

Semantic Chain-of-Trust: Autonomous Trust Orchestration for Collaborator Selection via Hypergraph-Aided Agentic AI

Botao Zhu, *Member, IEEE*, Xianbin Wang, *Fellow, IEEE*, and Dusit Niyato, *Fellow, IEEE*

Abstract—In collaborative systems, the effective completion of tasks hinges on task-specific trust evaluations of potential devices for distributed collaboration. However, the complexity of tasks, the spatiotemporal dynamism of distributed device resources, and the inevitable assessment overhead dramatically increase the complexity and resource consumption of the trust evaluation process. As a result, ill-timed or overly frequent trust evaluations can reduce utilization rate of constrained resources, negatively affecting collaborative task execution. To address this challenge, this paper proposes an autonomous trust orchestration method based on a new concept of semantic chain-of-trust. Our technique employs agentic AI and hypergraph to establish and maintain trust relationships among devices. By leveraging its strengths in autonomous perception, task decomposition, and semantic reasoning, we propose agentic AI to perceive device states and autonomously perform trust evaluations of collaborators based on historical performance data only during device idle periods, thereby enabling efficient utilization of distributed resources. In addition, agentic AI performs task-specific trust evaluations on collaborator resources by analyzing the alignment between resource capabilities and task requirements. Moreover, by maintaining a trust hypergraph embedded with trust semantics for each device, agentic AI enables hierarchical management of collaborators and identifies collaborators requiring trust evaluation based on trust semantics, thereby achieving a balance between overhead and trust accuracy. Furthermore, local trust hypergraphs from multiple devices can be chained together to support multi-hop collaboration, enabling efficient coordination in large-scale systems. Experimental results demonstrate that the proposed method achieves resource-efficient trust evaluation.

I. INTRODUCTION

WITH the escalating complexity of both applications and the proliferation of interconnected systems, it has become increasingly infeasible for individual resource constrained devices to independently execute computing tasks due to their limited computational power and energy resources [1]. To overcome such limitations, recent research has focused on a new collaborative paradigm that leverages distributed peer resources to enable collaborative task execution [2]. This paradigm emphasizes coordination among devices through resource sharing to enhance the overall system’s task-processing capability and efficiency. Distributed collaborative computing has seen broad adoption across industrial sectors such as smart

manufacturing, smart cities, and e-health, offering substantial benefits including reduced latency, improved resource efficiency, and enhanced service quality [3]. These advantages underscore its potential as a foundational enabler for next-generation collaborative systems.

In collaborative systems, selecting reliable collaborators is a critical prerequisite for ensuring the efficient and accurate execution of computing tasks. Existing studies have explored various strategies for assessing the reliability of potential collaborators. Some approaches rely on social attributes between devices—such as mutual friends, shared interests, group affiliations, and interaction frequency—to infer the reliability of collaborators [4]. Other studies focus on analyzing historical behavioural data, including task completion rates, response latency, and feedback ratings, to evaluate the stability and reliability of collaborators in past task execution [5]. Although these studies can assess the reliability of collaborators to a certain extent, they are often limited in comprehensively and accurately reflecting the true reliability of collaborators in complex and dynamic environments and task-specific considerations. To address this limitation [6], trust has been proposed as an effective means for collaborator evaluation. In this context, trust is defined as the expectation of a resource-constrained task owner that a collaborator will utilize its capabilities and resources to successfully complete a specific task assigned by the task owner [7]. However, trust evaluation in distributed collaborative systems can be much more complex and resource-consuming. With the involvement of multiple collaborators, its complexity arises from comprising a series of task-specific operations, including the collection of trust factor data for all collaborators, situation-related trust inference, task requirement analysis, and task-resource matching. All these operations require significant resource contributions from both the evaluators and the evaluated parties to ensure accurate and reliable assessment. Consequently, to achieve resource-efficient trust evaluation, there are several challenges that need to be solved.

First, it is critical to ensure trust evaluation does not impede collaborative task execution. As trust evaluation involves resource consumption, ill-timed initiation can readily cause collaborative task delays or interruptions. Therefore, precisely perceiving device real-time states and intelligently identifying appropriate temporal windows to initiate trust evaluations is essential. Leveraging the powerful knowledge comprehension and context modeling capabilities of large AI models (LAMs),

B. Zhu and X. Wang are with the Department of Electrical and Computer Engineering, Western University, London, Canada N6A 5B9 (Emails: {bzhu88, xianbin.wang}@uwo.ca)

D. Niyato is with the College of Computing and Data Science, Nanyang Technological University, Singapore (Email: dniyato@ntu.edu.sg).

agentic AI exhibits autonomous awareness, enabling it to independently perceive state changes, perform inference, and schedule tasks without external intervention [8]. Based on this, agentic AI offers a promising technical pathway for realizing state-aware trust evaluation.

In addition, realizing differentiated trust evaluation for collaborators is also an important issue that demands immediate attention. Given collaborators' dynamic nature across spatiotemporal dimensions, task owners must continually collect their data for trust assessment [5]. However, frequent and indiscriminate evaluation operations readily lead to resource waste, thereby undermining overall system efficiency. Consequently, adopting a differentiated update mechanism based on collaborators' trust status becomes essential. For instance, for long-term stable and trustworthy collaborators, historical evaluation results can be judiciously reused to mitigate redundant overhead. To this end, there is an urgent need to construct a connection mechanism between devices and collaborators embedded with trust semantics. This mechanism would enable devices to hierarchically manage evaluation frequency for different collaborators and intelligently schedule the reuse of historical results. Hypergraphs, with their ability to represent complex multi-dimensional relationships among multiple entities, offer strong support for achieving this objective.

Furthermore, due to the dynamic nature of task requirements and device resources, conducting task-specific evaluation of collaborator resources is a critical challenge, yet an indispensable component of trust evaluation. Task owners need to quickly identify the multidimensional requirements of tasks, such as computing and communication, and select the most suitable collaborators from a large pool of available devices. Traditional rule-based matching methods often struggle to cope with scenarios where task semantics are complex and dynamic, and resource combinations are highly heterogeneous [9]. Therefore, it is crucial to adopt intelligent approaches that leverage advanced technologies such as LAMs to rapidly analyze task demands and resources, gain a deep understanding of task semantics and resource characteristics.

To address the aforementioned challenges, this paper proposes an autonomous trust orchestration method: semantic chain-of-trust. The main contributions are summarized as follows.

- Leveraging agentic AI, each device can autonomously perceive its own state and initiate a series of trust evaluation operations during idle periods. This effectively reduces interference with collaborative tasks and enhances the utilization efficiency of distributed resources.
- With the powerful reasoning and learning capabilities of LAMs, the proposed method flexibly adapts to dynamic changes in tasks and resources, precisely performing task-specific trust evaluations of collaborator resources.
- Each device constructs hierarchical collaborator management by creating a trust hypergraph. This hypergraph establishes associations between each device and its collaborators, enabling the regulation of collaborator evaluation frequency and the reuse of historical assessment results

based on trust semantics. Trust hypergraphs from different devices can be dynamically merged, ultimately forming a system-level trust hypergraph that enables scalable and cross-device collaboration.

II. BENEFITS OF AGENTIC AI AND HYPERGRAPH FOR TRUST EVALUATION AND MANAGEMENT

A. Agentic AI for Autonomous Trust Evaluation

Agentic AI systems represent an advanced paradigm in which multiple specialized agents collaborate to achieve complex goals through autonomous perception, reasoning, and decision-making [10]. These systems comprise LAM-powered agents that facilitate goal-oriented task execution by simulating human-like reasoning and decision-making processes [11]. Given their strong capabilities in autonomy, adaptability, and contextual understanding, agentic AI systems are particularly well-suited for enabling intelligent trust evaluation in dynamic systems. Their key characteristics and roles in trust evaluation are summarized as follows.

- **Goal-Oriented Perception for Resource-Efficient Trust Evaluation.** Agentic AI exhibits the ability to autonomously perceive environmental conditions and comprehend contextual information, enabling it to identify task goals, decompose complex tasks into smaller subtasks, and automatically generate ordered execution plans for these subtasks. In trust evaluation scenarios, agentic AI can be used to monitor the operational status of its host device and utilize idle cycles to initiate trust evaluation of collaborators, thereby improving the efficiency of distributed resource utilization.

- **Context-Aware Autonomous Trust Evaluation.** By leveraging advanced semantic understanding and reasoning capabilities of LAMs, agentic AI can autonomously make task-specific decisions based on gathered contextual information. Agentic AI can rapidly and flexibly adapt its decision-making processes to evolving system conditions. In trust evaluation, this capability allows agents to interpret collected trust factors alongside task requirements, enabling autonomous, task-specific trust assessments and improving the precision and timeliness of trust decisions.

- **Continuous Interaction and Learning for Progressive Trust Optimization.** Agentic AI supports long-term, multi-round interactions, continuously acquiring feedback during collaboration and iteratively optimizing the agents' strategies. In trust evaluation, this capability enables dynamic adjustment and iterative refinement of evaluation strategies, thereby improving the accuracy of trust.

B. Hypergraph for Trust Management

Hypergraphs are a generalization of traditional graphs, consisting of an arbitrary number of nodes and hyperedges. Each hyperedge can simultaneously connect any number of nodes, representing relationships among them, which makes hypergraphs especially suitable for modeling complex one-to-many or many-to-many relationships [9]. Leveraging their advantages, hypergraphs can be employed to construct a

distributed, hierarchical, and dynamically evolving trust management framework. Their key characteristics and benefits to trust management are summarized as follows.

- **Complex Relationship Modeling for Multi-Collaborator Trust Management.** Graphs can only describe point-to-point relationships between two entities, while hypergraphs utilize hyperedges to connect multiple entities simultaneously, enabling the modeling of complex multi-entity relationships. In trust management, each device can employ a hyperedge to explicitly link all trusted collaborators, thereby capturing one-to-many trust relationships. Thus, hypergraphs are well-suited for modeling trust relationships among multiple collaborators.

- **Rich Semantic Representation for Hierarchical Trust Management.** Both nodes and hyperedges in a hypergraph can carry rich semantic information, such as node attributes and contextual features, enabling fine-grained and semantically expressive modeling of entities and their relationships in complex systems. In trust management, by assigning semantic labels such as trustworthy and untrustworthy to a hypergraph's hyperedges, a semantic and hierarchical trust management model can be intuitively and efficiently constructed.

- **Distributed Modeling and Temporal Evolution for Dynamic Trust Management.** The hypergraph structure naturally aligns with the characteristics of distributed systems. Each node only needs to maintain information about its neighbouring nodes and associated hyperedges, without requiring knowledge of the global information. In addition, the associations between nodes and hyperedges can dynamically evolve over time. In trust management, a device can use minimal storage resources to maintain a local hypergraph for managing its collaborators. As collaborators' trust values evolve, a device can dynamically reassign them to different semantically labelled hyperedges, enabling flexible and adaptive trust management.

III. SEMANTIC CHAIN-OF-TRUST

To enable resource-efficient trust evaluation in collaborative systems, this paper proposes the semantic chain-of-trust—an autonomous trust orchestration method that integrates agentic AI with hypergraph. This method enables devices to establish and maintain chained trust relationships with one another, offering the following key benefits:

- 1) *Efficient utilization of distributed computing and communication resources.* It allows each device to decompose complex trust evaluation tasks into smaller subtasks and autonomously collect relevant trust factors, such as historical behaviours, task completion quality, and available resources, from others during idle periods, enhancing the efficient utilization of distributed computing and communication resources.

- 2) *Autonomous trust evaluation and continuous optimization.* It enables each device to autonomously analyze and interpret task requirements and trust factors, and to perform task-specific trust evaluations of collaborators. Through ongoing interactions, each device continuously learns and refines its trust evaluation strategies.

- 3) *Hierarchical management of collaborators based on trust semantics.* It enables each device to dynamically classify collaborators into distinct trust-semantic groups, where each group is subject to a tailored evaluation frequency to balance trust accuracy and evaluation overhead.

- 4) *Dynamic construction of cross-device cooperation path.* It enables devices to flexibly construct multi-hop trusted collaboration paths based on task requirements, enhancing system-wide cooperation and ensuring reliable task completion.

In this section, we first present the trust model. Then, the agents involved in the semantic chain-of-trust are introduced. Finally, we describe how these agents collaborate to perform trust evaluation and management.

A. Trust Model

In a collaborative system with $B = \{b_1, \dots, b_N\}$ devices, each device b_i can act as a task owner by initiating a face recognition task c . Task c is composed of a set of photos, characterized as $\{\text{"size"} : \text{"100 MB"}, \text{"processing density"} : \text{"2,339 cycles/bit"}, \text{"maximum task completion tolerance time"} : \text{"60 seconds"}\}$. The task owner evaluates the trust of potential collaborators and offloads task c to a trusted device, which is then responsible for counting the total number of people in the photos. Hence, we define the trust of task owner b_i in collaborator b_j as the likelihood that b_j can successfully complete task c . This likelihood is inferred from b_j 's historical performance and available resources. It can be seen that trust evaluation is essentially a complex task, involving the collection of diverse trust factors, task analysis, evaluation execution, etc. If collaborator b_j is chosen to execute task c , the task owner b_i records b_j 's performance locally upon completion. Each record is formatted as $d_{b_i \rightarrow b_j}^{t_{\text{per}}} = \{\text{"device"} : \text{"}b_j\text{"}, \text{"time (}t_{\text{per}}\text{)"} : \text{"2025-07-06 15:36:44"}, \text{"response time"} : \text{"0.6 second"}, \text{"execution speed"} : \text{"2 MB/second"}, \text{"accuracy"} : \text{"98\%"}, \text{"feedback"} : \text{"satisfied"}\}$.

B. Specialized Agents

Each device b_i is equipped with an agentic AI implemented using MetaGPT [12], a general-purpose agent framework that supports multi-role, multi-task collaboration. The agentic AI breaks down the complex trust evaluation into multiple smaller subtasks, each handled by an LAM-enabled specialized agent. Following the trust evaluation workflow, we create six agents with distinct roles, and initialize each agent with specific knowledge and skills tailored to its responsibilities. They collaborate with one another to complete the trust evaluation. A detailed description of these agents is provided below.

State perceiver A_{sp} : It identifies the device's idle state through continuous monitoring of CPU activity. Upon detecting idleness, it triggers the subsequent trust evaluation process.

Trust manager A_{tm} : Based on trust semantics, it manages the collaborators of device b_i hierarchically and autonomously determines which collaborators require evaluation during each assessment cycle.

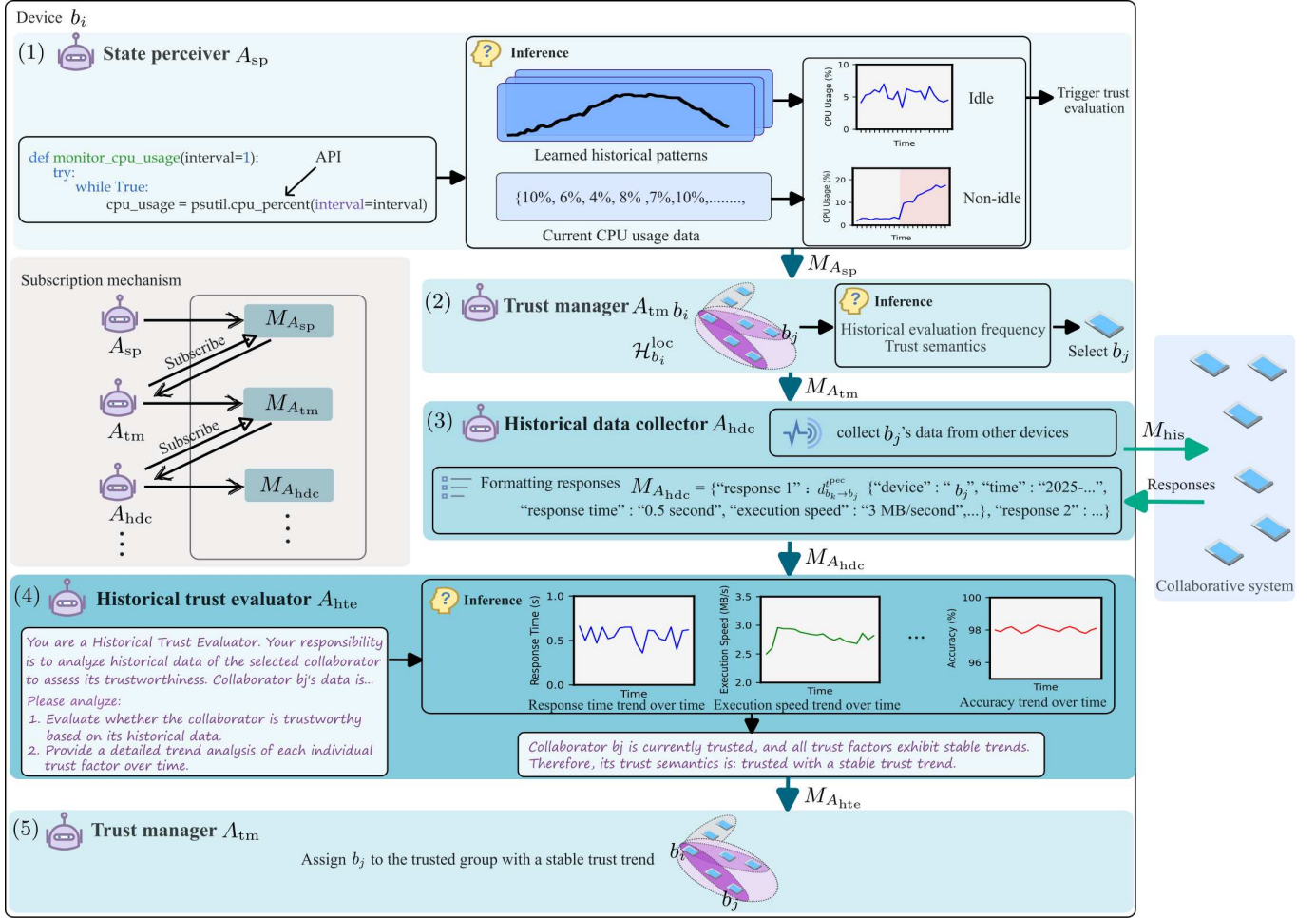


Fig. 1. Workflow of agents on device b_i for trust evaluation based on historical performance data. (1) Agent A_{sp} detects the CPU idle state. (2) Agent A_{tm} decides which devices require trust evaluation. (3) Agent A_{hdc} collects historical performance data of the selected device. (4) Agent A_{hte} performs trust evaluation of the selected device using historical performance data. (5) Agent A_{tm} reassigns the evaluated device to a different group.

Historical data collector A_{hdc} : It invokes external modules to request historical performance data of collaborators to be evaluated from other devices, and receives their responses.

Historical trust evaluator A_{hte} : Based on the collected historical performance data, it infers the trust semantics of collaborators to be evaluated, including their current trust values and the trends of trust evolution over time.

Resource data collector A_{rde} : When device b_i generates a task c , A_{rde} invokes external modules to request the current available resource data from all collaborators within the trusted group and receives their responses accordingly.

Resource trust evaluator A_{rte} : Based on the received available resource data of collaborators and the requirements of task c , it performs a task-specific trust evaluation for each collaborator.

C. Implementation of Semantic Chain-of-Trust via a Streamlined Cross-Agent Workflow

Trust evaluation consists of two components: assessing the historical performance of collaborators and evaluating their current resource availability upon the generation of task c .

The task owner combines the results of these two evaluations to select a trusted collaborator for task execution. Within each component, specialized agents execute trust evaluation subtasks following a streamlined workflow. Agents interact through a subscription-based communication mechanism, where each downstream agent subscribes to the outputs of the upstream agent. Following the model context protocol (MCP), agents exchange messages in a structured format. Additionally, some agents interact with external modules via application programming interfaces (APIs). The workflow of agents for historical data-based trust evaluation is detailed in Fig. 1 and elaborated below.

1) Historical Data-Based Trust Evaluation Workflow

Step 1: Agent A_{sp} detects the CPU idle state. To optimize the utilization of distributed resources, each device b_i conducts historical data-based trust evaluation for collaborators only during idle periods. To this end, agent A_{sp} operates in an “observe–infer–act” cycle. It continuously monitors device b_i 's CPU activity via API calls. However, relying on a single instance of low CPU utilization to determine idleness may yield inaccurate results. Instead, agent A_{sp} infers the state of device b_i by combining recent CPU utilization data with

learned historical CPU activity patterns. Once device b_i is confirmed idle, agent A_{sp} immediately outputs a message $M_{A_{sp}}$ to trigger the trust evaluation process.

Step 2: Agent A_{tm} decides which devices require trust evaluation. Since agent A_{tm} subscribes to messages from agent A_{sp} , upon receiving the message $M_{A_{sp}}$, it autonomously determines which collaborators' trust should be evaluated. Agent A_{tm} manages all collaborators of device b_i by maintaining a local trust hypergraph $\mathcal{H}_{b_i}^{loc}$, which establishes a hierarchical structure based on trust semantics, as shown in Fig. 1 and Fig. 3 (a). These collaborators are categorized into trusted and untrusted groups. It is worth noting that the groups can be dynamically extended, such as trusted, low-trust, and medium-trust categories. The trusted group is encapsulated by hyperedge $e_{b_i}^{tr}$, with its edge attribute assigned the semantic label "trusted". Similarly, the untrusted group is encapsulated by hyperedge $e_{b_i}^{utr}$, and its edge attribute is assigned the semantic label "untrusted". The trusted group is further divided into two subgroups: trusted with a stable trust trend and trusted with a declining trust trend. These two subgroups are also represented by separate hyperedges, each assigned a corresponding semantic label. Therefore, these four hyperedges together form a hypergraph $\mathcal{H}_{b_i}^{loc}$. Each collaborator b_j in $\mathcal{H}_{b_i}^{loc}$ is associated with a set of attribute information, including its trust status, evaluation timestamp, and trust trend. This is represented in the form {"device": " b_j ", "time (t^{tru})": "2025-07-5 10:00:00", "status": "trusted", "trend": "declining"}.

Agent A_{tm} determines which collaborators need to be evaluated by analyzing their historical evaluation frequency along with current trust semantics. A collaborator's evaluation priority decreases when its trust status is stable and it has been frequently evaluated. Conversely, its evaluation priority increases if its trust trend is declining or it has received infrequent evaluation. We assume that collaborator b_j is chosen for trust evaluation due to its limited evaluation frequency and current status as "trusted with a declining trust trend". Agent A_{tm} subsequently outputs a message $M_{A_{tm}}$ = "The collaborator selected for trust evaluation is {"device": " b_j ", "time (t^{tru})": "2025-07-5 10:00:00"}".

Step 3: Agent A_{hdc} collects historical performance data of the selected device. Agent A_{hdc} is a subscriber of the messages of agent A_{tm} . Upon receiving the message $M_{A_{tm}}$, agent A_{hdc} formulates a new message M_{his} = "I would like to know whether you have historical performance data for device b_i after time t^{tru} : 2025-07-5 10:00:00." This message is then broadcast to other devices in the system via the communication module. Upon receiving the broadcast, devices in a busy state do not respond. Devices in an idle state search their locally stored records based on the specified device and time. If relevant records are found, the devices promptly respond with the data; otherwise, they withhold any reply. For example, device b_m retrieves a record $d_{b_m \rightarrow b_j}^{t^{per}}$ related to device b_j and sends it to device b_i . After receiving responses, agent A_{hdc} generates a message $M_{A_{hdc}}$ by organizing them into a structured format.

Step 4: Agent A_{hte} performs trust evaluation of the selected device using historical performance data. Agent A_{hte} is a subscriber to the messages sent by agent A_{hdc} . Upon receiving the message $M_{A_{hdc}}$, A_{hte} first queries device b_i local database to check whether it has historical performance records of device b_j . If such records exist, A_{hte} combines the local historical data with the received message to infer the trust semantics of device b_j . The inference process involves not only determining whether device b_j is currently trustworthy, but also analyzing the temporal trends of individual trust factors. By doing so, A_{hte} can perform a more comprehensive and fine-grained trust evaluation, enhancing the understanding of device behavior and improving the accuracy of trust evaluation. As illustrated in Fig. 1, A_{hte} analyzes the trust trends of device b_j in terms of accuracy, execution speed, and response time. Based on the inference result, agent A_{hte} generates a new message $M_{A_{hte}}$ that contains the trust semantics of device b_j and the evaluation time, formatted as "The updated trust of device b_j is {"device": " b_j ", "time (t^{tru})": "2025-07-10 10:56:22", "status": "trusted", "trend": "stable"}".

Step 5: Agent A_{tm} reassigns the evaluated device to a different group. Agent A_{tm} subscribes to messages published by agent A_{hte} . Upon receiving the message $M_{A_{hte}}$, agent A_{tm} analyzes the trust semantics contained in the message and reassigns the evaluated device to the appropriate trust group accordingly. For example, device b_j is determined to be trusted with a stable trust trend, hence it is moved from the "trusted with a declining trust trend" group to the "trusted with a stable trust trend" group, thereby enabling dynamic trust management.

The five steps in this component are executed cyclically during the idle states of devices in the system, gradually establishing connections between devices based on trust semantics.

2) Resource Data-Based Trust Evaluation Workflow

When device b_i initiates a task c , it needs to assess the resource trust of collaborators within the trusted group to ensure they possess reliable capabilities to execute task c . Note that this component reuses evaluation results derived from collaborators' historical performance data and therefore focuses solely on assessing their current resources. The agent workflow for this component is illustrated in Fig. 2.

Step 1: Agent A_{tm} selects collaborators that need resource evaluation. Upon receiving a task generation notification, A_{tm} extracts all collaborators from the trusted group $e_{b_i}^{tr}$ in hypergraph $\mathcal{H}_{b_i}^{loc}$. As shown in Fig. 2 and Fig. 3 (a), devices b_u , b_j , b_w , and b_m are selected. These trusted collaborators are then packaged into a structured message $M'_{A_{tm}}$.

Step 2: Agent A_{rde} collect resource data of collaborators. Upon receiving the message $M'_{A_{tm}}$, agent A_{rde} , as a subscriber to messages from agent A_{tm} , invokes the communication module to send a resource inquiry message M_{res} to collaborators in the trusted group of device b_i . M_{res} comprises resource-related details required for communication and computing. It is denoted as "Please provide your current resource status

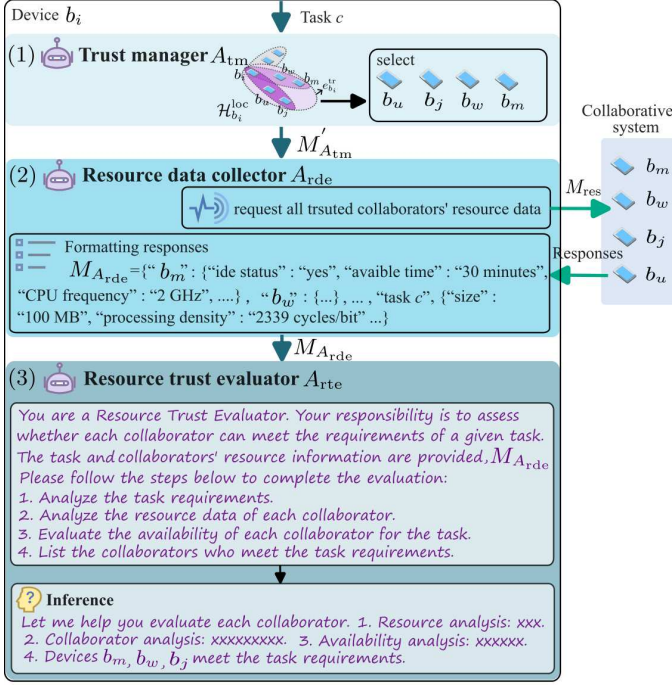


Fig. 2. Workflow of agents on device b_i for resource trust evaluation. (1) Agent A_{tm} selects collaborators that need resource evaluation. (2) Agent A_{rde} collect resource data of collaborators. (3) Agent A_{rte} evaluates the resource trust of collaborators.

including: idle status, available time, CPU frequency, available CPU capacity, storage space, network bandwidth, connection stability, ...". Each trusted collaborator responds to the request message M_{res} by sending its resource information to device b_i . Then, agent A_{rde} organizes the received responses into a unified format, and combines them with task c to generate a new message, $M_{A_{rde}}$.

Step 3: Agent A_{rte} evaluates the resource trust of collaborators. Agent A_{rte} subscribes to messages published by agent A_{rde} . Upon receiving the message $M_{A_{rde}}$, A_{rte} initiates the resource trust inference process. Considering the complexity of this procedure, the prompt is designed with a stepwise guidance strategy to ensure the accuracy of the inference. First, agent A_{rte} is guided to analyze the task requirements. Next, it is instructed to examine the resource information of collaborators. Finally, it compares the results of the two preceding analyses. Collaborators whose resources satisfy the task requirements are identified as task-specific trusted collaborators. Because agent A_{rte} is pre-trained on a large volume of technical documentation, it possesses sufficient knowledge of communication and computing to generate accurate results. As shown in Fig. 3 (b), devices b_w, b_m , and b_j are identified as task-specific trusted collaborators, and they form a task-specific trust hypergraph $\mathcal{H}_{b_i}^{task}$. Note that this hypergraph contains only a single hyperedge. Device b_i can select any collaborator in this hypergraph to execute task c .

To forward a task to a distant collaborator, a device can incrementally integrate its own task-specific trust hypergraph with those of intermediate collaborators, forming a chained

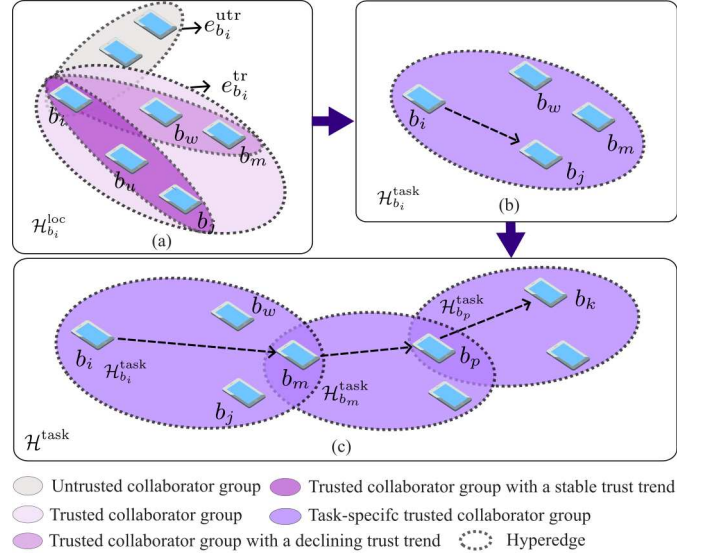


Fig. 3. Hypergraph-assisted hierarchical management of collaborators and task-specific trusted collaborator selection. (a) Device b_i 's local trust hypergraph $\mathcal{H}_{b_i}^{loc}$ hierarchically organizes collaborators based on trust semantics. (b) Device b_i 's task-specific trust hypergraph $\mathcal{H}_{b_i}^{task}$ enables one-hop collaborator selection. (c) A composite task-specific trust hypergraph formed by multiple devices enables multi-hop collaborator selection.

hypergraph structure. This structure facilitates the stepwise establishment of a trust path toward the target collaborator, thereby enabling connection and task delivery across multiple trusted collaborators. For instance, in Fig. 3 (c), device b_i intends to forward task c to device b_k . Due to the absence of a direct trust link between them, device b_i connects its task-specific trust hypergraph $\mathcal{H}_{b_i}^{task}$ to that of its trusted collaborator, device b_m . Subsequently, the task-specific trust hypergraph $\mathcal{H}_{b_p}^{task}$ of device b_p , a trusted collaborator of device b_m , is also incorporated. Through this step-by-step integration, a composite task-specific hypergraph \mathcal{H}^{task} is constructed, supporting multi-hop cooperation and enabling a trustworthy task transmission path from device b_i to device b_k .

IV. EXPERIMENTAL ANALYSIS

We validate the proposed semantic chain-of-trust in a collaborative system comprising a group of DELL 5280 computers and Google Pixel 8 smartphones. All devices are interconnected via Wi-Fi and equipped with face recognition software. The detailed task parameters are described in Section III-A. An idle timeslot is defined as 30 seconds. By adjusting the number of idle timeslots within one hour, the number of trust evaluations accurately triggered during these slots is measured. As shown in Fig. 4, the proposed method achieves nearly 100% utilization of idle timeslots, significantly outperforming the statistical-based model [13].

Fig. 5 (a) compares the average number of trust evaluations based on historical data. This is computed as the total count of historical data-based trust assessments performed within the system divided by the total number of devices. It can be observed that the proposed semantic chain-of-trust significantly reduces the number of trust evaluations compared to

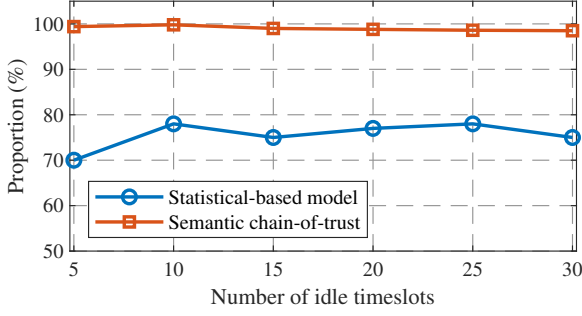


Fig. 4. Comparison of the proportion of trust evaluation operations performed in idle timeslots.

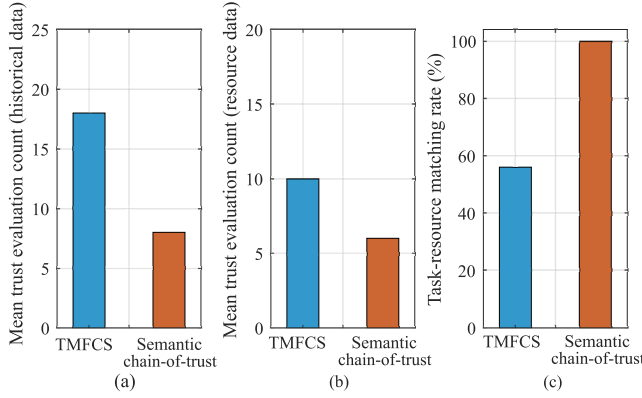


Fig. 5. Performance comparison between semantic chain-of-trust and TMFCS. (a) Comparison of the average number of trust evaluations based on historical data. (b) Comparison of the average number of collaborators requiring resource evaluation. (c) Comparison of task-resource matching rate.

the trust model with fitness-based clustering scheme (TMFCS) [14]. This improvement stems from the introduction of trust semantics, which enables hierarchical management and selective evaluation of collaborators, effectively avoiding unnecessary trust assessments and reducing resource consumption. Fig. 5 (b) presents a comparison of the average number of collaborators requiring resource evaluation per task by the task owner. The results clearly indicate that, compared to TMFCS, the proposed method reduces the number of collaborators requiring evaluation, thanks to its more granular collaborator management approach. Fig. 5 (c) presents a comparison of task-resource matching rate. The proposed method achieves a 100% matching rate, significantly outperforming the comparison algorithm, which reaches only 56%. This improvement is attributed to the capabilities of LAMs, including self-learning, semantic understanding, and reasoning, which collectively enable more accurate and intelligent task-resource alignment.

V. CONCLUSION

To achieve resource-efficient trust evaluation and enhance the overall performance of collaborative systems, this paper

proposes a semantic chain-of-trust. This mechanism leverages the strengths of agentic AI and hypergraph modeling to enable devices to autonomously establish and maintain trust relationships. By utilizing the powerful perception and reasoning capabilities of agentic AI, the semantic chain-of-trust can detect device idle states and perform trust data collection, trust inference, task understanding, and task-resource matching inference during these idle periods, thereby realizing an autonomous and resource-efficient trust evaluation process. Meanwhile, the hypergraph embedded with trust semantics enables hierarchical management of collaborators and accurately identifies those requiring evaluation, thereby effectively reducing redundant trust assessments. Experimental results demonstrate that the proposed method can fully utilize device idle time and significantly reduce the number of trust evaluations, thereby improving the system's resource efficiency.

REFERENCES

- [1] H. Tran-Dang, S. Bhardwaj, T. Rahim, A. Musaddiq, and D.-S. Kim, "Reinforcement learning based resource management for fog computing environment: Literature review, challenges, and open issues," *J. Commun. Netw.*, vol. 24, no. 1, pp. 83–98, Feb. 2022.
- [2] M. Tang, L. Gao, and J. Huang, "Communication, computation, and caching resource sharing for the Internet of Things," *IEEE Commun. Mag.*, vol. 58, no. 4, pp. 75–80, Apr. 2020.
- [3] S. Zhang, N. Yi, and Y. Ma, "A survey of computation offloading with task types," *IEEE Trans. Intell. Transp. Syst.*, vol. 25, no. 8, pp. 8313–8333, Aug. 2024.
- [4] A. Souri, Y. Zhao, M. Gao, A. Mohammadian, J. Shen, and E. Al-Masri, "A trust-aware and authentication-based collaborative method for resource management of cloud-edge computing in social Internet of Things," *IEEE Trans. Comput. Social Syst.*, vol. 11, no. 4, pp. 4899–4908, Aug. 2024.
- [5] M. Song *et al.*, "Trustworthy intelligent networks for low-altitude economy," *IEEE Commun. Mag.*, vol. 63, no. 7, pp. 72–79, Jul. 2025.
- [6] J. Wang, Z. Yan, H. Wang, T. Li, and W. Pedrycz, "A survey on trust models in heterogeneous networks," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 4, pp. 2127–2162, Fourthquarter 2022.
- [7] B. Zhu, X. Wang, L. Zhang, and X. S. Shen, "Chain-of-trust: A progressive trust evaluation framework enabled by Generative AI," *IEEE Netw.*, Jun. 2025, Early Access, doi: 10.1109/MNET.2025.3582407.
- [8] S. Hosseini and H. Seilani, "The role of agentic AI in shaping a smart future: A systematic review," *Array*, vol. 26, p. 100399, Jul. 2025.
- [9] B. Zhu and X. Wang, "Networked physical computing: A new paradigm for effective task completion via hypergraph aided trusted task-resource matching," *IEEE Trans. Netw. Sci. Eng.*, Jul. 2025, Early Access, doi: 10.1109/TNSE.2025.3592859.
- [10] F. Jiang, Y. Peng, L. Dong, K. Wang, K. Yang, C. Pan, and X. You, "Large AI model-based semantic communications," *IEEE Wireless Commun.*, vol. 31, no. 3, pp. 68–75, Jun. 2024.
- [11] F. Jiang, Y. Peng, L. Dong, K. Wang, K. Yang, C. Pan, D. Niyato, and O. A. Dobre, "Large language model enhanced multi-agent systems for 6G communications," *IEEE Wireless Commun.*, vol. 31, no. 6, pp. 48–55, Dec. 2024.
- [12] S. Hong *et al.*, "MetaGPT: Meta programming for a multi-agent collaborative framework," in *Proc. Int. Conf. Learn. Represent.*, 2024, pp. 1–29.
- [13] Q. Diao and J. Song, "Prediction of CPU idle-busy activity pattern," in *Proc. IEEE Int. Symp. High Perform. Comput. Archit.*, 2008, pp. 27–36.
- [14] J. Gao, C. Cheong, M. Zhang, Y. Cao, T. Peng, and S. Pervez, "A trust model with fitness-based clustering scheme in FANETs," in *Proc. IEEE Int. Conf. Trust, Secur. Priv. Comput. Commun.*, 2024, pp. 978–985.