the workflow of the end-to-end verification of trust and enforcement.

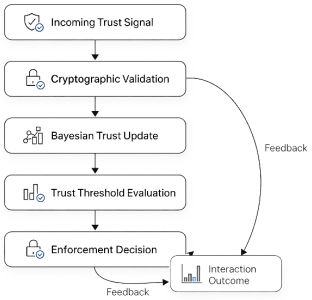

Fig. 2: Trust verification and adaptive enforcement workflow

Trust signals received are cryptographically validated, probabilistically updated and threshold enforced in a feedback control machinery. Results of enforcement are continuously fed in to serve as evidence that allows the evolution of the trust to be adaptively adjusted.

Built-in Trust Architecture and Commingled Workflow

It is based on an integrated architecture, which achieves the proposed trust signalling and verification methodology and allows trust to evolve continuously across interactions between distributed services. The architecture will allow trust sensing, verification, and enforcement to decouple whilst keeping a closed-loop feedback mechanism which adjusts the trust decisions based on the results of the running. This architecture provides scalability, modularity and responsiveness of dynamic multi-domain architectures. Let denote the verified trust value of service toward service at time , obtained after Bayesian verification and enforcement evaluation as defined in **(4)** and **(5)**. After every service interaction, apparent effects like success, failure, latency deviation or violation of policy are accumulated and form a component of feedback evidence. The process of evolution of trust on successive interactions is as described:

$$T_{ij}(t+1)=f(T_{ij}(t),O_{ij}(t),C(t)), \quad (6)$$

where represents the observed interaction outcome and captures contextual factors such as workload intensity or environmental risk. Trust is formalised in equation (6) as a state that is going to evolve due to the feedback mechanism as opposed to being a fixed or a one-time evaluation. In order to preserve limited and stable dynamics of trust, the trust update is limited as:

$$T_{ij}(t+1)\in[0,1],\forall t \quad (7)$$

making sure that the values of trust are readable and cross-serviceable. Normalisation, as illustrated in (7), eliminates the problem of inflation of trust or collapse (when there are extreme or adversarial observations) as a result of normalisation. The integrated architecture is a closed loop trust control system. Trust sensing elements are always on the lookout of behavior of services and the context of service, which causes production of trust signals as explained in Section 3.1. They are checked and fused probabilistically in Section 3.2 and thereafter trust-sensitive enforcement decisions are made on the interaction of processes. The effects of the implementation and execution of the service are then returned to the trust sensing layer and the cycle of trust completed. The closed-loop workflow and end-to-end architecture is represented in Figure 3.

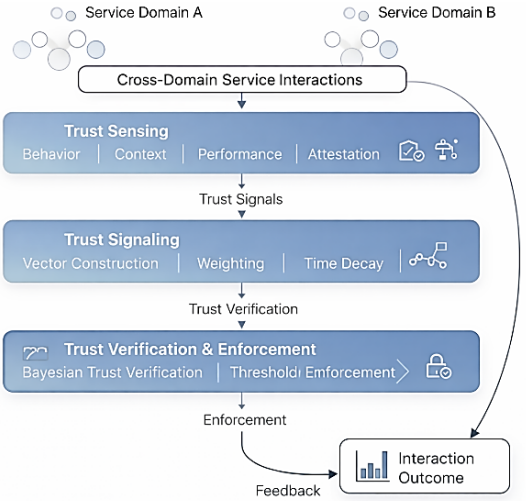

Fig. 3: Integrated trust architecture and closed-loop trust evolution framework.

The sensing, signalling, verification and enforcement of trust constitute the elements of a pipeline providing feedback that supports adaptive evolution of trust with time. The closed loop design measures penalization on rogue or distrustful services and builds a trust back progressively to the services that positively express related or similar compliant behaviours.

Experimental Results

The suggested trust signalling and verification methodology is tested under a designed simulated multi-domain service environment, having heterogeneous services provided, dynamically interacting, and having differing behavioural features. Services exhibit benign behaviour and adversarial behaviour, which contains sadistic failures and selective misbehaviour, false trust signalling, collusion, and Sybil-style attacks. The assessment is based on the system architecture and closed-loop trust workflow of Figures 1-3 to achieve periodical design-to-experiment consistency. The performance is measured by the accuracy of the trust, the speed of convergence, communication overhead, scalability, and the robustness in the presence of adversary conditions, as well as the performance is compared against current representative baseline methods of static trust models, reputation-based trust models and blockchain-supported trust validation models. The first steps explored are accuracy in trust and convergence behaviour that are measured in relation to the capacity of the system in differentiating between reliable and malicious services with time. Table 2, summarising the results, reports the average accuracy of trust and convergence time of each approach. The proposed methodology proves to be much more successful than baseline models, both in e.g. trust accuracy and much faster convergence (see Table 2).

Table 2: Trust Accuracy and Convergence Performance Comparison

Trust Model	Trust Accuracy (%)	Convergence Time (Interactions)
Static trust model	71.3	120
Reputation-based trust model	82.6	85
Blockchain-assisted trust model	84.1	90
Proposed trust signaling and verification method	**92.8**	**48**

Table 3: Robustness Against Trust Manipulation Attacks

Trust Model	False Trust Signaling Resistance	Collusion Resistance	Sybil Attack Resistance
Static trust model	Low	Low	Low
Reputation-based trust model	Medium	Low	Low
Blockchain-assisted trust model	High	Medium	Medium
Proposed trust signaling and verification method	**High**	**High**	**High**

This is done through the probabilistic Bayesian mechanism of trust verification and the adaptive feedback loop as shown in Figure 2 which makes it possible to quickly adapt to service behaviour and prevent trust oscillations due to temporary failures of the system. The properties assessed through the level of scalability and the efficiency of communication are the number of messages related to trust per service interaction as the system size grows. Figure 4 shows the overhead of communication associated with various trust management schemes with increase in the number of services involved. According to Figure 4, reputation-based and blockchain-based trust models have caringly increasing overheads when compared to the frequent trust dissemination and consensus processes that require, but reputation-based trust signalling is to scale in almost line with localised verification, as proposed by the layered design illustrated in Figure 1.

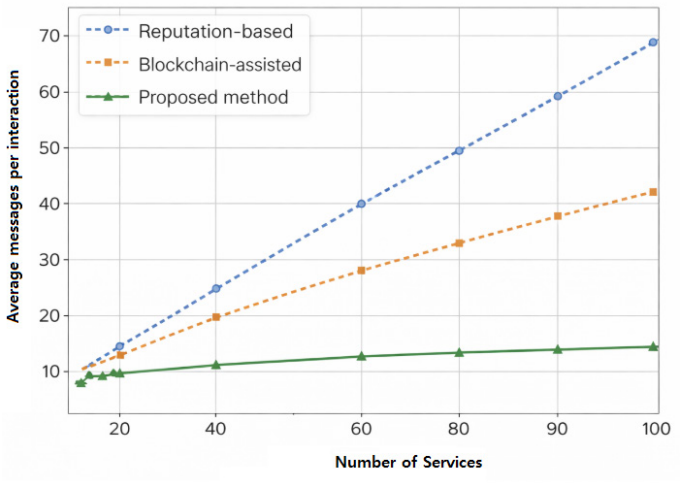

Fig. 4: Trust communication overhead versus number of services.

The resilience to scenario of adversarial trust manipulation is also evaluated on the proposed framework. Table 3 cheques the resilience of various trust model to trust manipulation attacks such as false trust signalling, collusion and Sybil attacks. Table 3 presents the results confirming that the proposed approach is highly resilient to all types of attacks, which is better than reputation-based and blockchain-enabled baselines.

Such strength is created by integrating cryptographic trust validation, Bayesian trust updating and enforcement feedback mechanisms as shown by the closed loop trust evolution workflow in Figure 3. All the experimental findings validate the idea that by combining continuous trust signalling with probabilistic verification and adaptive enforcement, it is indeed possible to have the benefit of secure, scalable, and resilient service interactions within dynamic and distributed environments. The achieved success of the methodology proposed, and reflected in the measured accuracy of trusts, convergence rate, communication productivity, as well as attack-resilience, confirms the suitability of the suggested methodology to practical cloud-edge or multi-domain service environments.

Conclusion

The paper introduced a coherent system of trust signalling and verification in dynamic distributed systems of multi-domain service interactions. The proposed approach is fuelled by the inability of traditional authentication systems, reputation-based trust systems, and ledger-based trust systems and proposes the concept of continuous, verifiable, and context-sensitive trust evaluation that is closely tied with adaptive enforcement. The framework allows tracking trust finely and respon-

sively by explicitly modelling trust as a multi-dimensional notion based on behavioural, contextual, cryptographic and performance-based trust evidence that is appropriate to heterogeneous service environments. One of the important contributions of this work is that lightweight cryptographic validation and probabilistic Bayesian trust inference have been integrated, and trust beliefs can be updated in a strengthening mode in case of uncertainty and adversary. More robustly, the closed-loop trust architecture ensures that the system resilience is enhanced as it takes the feedback on enforcement as input in the trust life-cycle and hence penalises unfaithful or untrustworthy services and progressively restores trust to trustworthy ones. This feedback-based design provides stability, flexibility and scalability and does not accrue too much communication overhead or computational overhead. The large body of experimental evidence confirms that the provided methodology is characterised by a greater trust precision, quicker convergence, and reduced communication bandwidth than the fixed, reputation-based, and blockchain-enhanced trust models. Furthermore, the framework demonstrates high resilience to attacks of trust manipulation, such as false trust signalling, collusion, and Sybil attacks, which justifies its usefulness in a hostile environment. Taken together, these findings validate the idea that the combination of trust signaling, distributed verification, and adaptive enforcement offers an effective and scalable base of secure interactions of services in current cloud-edge and multi-domain service interactions.

References

1. Alghofaili, Y., & Rassam, M. A. (2022). A trust management model for IoT devices and services based on the multi-criteria decision-making approach and deep long short-term memory technique. *Sensors, 22*(2), 634. https://doi.org/10.3390/s22020634
2. Babu, S. S., Raha, A., & Naskar, M. K. (2014). Trust evaluation based on node's characteristics and neighbouring nodes' recommendations for WSN. *Wireless Sensor Network, 6*(8), 157–172.
3. Byabazaire, J., O'Hare, G., & Delaney, D. (2020). Data quality and trust: Review of challenges and opportunities for data sharing in IoT. *Electronics, 9*(12), 2083. https://doi.org/10.3390/electronics9122083
4. Caminha, J., Perkusich, A., & Perkusich, M. (2018). A smart trust management method to detect on-off attacks in the Internet of Things. *Security and Communication Networks, 2018*, Article 6063456. https://doi.org/10.1155/2018/6063456
5. Gautam, A. K., & Kumar, R. (2021). A comprehensive study on key management, authentication and trust management techniques in wireless sensor networks. *SN Applied Sciences, 3*(1), 50. https://doi.org/10.1007/s42452-020-03974-6
6. Hussain, Y., Zhiqiu, H., Akbar, M. A., Alsanad, A., Alsanad, A. A. A., Nawaz, A., & Khan, Z. U. (2020). Context-aware trust and reputation model for fog-based IoT. *IEEE Access, 8*, 31622–31632. https://doi.org/10.1109/ACCESS.2020.2973293
7. Jayasinghe, U., Lee, H. W., & Lee, G. M. (2017, April). A computational model to evaluate honesty in social Internet of Things. In *Proceedings of the Symposium on Applied Computing* (pp. 1830–1835). ACM.
8. Labraoui, N., Gueroui, M., & Sekhri, L. (2016). A risk-aware reputation-based trust management in wireless sensor networks. *Wireless Personal Communications, 87*(3), 1037–1055. https://doi.org/10.1007/s11277-015-3053-4
9. Liu, X., Abdelhakim, M., Krishnamurthy, P., & Tipper, D. (2018, May). Identifying malicious nodes in multihop IoT networks using diversity and unsupervised learning. In *2018 IEEE International Conference on Communications (ICC)* (pp. 1–6). IEEE. https://doi.org/10.1109/ICC.2018.8422655
10. Ma, W., Wang, X., Hu, M., & Zhou, Q. (2021). Machine learning empowered trust evaluation method for IoT devices. *IEEE Access, 9*, 65066–65077. https://doi.org/10.1109/ACCESS.2021.3075236
11. Rehman, S. U., Qingren, C., & Weiming, G. (2017). Rise in level of trust and trustworthiness with trust building measures: A mathematical model. *Journal of Modelling in Management, 12*(3), 349–363. https://doi.org/10.1108/JM2-06-2015-0037
12. Zawaideh, F., & Salamah, M. (2019). An efficient weighted trust-based malicious node detection scheme for wireless sensor networks. *International Journal of Communication Systems, 32*(3), e3878. https://doi.org/10.1002/dac.3878