IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 14, 2022, accepted April 7, 2022, date of publication April 22, 2022, date of current version May 5, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3169788

ConTrust: A Novel Context-Dependent Trust Management Model in Social Internet of Things

RABIA LATIF
Artificial Intelligence and Data Analytics Laboratory, College of Computer and Information Sciences (CCIS), Prince Sultan University, Riyadh 11586, Saudi Arabia

e-mail: rlatif@psu.edu.sa

This work was supported by the Artificial Intelligence and Data Analytics Laboratory (AIDA), College of Computer and Information Sciences (CCIS), Prince Sultan University, Riyadh, Saudi Arabia.

ABSTRACT The global population is around 7.4 billion people. This population density requires connectivity to improve the standard of living by transmitting and receiving variety of services. As a result, numerous forms of communication among objects are required for our everyday living demands, independent of their nature. Furthermore, to create a good relationship, every object that is regarded as associate of another object should have distinct criteria such as scalability, interoperability, and trustworthiness. Many security threats, however, have an impact on the social interaction between objects in a social internet of things (SIoT) context, including illegal admittance and suspicious behavior owing to a lack of verification architecture. Others include attempting to provide a proper viewpoint of a malicious object to earn the trust of other objects. As a result, there is a requirement for an acceptable method to check the behavior of objects such as capability, commitment, reliability, and previous job satisfaction before proceeding with any type of job assignment. This will aid in distinguishing between malicious and trustworthy objects by anticipating their upcoming behavior, allowing better judgments regarding service assignment to be made. This study proposes a context-dependent trust management technique (ConTrust) for choosing and allocating jobs in a SIoT environment. The feature-property match approach, as well as the combination of capability, commitment, and satisfaction, were utilized to increase the efficiency of trust assessment and the resolution of context-dependent difficulties. The proposed trust model considers job characteristics, object capabilities and honesty, and the impact of malicious conduct. The experimental results show that the proposed ConTrust model is viable and capable of ensuring the reliability and efficacy of SIoT service sharing between objects as compared to the benchmark models considered in this work.

INDEX TERMS Context based trust management, SIoT, trust management.

I. INTRODUCTION

As information and communication technology has advanced, a wide variety of Social Internet of Things (SIoT)-based applications, such as smart traffic management [1], smart airport [2], and smart home [3], have evolved [4]. In this type of SIoT environment, a user's system application (service requester) can communicate with other service provider systems identified by co-location relations to seek its required job assignment and provision. Service provider systems can, on the other hand, either be honest with high-quality services or dishonest with low-quality services [5]. Malicious attacks, such as bad-mouthing attacks, ballot-stuffing attacks, self-promoting attacks, and on-off attacks, are example of attacks that can be carried out by such malicious service providers. The issue of trust evaluation in SIoT contexts develops and becomes significant to mitigate against such attacks. In a SIoT scenario, a dependable ecosystem must be constructed on an efficient trust management method for identifying trustworthy service providers [5].

Recently, several context-aware trust evaluation methods have been presented [5]–[12] to address issues related to trust management in SIoT. They do not, however, consider social relationships between systems or the characteristics of Internet of Things (IoT) service computing environments. Furthermore, the existing SIoT trust management techniques do not support in-depth social connections between systems, which are critical aspects of SIoT settings [13]–[15].

The associate editor coordinating the review of this manuscript and approving it for publication was Xiaolong Li.

It is crucial to highlight that present methods are primarily concerned with assessing the trustworthiness of social actors by considering their social settings [13]–[16]. In terms of assessing trust, information is typically gathered from two primary sources: direct and indirect experiences. Direct experience is based on prior observations of direct interactions between the service requester and the service provider [6], [7]. Indirect experience, on the other hand, may be divided into two types: familiar object experience and unfamiliar object experience [17].

Social connections between objects are utilized in SIoT to categorize objects into familiar and unfamiliar groupings [13]–[16]. Objects will create five sorts of social connections which are co-work, ownership, social, parental, and co-location relationships [6], [18]. Because the social relationship is a very volatile and dynamic social connection, it is classed as an unfamiliar object relationship. However, the effectiveness of using familiar or unfamiliar objects relationship techniques depends on the effective job assignment scheme used to assign the right job to the right service provider. Service or job assignment in SIoT is categorized into two categories of dependences: Strong Dependency and Weak Dependency [19], [20]. When a service requester lacks the necessary abilities or resources to work on a job, forcing them to assign the job to a reliable service provider, this is termed as strong dependency. In the situation of weak dependency, a service requester has sufficient abilities to fulfil its purpose [13]–[16].

The most trustworthy experience is direct contact in general, but unfamiliar objects have less credibility as far as job assignments are concerned. For trust-related information, the trust model in this study will estimate various levels of confidence from various sources. This study will primarily concentrate on a trust model that will help the service requester to select a better service provider for its job assignment in the context of strong dependency. Thus, the precise influence of economic issues on the trust model and the process of job assignments is outside the scope of this study, but they will be of future interest to us. The following points highlights the main contributions of this paper:

1) A context dependent trust management in Social IoT is presented to compute trust, which leverages the service provider's capability (section IV-A), commitment (section IV-B), and job satisfaction feedback (section IV-C) as parameters for trustworthy assessment, allowing the trust model to be highly versatile to dynamic situations.
2) Trust assessment was designed to be performed utilizing a variety of sources (both familiar and unfamiliar), and cooperative filtering was used to obtain trust input from previous requesters that receive services in the same context (section IV-D).
3) Several experiments were carried out in section-VI to check the security, feasibility, and efficacy of the proposed model, demonstrating that the model can successfully choose qualified and truthful service providers to execute job and prevent malicious behaviors to a significant amount.

The remainder of the paper is structured as follows. Section 2 goes through the related work. Section 3 presents the system model. In Section 4, the proposed context-dependent trust management in Social IoT is presented. Section 5 contains the security analysis. Section 6 discusses performance analysis. Finally, Section 7 brings the paper to a close.

II. LITERATURE REVIEW

Previously, researchers conducted a comprehensive examination of trust management techniques and their associated benefits and drawbacks in many works such as [21]. They aimed to conduct a systematic examination of the most relevant trust management techniques to establish how different systems interact to offer the needed functions without relying on a range of research standards. Nevertheless, the chosen methodologies were investigated without regard for categorization [22], [23].

Since there are numerous trust building models in SIoT, and the reliability and efficiency of each model must be evaluated, evaluation and model idea are inextricably linked [13]–[16]. As a result, the importance of such models in assisting service requests to achieve their SIoT-environment job assignment goals cannot be overstated [4], [6]. To develop a trust building model in SIoT, [1], [2] and [18] presented an evolving trust models that depend on the degree of truthfulness among distinct objects. In [18] model, two ways to trust evaluation were presented: subjective and objective. The subjective method has a relatively slow transient reaction as compared to objective one; moreover, objective analysis as well as trust data storage are conducted in a data hash table structure that is visible to all objects. Using these studies, mistrust objects and network effects can distinguish effectively. Furthermore, trust performance evaluation was carried out amongst collaborating linked objects thereby keeping in mind that any object behaving in an unusual way in the system may be malicious. Although some objects are friendly and engage in their social activities, others are not. The drawbacks of these studies are the lack of utilization of direct observation to analyze trust measures, instead focusing on indirect trust observations [13]–[16].

To address the challenges established in [1], [2] and [18], an SIoT assurance and integrity trust assessment technique using object conduct was presented by [5], [21], [22] to investigate direct and indirect observation approaches. The goal is to offer an appropriate service response, and several useful approaches, such as credibility and trustworthiness scores, were utilized to assess the level of trust among objects. Each object that offers a full job receives a better score than those that didn't participate or didn't provide any acceptable job; ultimately, malicious objects have a lower score. These studies are characterized as a viable technique to determining fraudulent objects, however it does not consider all major

trust factors in big scale systems, such as scalability [8]–[10]. Moreover, three types of social trust elements based on provider contact were described in [8], including scalability, social interaction, relationship, and group of Interest connection. These are predicated on mutual values, as well as the system's resilience towards opportunistic service threats. The drawback of these studies are that they do not necessarily reflect attack strategies [7].

Different attack strategies were considered in [5], [6] to address the challenges in [8]–[10] so that to ensure users reliability, safety, and data protection during interaction. They used diverse conceptual analyses and digital experiments in the deployment of their proposed model, and they also contributed to testing the proposed approach's efficiency using real data. Besides, an adaptive trust management model was presented in [8], [10], [11] to evaluate trust responses based on the major trust management aspects, which include: 1. Honesty, which is based on direct or indirect information or if the object is trustworthy. 2. Cooperation, which is related to the level of social engagement among friends in a society, such as social interaction. 3. Group of Interest, which is based on mutual values and wants or some analogous capacities shared by objects put in a similar social system, such as co-location or co-work [16]. This study, however, has a flaw in that it does not account for dynamic environmental concerns. According to trust information, [23] defined a generic definition for trust in all SIoT components. They created a platform to evaluate trust services that consists of three major components: (1) credibility, which is based on user opinion, (2) recommendation, which is based on user recommendations to accept or reject an object, and (3) knowledge, which is predicated on each object's basic awareness [16].

In [27], a trust management solution for IoT was presented that can determine a node's trust level based on its previous conduct in separate cooperative services. The primary objective of this solution is to manage collaboration in a heterogeneous IoT architecture while taking into consideration the capabilities of the various nodes via the use of a decentralized method. To update trust levels, this model considers both first-hand information such as direct observations and personal experiences and second-hand information such as indirect observations and observations provided by nearby nodes. This approach involves several phases, including the following: collects information about the truthfulness of participating nodes; establishes a cooperative service with requesting nodes; learns from its past operations by performing self-updates aimed at improving future operations; and allocates a quality feedback score to each node following each contact during the process of learning.

In [28], researchers created CATrust, a context-aware trust management approach for service-oriented ad hoc networks, peer-to-peer networks, and the Internet of Things. Rather than determining sincerity based on satisfactory/unsatisfactory past in networks, this approach used logistic regression to forecast service provider behavior patterns in a new situation. CATrust achieved accuracy against colluding assaults, as well as confirmed convergence and robustness, by including a suggestion filtering system and isolating dishonest nodes. In terms of False negative and False positive probability, the suggested model outperforms Beta reputation scheme with belief discounting and adaptive trust management with collaborative filtering. To determine CATrust's applicability, the researchers in [29] recommend that the model be tested first using actual geo-distributed data acquired by PlaneLab. Second, the value of the system should be proved by integrating it with social P2P/IoT systems that are defined by QoS and social characteristics. Finally, its resistance to complex noisy settings, specific mobility applications, and hostile behaviors such as opportunistic and collision assaults should be evaluated.

Furthermore, additional difficulties of trust plague different types of service provisioning systems, such as fog computing and wireless sensor nodes (SNs). Offloading data to a rogue fog node might result in the gathering or modification of users' sensitive information without their knowledge. Authors in [24] used a trust architecture to detect and isolate rogue fog computing nodes, therefore mitigating security threats. Similarly, SNs, like any other piece of hardware or software, may be attacked. Technique [25] offers an energy-efficient, network-based mobile code-driven trust mechanism that utilizes mobile code to visit SNs according to predetermined routes. However, these approaches ([24], [25]) suffer from several drawbacks, including bottleneck problems caused by a single point of failure [26]. Table 1 provides the summary of the most current and related works.

TABLE 1. Summary of the related works.

Reference	Objectives	Achievements	Limitations
[1], [2], [18]	Trust building in SIoT	High reliability and efficiency	Direct observations not considered
[5], [24], [25]	Direct and indirect observation approaches	High performance and reliability	Scalability issues
[8]–[10]	Scalability, social interaction, relationship, and group of Interest connection	High performance and scalability	Limited to few attack strategies protection
[5], [6], [27]	reliability, safety, and data protection	High performance, reliability, scalability, and security	Dynamic environment problems were not considered

III. SYSTEM MODEL

The model is made up of a group of service requesters ($\mathfrak{R}$s) and a set of service providers ($\mathfrak{f}$s) in a generic trust situation in SIoT. The $\mathfrak{R}$ serves as the trustor in the trust relationship by requesting services and delegating jobs. $\Omega_i = \{r_1, r_2, \ldots, r_n\}$ denotes the set of $\mathfrak{R}$s. Furthermore, the $\mathfrak{f}$ is the trustee in the trust relationship because it provides services or performs jobs for the $\mathfrak{R}$. $\mathcal{P}_j = \{p_1, p_2, \ldots, p_m\}$ defines the set of $\mathfrak{f}$s.

The features of $\mathfrak{f}_{p_j}$ is given as the set $\mathrm{F}_{p_j} = \left\{\mathfrak{f}^1_{p_j}, \mathfrak{f}^2_{p_j}, \mathfrak{f}^3_{p_j} \ldots\right\}$. The $\mathfrak{f}$'s trustworthy assessment and job assignment will be evaluated based on these features assessment.

The trust model relationship in this study is context dependent since the outcome of job assignment varies depending on the environment. As a result, context C comprises the job type as well as the precise environment in which the service will be offered.

The precise jobs that the delegated $\mathfrak{f}$ should do are included in Job $\mathfrak{j}$, which was requested by the $\mathfrak{R}$. Aside from the broad description, Job $\mathfrak{j}_x$ will include tangible qualities or precise demands that are required for job execution to succeed and accomplish the $\mathfrak{R}$ goal. $\mathcal{P}_{\mathfrak{j}_x} = \left\{\mathscr{p}^1_{\mathfrak{j}_1}, \mathscr{p}^2_{\mathfrak{j}_2}, \mathscr{p}^3_{\mathfrak{j}_3}, \ldots\right\}$ C denotes the set of properties of the Job $\mathfrak{j}$ that occur in a specific context C. The $\mathfrak{R}$ goals can be described as a set of goals $\mathfrak{G}_{\mathfrak{r}} = \left\{g_{r_1}(\mathfrak{j}_1), g_{r_2}(\mathfrak{j}_2), \ldots, g_{r_n}(\mathfrak{j}_z)\right\}$, where $g_{r_i}\left(\mathfrak{j}_x\right) \in \mathfrak{G}_{\mathfrak{r}}$ represents the $\mathfrak{R}_{r_i}$'s goal for requesting a Job $\mathfrak{j}_x$. If the job is successfully completed by the delegated $\mathfrak{f}$, the job result $R_{\mathfrak{j}_x}$ will achieve the goal $g_{r_i}\left(\mathfrak{j}_x\right)$ (denoted as $R_{\mathfrak{j}_x} = 1$), while $R_{\mathfrak{j}_x} = 0$ if the job fails.

In this study, trust will be utilized as a quantified indication to explain how much the $\mathfrak{R}_{r_i}$ (whose goal is $g_{r_i}\left(\mathfrak{j}\right)$) trusts $\mathfrak{f}_{p_j}$ to complete the Job $\mathfrak{j}_x$ in context C, represented as $\mathrm{T}^{\mathfrak{j}}_C\left(r_i, p_j\right)$. In SIoT, our trust model seeks to assist the $\mathfrak{R}$ in determining the trustworthiness of prospective $\mathfrak{f}$ for service delegation. However, while evaluating $\mathfrak{f}$'s trustworthiness, the $\mathfrak{R}$ must consider: (1) the $\mathfrak{f}$'s Capabilityto perform the job; (2) the $\mathfrak{f}$'s Commitment to carry out the job; and (3) the $\mathfrak{R}$'s Satisfactionon the job offered by $\mathfrak{f}$. Hence, to achieve scalability, each $\mathfrak{R}$ computes its trust score in relation to a restricted selection of requested services with which it interacts. This is also dependent on the context of the service requested from the $\mathfrak{f}$. To achieve three objectives, we consider the following parametric definition as suggested in [7]:

1) A set $\mathfrak{P}_j = \{p_1, p_2, \ldots, p_m\}$ denotes a list of $\mathfrak{f}$ IDs with which $\mathfrak{R}_{r_i}$ interacted and obtained services.
2) A set $L_j = \{l_1, l_2, \ldots, l_n\}$ representing the location of $\mathfrak{f}_{p_j}$ that performs a given job to $\mathfrak{R}_{r_i}$.
3) A set $J_x = \left\{\mathfrak{j}_1, \mathfrak{j}_2, \ldots\ldots, \mathfrak{j}_z\right\}$, representing the type of job $\mathfrak{R}_{r_i}$ requested from $\mathfrak{f}_{p_j}$.
4) A list of $\mathfrak{R}_{r_i}$ experiences represented by $E_{r_i,p_j} = \left\{\left(a_{r_i,p_j}, b_{r_i,p_j}\right), \ldots, \left(a_{r_n,p_m}, b_{r_n,p_m}\right)\right\}$, where a_{r_i,p_j} and b_{r_i,p_j} represent the positive and negative experiences of the $\mathfrak{R}_{r_i}$ respectively towards $\mathfrak{f}_{p_j}$ requesting a job $\mathfrak{j}_x$, where $x = \{1, 2, \ldots, z\}$, $i = \{1, 2, \ldots, n\}$ and $j = \{1, 2, \ldots\ldots, m\}$.
5) A list of unit trust scores (τ_{r_i,p_j}) in which $\mathfrak{R}_{r_i}$ has towards $\mathfrak{f}_{p_j}$ for performing job $\mathfrak{j}_x$ in context C. This is represented by a set $\mathrm{T}^{\mathfrak{j}}_C\left(r_i, p_j\right) = \{\tau_{r_i,p_j}, \ldots, \tau_{r_n,p_m}\}$, where $i = \{1, 2, 3, \ldots n\}$ and $j = \{1, 2, 3, \ldots m\}$.

A. ADVERSARY MODEL

In this study, we consider our adversary to have the following features:

i. An adversary can be inactive and engage in fraudulent actions to get self-centered advantages.
ii. To carry out trust-related attacks, adversaries primarily use two methods: interior enrichment and exterior exploitation.
iii. Interior enrichment illustrates how the adversary boosts its credibility through deception. Example includes whitewashing, opportunistic service, and self-promoting attacks

1) Exterior exploitation portrays the adversary purposefully increasing or decreasing the credibility of others through deception. Example includes discriminatory bad-mouthing, and ballot-stuffing attacks.

IV. PROPOSED TRUST MANAGEMENT MODEL

The general working principle of the proposed model is depicted in Figure 1. The $\mathfrak{R}_{r_i}$ will first publicize a job $\mathfrak{j}_x$ to the public, outlining its practical requirements. $\mathfrak{f}$s will assess if they can execute the request after getting it from the $\mathfrak{R}_{r_i}$, as well as the potential advantages. If an $\mathfrak{f}_{p_j}$ wishes to do the job $\mathfrak{j}_x$, it will send a response to the $\mathfrak{R}_{r_i}$ expressing its willingness to complete the specified job. After receiving the answer from the $\mathfrak{f}$s, the $\mathfrak{R}_{r_i}$ will evaluate the trustworthiness of the candidates $\mathfrak{f}$s as $\mathrm{T}^{\mathfrak{j}}_C\left(r_i, p_1\right), \mathrm{T}^{\mathfrak{j}}_C\left(r_i, p_2\right), \ldots, \mathrm{T}^{\mathfrak{j}}_C\left(r_i, p_m\right)$. Given the concluding assessment result from the trust model, the $\mathfrak{R}_{r_i}$ will select which candidate $\mathfrak{f}$ will complete the job $\mathfrak{j}_x$.

The $\mathfrak{f}_{p_j}$ will conduct the job after the delegation of the $\mathfrak{R}_{r_i}$ and provide the performance result to the $\mathfrak{R}_{r_i}$. The $\mathfrak{R}_{r_i}$ assesses and decides if it is effectively performed. As evaluation feedback to the trust model, the service findings (success or failure) are conveyed. When the $\mathfrak{R}_{r_i}$ issues the next job or service, the trust model will be updated.

As a result, we integrate three archetypal components, including Capability, Commitment, and Satisfaction, for service provider trustworthy assessment in SIoT by reference to the trust composition in social trust theory [28]. Capability denotes the $\mathfrak{f}_{p_j}$'s skills and ability to perform the assignment. Commitment shows the $\mathfrak{f}_{p_j}$'s honesty, perseverance, and drive to continue working on the assignment while remaining loyal to the $\mathfrak{R}_{r_i}$. The Satisfaction represents the $\mathfrak{R}_{r_i}$'s level of gratification towards the services rendered by $\mathfrak{f}_{p_j}$. Each of these components are discussed in detail in the following subsections.

A. CAPABILITY EVALUATION

As previously stated, service circumstances and job kinds in SIoT are various, therefore direct experience from $\mathfrak{f}_{p_j}$'s earlier task execution does not necessarily lead to an accurate assessment of its capacity to accomplish job. As a result, the capability assessment is aimed to determine if an object has adequate communication, processing, and memory resources and abilities to perform the job. Moreover, even though they are performing the same job, they may differ in form or character since various conditions require diverse demands.

As a result, it is critical to investigate if the $\mathfrak{f}_{p_j}$'s features can match the unique properties of a job $\mathfrak{j}_x$, and if

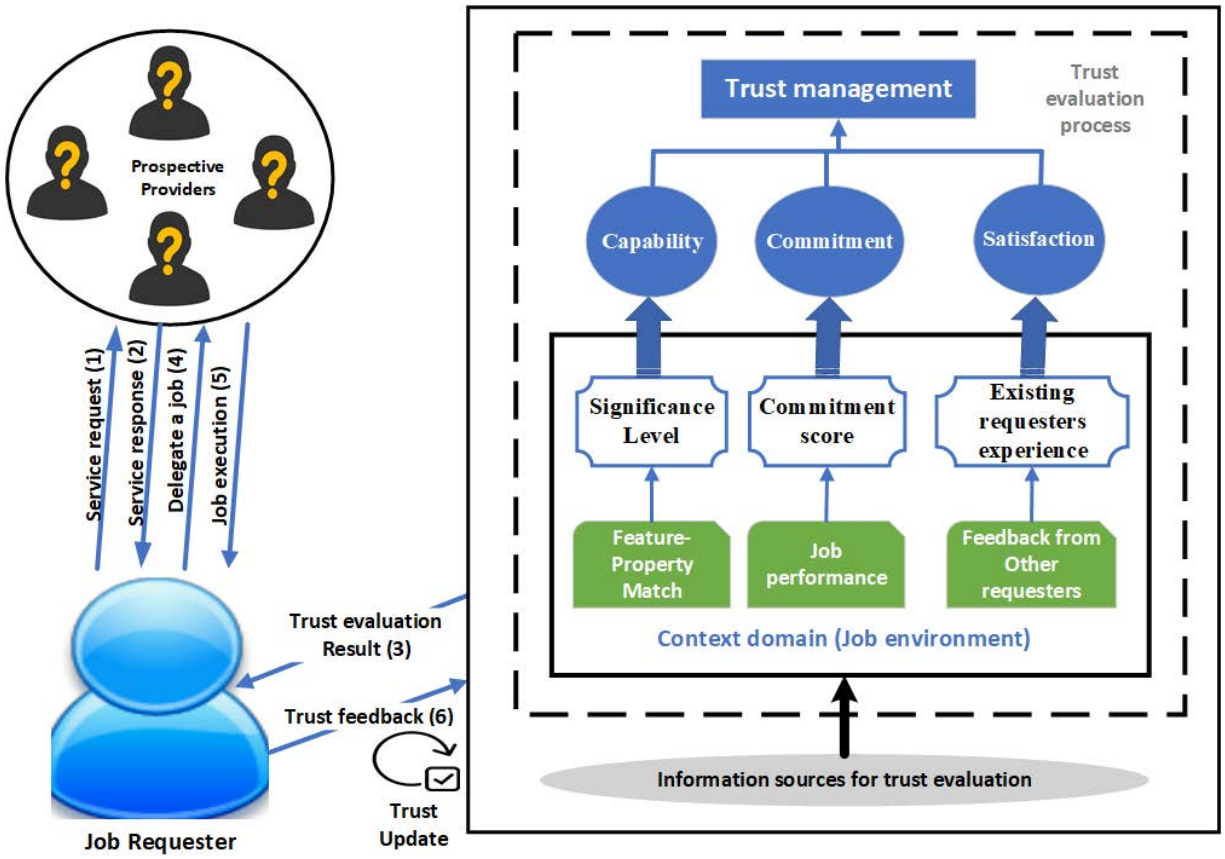

FIGURE 1. Proposed trust management model.

so, what impact such a feature has on the job's completion. To achieve a more accurate view of such appropriateness and level assessment, $\mathfrak{R}_{r_i}$ must also analyses the job satisfaction of the $\mathfrak{f}_{p_j}$s with comparable characteristics to the $\mathfrak{f}_{p_j}$. Thus, for Feature-Property matching, two parameters (Significance Level (SL) and Capability ($\mathcal{K}$)) were introduced. The SL uses past interactions to evaluate the significance of each feature to the property. And the $\mathcal{K}$ can be assessed by combining several SL.

1) SIGNIFICANCE LEVEL (SL) COMPUTATION

Given two successful consecutive job $\mathfrak{j}_1$ and $\mathfrak{j}_2$ with $\mathfrak{f}_{p_j}$ features of $\mathrm{F}_{p_j}^{\mathfrak{j}_1} = \left\{\mathfrak{f}_{p_j}^1, \mathfrak{f}_{p_j}^2, \mathfrak{f}_{p_j}^3\right\}$, and $\mathrm{F}_{p_j}^{\mathfrak{j}_2} = \left\{\mathfrak{f}_{p_j}^3, \mathfrak{f}_{p_j}^4, \mathfrak{f}_{p_j}^5\right\}$, and Job properties of $\mathcal{P}_{\mathfrak{j}_1} = \left\{\mathcal{P}_{\mathfrak{j}}^1, \mathcal{P}_{\mathfrak{j}}^2\right\} C$, and $\mathcal{P}_{\mathfrak{j}_2} = \left\{\mathcal{P}_{\mathfrak{j}}^2, \mathcal{P}_{\mathfrak{j}}^3\right\} C$ respectively and all with $R_{\mathfrak{j}_x} = 1$ success result. Then, for the past interaction and task information, the two-part feature-property relation can be computed as: $\mathrm{N}_{\mathfrak{j}_x} = \{\mathrm{F}_{p_j}^{\mathfrak{j}_x}, \mathcal{P}_{\mathfrak{j}_x}\}$. Hence, Job $\mathfrak{j}_1$ can be expressed as $\mathrm{N}_{\mathfrak{j}_1} = \left\{\left\{\mathfrak{f}_{p_j}^1, \mathfrak{f}_{p_j}^2, \mathfrak{f}_{p_j}^3\right\}, \left\{\mathcal{P}_{\mathfrak{j}}^1, \mathcal{P}_{\mathfrak{j}}^2\right\} C\right\}$. Hence, the SL of the feature $\mathfrak{f}_{p_j}^x$ to a specific property $\mathcal{P}_{\mathfrak{j}}^x$ can be expressed as:

$$SL\left(\mathfrak{f}_{p_j}^x, \mathcal{P}_{\mathfrak{j}}^x, C\right) = \frac{\sum_{\mathfrak{j}' \in \lambda} \mathcal{I}(\mathfrak{f}_{p_j}^x \in \mathrm{N}_{\mathfrak{j}'_x} R_{\mathfrak{j}'_x} = 1) C}{\sum_{\mathfrak{j}' \in \lambda} \mathcal{I}(R_{\mathfrak{j}'_x} = 1) C} \tag{1}$$

where $\mathcal{I}(\cdot)$ is indicator function and $\lambda = \{\mathfrak{j}' | \mathcal{P}_{\mathfrak{j}}^x \in \mathcal{P}_{\mathfrak{j}_x}\}$. In this regard, when a feature occurs repeatedly in accomplished jobs with a certain property, then it is highly relevant to the associated property, and conversely. For instance, considering the cases of job $\mathfrak{j}_1$ and job $\mathfrak{j}_2$, $SL\left(\mathfrak{f}_{p_j}^2, \mathcal{P}_{\mathfrak{j}}^2\right) = 1/2$, $SL\left(\mathfrak{f}_{p_j}^3, \mathcal{P}_{\mathfrak{j}}^2\right) = 1$, and $SL\left(\mathfrak{f}_{p_j}^4, \mathcal{P}_{\mathfrak{j}}^2\right) = 1/2$.

2) CAPABILITY COMPUTATION

By integrating the SL, the capability ($\mathcal{K}$) based on direct experience will be determined. When computing $\mathcal{K}$ value of a prospective $\mathfrak{f}_{p_j}$ for a new assignment, the SL of each feature of p_j for each property will be combined to get the $\mathcal{K}$ value. This can be achieved as follow:

$$\mathcal{K}\left(p_j, r_i, \mathfrak{j}_x, C\right) = \sum_{\mathcal{P}_{\mathfrak{j}_x}^h \in \mathcal{P}_{\mathfrak{j}_x}} \left(\sum_{\mathfrak{f}_{p_j}^x \in \mathrm{F}_{p_j}^{\mathfrak{j}_x}} SL\left(\mathfrak{f}_{p_j}^x, \mathcal{P}_{\mathfrak{j}}^x, C\right) / \left|\mathrm{F}_{p_j}^{\mathfrak{j}_x}\right|\right) / \left|\mathcal{P}_{\mathfrak{j}_x}\right| \tag{2}$$

where $\mathrm{F}_{p_j}^{\mathfrak{j}_x} = \left\{\mathfrak{f}_{p_j}^x | SL\left(\mathfrak{f}_{p_j}^x, \mathcal{P}_{\mathfrak{j}}^x, C\right) \geq \text{The threshold of SL in } \mathcal{K} \text{ function}\right\}$. If $SL\left(\mathfrak{f}_{p_j}^x, \mathcal{P}_{\mathfrak{j}}^x, C\right) <$ The threshold of SL in $\mathcal{K}$ function, then $\mathfrak{f}_{p_j}^x$ significance over $\mathcal{P}_{\mathfrak{j}}^x$ can be neglected. Thus, for most smart devices, the complexity of $\mathcal{K}$ computation is acceptable. It is worth noting that the $\mathcal{K}$ value is not the

$\mathfrak{f}_{p_j}$'s ultimate quantified responsibility for a given job $\mathfrak{j}_x$ at a given context C.

B. COMMITMENT EVALUATION

The $\mathfrak{f}_{p_j}$'s commitment ($\mathfrak{Q}$) can be measured by integrating the results of previous jobs. If the $\mathfrak{f}_{p_j}$ succeeds more than it has in prior jobs, then $\mathfrak{f}_{p_j}$ is more sincere and committed to continue doing the job after delegation, and vice versa. Furthermore, the timing of the job should be considered during the $\mathfrak{Q}$ design process, thus, another constrain is introduced referred as the commitment score (CS) function, which analyses performance and behaviors to fully measure the $\mathfrak{f}_{p_j}$'s commitment.

1) COMMITMENT PROPERTIES

The commitment ($\mathfrak{Q}$) should include the following properties to ensure the logic of the commitment assessment:

i. The $\mathfrak{Q}$ is supposed to be restricted to the range [0,1]. Thus, to include the results of the multidimensional assessment, $\mathfrak{Q}$ should have a consistent value space with CS.
ii. Unsuccessful jobs should weigh more than successful jobs. This is because it is wasteful to incur all expenses, such as delegated expenses, marginal expenses, communication expenses, and any additional expenses, if a task does not materialize. As a result, the $\mathfrak{Q}$ computation exhibits a bias for the value loss due to job failure that is different from increasing the credit for job success.
iii. The effect of $\mathfrak{Q}$ on job performance should be time-bound. Thus, new job performance has a larger impact on the $\mathfrak{f}_{p_j}$'s appraisal than long-standing job performance.

2) COMMITMENT COMPUTATION

As previously stated, the effect of success or failure in computing the $\mathfrak{Q}$ should decayed over time (i.e., time dependent) for a given context C. As a result, the CS is defined as follows:

$$CS\left(\mathfrak{j}_x\right) = \mu_1 R^C_{\mathfrak{j}_x} + \mu_2\left(1 - R^C_{\mathfrak{j}_x}\right) \tag{3}$$

where $\mu_1 = 1 - \left(t_0 - t_{\mathfrak{j}_x} / \mathcal{T}_{\mathfrak{t}_1}\right)^{d_1+1}$, $t_0 - t_{\mathfrak{j}_x} \leq \mathcal{T}_{\mathfrak{t}_1}$, $d_1 \geq 0$, $\mu_2 = 1 - \left(t_0 - t_{\mathfrak{j}_x} / \mathcal{T}_{\mathfrak{t}_2}\right)^{d_2+1}$, $t_0 - t_{\mathfrak{j}_x} \geq \mathcal{T}_{\mathfrak{t}_2}$, $d_2 \geq 0$. μ_1 is the decay factor for successful jobs completed, while μ_2 is the decay factor for the unsuccessful jobs. The current time instance is given as t_0, while $\mathcal{T}_{\mathfrak{t}}$ (such as $\mathcal{T}_{\mathfrak{t}_1}$ and $\mathcal{T}_{\mathfrak{t}_2}$) is the time threshold. Job $\mathfrak{j}_x$ will not be considered for CS calculation if the interval from $t_{\mathfrak{j}_x}$ to t_0 is greater than the $\mathcal{T}_{\mathfrak{t}}$. Alternatively, activities from the past are no longer relevant in representing the service provider's present commitment. The parameter d describes the rate of decay.

The $\mathcal{T}_{\mathfrak{t}}$ also represents the sensitivity factor, which regulates the impact of period between t_0 and $t_{\mathfrak{j}_x}$ to $CS(\mathfrak{j}_x)$. For example, if the current time $t_0 = t_{\mathfrak{j}_x} + \mathcal{T}_{\mathfrak{t}}$, the $CS(\mathfrak{j}_x)$ with $\mathcal{T}_{\mathfrak{t}_1}$ will be of the preceding time (i.e., 0). However, the $CS(\mathfrak{j}_x)$ with $\mathcal{T}_{\mathfrak{t}_2}$ stays high, indicating that with a higher $\mathcal{T}_{\mathfrak{t}}$, Job $\mathfrak{j}_x$ will have a longer impact on commitment assessment. Thus, with a greater d and $\mathfrak{j}_x$ set in μ_2 than those in μ_1 (i.e. $d_2 > d_1$ and $\mathcal{T}_{\mathfrak{t}_2} > \mathcal{T}_{\mathfrak{t}_1}$), the $CS(\mathfrak{j}_x)$ will have a slower decay rate and a lengthier period when $R_{\mathfrak{j}_x} = 0$. Given the function of $CS(\mathfrak{j}_x)$, the commitment $\mathfrak{Q}\left(r_i, p_j\right)$ is expressed as follows:

$$\mathfrak{Q}\left(r_i,\ p_j\right) = \left(\left[\sum\nolimits_{\mathfrak{j}_x \in J, R_{\mathfrak{j}_x}=1} CS\left(\mathfrak{j}_x\right)\right] + 1\right) \Big/ \left[\sum\nolimits_{\mathfrak{j}_x \in J} CS\left(\mathfrak{j}_x\right)\right] + 2 \tag{4}$$

where $J = \{\mathfrak{j}_x | \mathfrak{f}_{\mathfrak{j}_x} = p_j,\ \mathfrak{r}_{\mathfrak{j}_x} = r_i\}$. Consequently, the computation of $\mathfrak{Q}$ meets all three of the properties at the same time. It is presumed that the initial value of $\mathfrak{Q}$ is 0.5, indicating that the $\mathfrak{r}_{r_i}$ is entirely unsure about the $\mathfrak{f}_{p_j}$'s commitment. By integrating CS, $\mathfrak{r}_{r_i}$ will have a more precise idea of the $\mathfrak{f}_{p_j}$'s commitment as they continue to engage and provide services. It is important to emphasize that the $\mathfrak{Q}$ estimated does not represent the $\mathfrak{f}_{p_j}$'s ultimate trust score in each job.

C. SATISFACTION EVALUATION

The satisfaction $\mathcal{S}^{\mathfrak{j}_x}_{r_i,p_j}$ of $\mathfrak{r}_{r_i}$ over a job $\mathfrak{j}_x$ completed by $\mathfrak{f}_{p_j}$ can be evaluated using direct requester interaction experience ratings, which are dependent on the $\mathfrak{f}_{p_j}$'s various accessible contexts. The major contexts examined in this section is the quality of service achieved based on a given context in terms of non-functional qualities such as response time for each requested job. In job assessment, $\mathfrak{r}_{r_i}$ can offer a feedback evaluation of $\mathfrak{f}_{p_j}$ based on non-functional qualities following direct contacts. Response time, throughput, $\mathfrak{f}_{p_j}$ availability, job cost, and so on are examples of non-functional characteristics. Thus, E_{r_i,p_j} is the existing requester interaction experience of $\mathfrak{r}_{r_i}$ towards $\mathfrak{f}_{p_j}$ offering job $\mathfrak{j}_x$ at a given location based on established context of non-functional qualities.

Given the scale of the trust measures, the proposed model uses the existing requester experience E_{r_i,p_j}'s value between 0 and 1. Table 2 shows all requester experience values to which $\mathfrak{r}_{r_i}$ can assign an E_{r_i,p_j} value. When a given $\mathfrak{r}_{r_i}$ has reputable interaction with its peer ($\mathfrak{f}_{p_j}$), it assigns a number ranging from 0.6 to 1, with 1 being a fully trusted interaction. Likewise, when identifying harmful behavior on the $\mathfrak{f}_{p_j}$, then $\mathfrak{r}_{r_i}$ can assign a value between 0 and 0.5, with 0 being a totally malicious interaction and 0.5 representing a relatively low degree of mistrust. These values, which are allocated to E_{r_i,p_j} are utilized to compute $\mathfrak{f}_{p_j}$ satisfaction $\mathcal{S}^{\mathfrak{j}_x}_{r_i,p_j}$ over a job $\mathfrak{j}_x$.

From equation (1), the parameters a_{r_i,p_j} and b_{r_i,p_j} are adjusted based on trust decay while considering the existing requester experience E_{r_i,p_j}.

$$\begin{aligned} a_{r_i,p_j} &= \varepsilon^{-\mu\Delta t} \times a_{r_i,p_j}(old) + E_{r_i,p_j} \\ b_{r_i,p_j} &= \varepsilon^{-\mu\Delta t} \times b_{r_i,p_j}(old) + (1 - E_{r_i,p_j}) \end{aligned} \tag{5}$$

where μ is the decay factor, Δt represents the trust update cycle and $\varepsilon^{-\mu\Delta t}$ is the exponential decay on old values of a_{r_i,p_j} and b_{r_i,p_j}, while E_{r_i,p_j} and $1 - E_{r_i,p_j}$ contribute to positive and negative experiences respectively.

TABLE 2. Experience assessment scales.

Values	Experience level
0	Inexperience
0.1	Absolute mistrust
0.2	Severe mistrust
0.3	High mistrust
0.4	Relatively high mistrust
0.5	Relatively low mistrust
0.6	Relatively low trust
0.7	Relatively high trust
0.8	High trust
0.9	Strong trust
1	Absolute trust

Hence, the satisfaction $\mathcal{S}^{j_x}_{r_i,p_j}$ of requester $\mathcal{R}_{r_i}$ towards a job j_x offered by a provider $\mathcal{f}_{p_j}$ can be expressed as:

$$\mathcal{S}^{j_x}_{r_i,p_j} = \frac{a_{r_i,p_j}}{a_{r_i,p_j} + b_{r_i,p_j}} \tag{6}$$

D. OVERALL TRUST COMPUTATION

Having all the three parameters (capability, commitment, and satisfaction) explained, the overall trust formulation can be expressed as follow:

$$\mathcal{T}^{j}_{C}\left(r_i, p_j\right) = \alpha\left(\mathcal{K}\left(p_j, r_i, j_x, C\right)\right) + \beta\left(\mathcal{Q}\left(r_i, p_j\right)\right) + \gamma\left(\mathcal{S}^{j_x}_{r_i,p_j}\right) \tag{7}$$

where α, β, γ are the respective weight used in the equation. Besides, the overall trust computation processes are summarized in Algorithm 1.

E. JOB ASSIGNMENT

The job assignment is carried out following the successful computation of capability ($\mathcal{K}$), commitment ($\mathcal{Q}$), satisfaction ($\mathcal{S}^{j_x}_{r_i,p_j}$), and total trust value. This can be achieved as follow:

$$\mathcal{f}_{p_j} = arg_{p_j} \max \mathcal{T}^{j}_{C}\left(r_i,\ p_j\right) \quad s.t. \begin{cases} \mathcal{K}\left(p_j, r_i, j_x, C\right) \geq \mathcal{T}_{\mathcal{K}} \\ \mathcal{Q}\left(r_i, p_j\right) \geq \mathcal{T}_{\mathcal{Q}} \\ \mathcal{S}^{j_x}_{r_i,p_j} \geq \mathcal{T}_{\mathcal{S}} \end{cases} \tag{8}$$

where the $\mathcal{T}_{\mathcal{K}}, \mathcal{T}_{\mathcal{Q}}$, and $\mathcal{T}_{\mathcal{S}}$ are the thresholds for the capability, commitment, and satisfaction respectively. The thresholds support the service requester in selecting a more appropriate service provider.

Furthermore, the thresholds aid in avoiding trust forgery in malicious behavior. A potential service provider may urge object to enhance its trust thereby misleading the service requester about its high capability and commitments in a counterfeit method. Moreover, even if the service provider's overall trust score is good, the service provider is still untruthful to the service requester if the degree of satisfaction is less than the threshold.

Algorithm 1: Trust Computation Process

Input: $\alpha, \beta, \gamma, f^{x}_{p_j}, \mathcal{P}^{x}_{j}, C, j_x$

Output: $\mathcal{T}^{j}_{C}\left(r_i, p_j\right)$

Function *Compute_Capability_Commitment_Satisfaction* $(\mathcal{K}, \mathcal{Q}, \mathcal{S}^{j_x}_{r_i,p_j})$
  For all $J_x = \{j_1, j_2, \ldots\ldots, j_z\}$, *and* $\mathcal{P}_j = \{p_1, p_2, \ldots, p_m\}$ **do**
    While $\mathcal{R}_{r_i}$.Request = True *and* $\mathcal{f}_{p_j}$.*Response* = *True* **do**
      Compute: $SL\left(f^{x}_{p_j}, \mathcal{P}^{x}_{j}, C\right)$ using equation (1)
      Compute: $\mathcal{K}\left(p_j, r_i, j_x, C\right)$ using equation (2)
      Compute: $CS\left(j_x\right)$ using equation (3)
      Compute: $\mathcal{Q}\left(r_i, p_j\right)$ using equation (4)
      Compute: a_{r_i,p_j} and b_{r_i,p_j} using equation (5)
      Compute: $\mathcal{S}^{j_x}_{r_i,p_j}$ using equation (6)
      Return $\mathcal{K}\left(p_j, r_i, j_x, C\right), \mathcal{Q}\left(r_i, p_j\right), \mathcal{S}^{j_x}_{r_i,p_j}$
    End
  End
Function *Compute_Trust_Score* $\left(\mathcal{T}^{j}_{C}\left(r_i, p_j\right)\right)$
  While $\mathcal{R}_{r_i}$.Request = True *and* $\mathcal{f}_{p_j}$.*Response* = *True* **do**
    $\mathcal{T}^{j}_{C}\left(r_i, p_j\right) = \alpha\left(\mathcal{K}\left(p_j, r_i, j_x, C\right)\right) + \beta\left(\mathcal{Q}\left(r_i, p_j\right)\right) + \gamma\left(\mathcal{S}^{j_x}_{r_i,p_j}\right)$
    Return $\mathcal{T}^{j}_{C}\left(r_i, p_j\right)$
  End

V. SECURITY ANALYSIS

In this SIoT-based proposed trust model, we identify and explain six common forms of trust-related attacks based on the given adversary model. Discussions on security analysis were provided in this section to examine how the trust model resists the aforesaid trust-related attacks.

A. INTERIOR ENRICHMENT

1) WHITEWASHING ATTACK

A hostile service provider will try to redefine its confidence by adding a new identity to the system in this kind of attack. Although a malicious service provider may alter their identity very quickly, it requires time and expense to repair trustworthiness social ties, the malicious service provider must also reject all trust that certain service requesters have previously built. It is crucial to highlight that our model's primary focus is weak security problems; hence, identification checks alone may not be sufficient to avoid this type of attack.

2) OPPORTUNISTIC SERVICE ATTACK

It is assumed in this study that a drop in a service provider's trustworthiness is proportionate to a fall in the probability of service delegation. As a result, if a malicious service provider's reputation is low, the likelihood of job assignments lowered. Thus, it cannot opportunistically boost its trustworthiness by delivering a huge number of services in the near term. Furthermore, given the values of $\mathcal{T}_{t_2}$ *and* d_2 in equation (3), poor performance will be penalized, resulting in

longer and more significant negative impacts on assessment, thus opportunistic service attack cannot remove such negative effects in the near run.

3) SELF-PROMOTING ATTACK

The model is based on past job histories to determine the credibility of the prospective service provider, which will prevent the attack since the service requester will not accept the prospective malicious service provider's self-recommendation. Another unique attack method is for the malicious service provider to generate many false feedbacks to endorse it as credible. However, in this trust model, this method is equally ineffectual since these false feedbacks will have a low weight in the sight of the service requesters, and the contribution of the trust-related information they offer will be worthless to the trust assessment of the malicious service provider.

B. EXTERIOR EXPLOITATION

1) DISCRIMINATORY ATTACK

The computation of trust assimilation from various sources in this approach is dependent on the degree of social relationship, which the adversary lacks. If an adversary wishes to launch the discriminatory attack, it must first discover as many social links as possible among objects to create conflict, which is difficult and impractical. Furthermore, initiating discriminatory attack is hazardous because it may result in the model's adversary being punished for lack of trust. Besides, the trust score of an adversary suffers greatly when it launches a discriminatory attack to a powerful service requester. As a result, discriminatory attack is ineffective in this trust model.

2) BAD-MOUTHING ATTACK

The more feedbacks the service requester received in this model; the less weight the harmful object's opinions had on the evaluation of the prospective service provider. Thus, for a malicious object to carry out this type of attack against a trustworthy service provider, the malicious object must first establish a high social relationship with the service requester, and trust-related feedback obtained by the service requester from other sources about the trustworthy service provider should be as limited as possible. As a result, malicious objects have a great difficulty determining or incorrectly influencing general trust-related feedbacks, thus it will be difficult for bad-mouthing attack to succeed.

3) BALLOT-STUFFING ATTACK

Ballot-stuffing attack's condition is nearly identical to bad-mouthing attack's; nevertheless, ballot-stuffing attack is more difficult to attain than bad-mouthing attack. As a result, in addition to the constraint set above against bad-mouthing attack, the adversary must guarantee that the condition $\mathcal{Q}\left(r_i, p_j\right) \geq \mathcal{T}_{\mathcal{Q}}$ and $\mathcal{K}\left(p_j, r_i, \mathrm{j}_x, C\right) \geq \mathcal{T}_{\mathcal{K}}$ is satisfied as indicated in equation (9). This requirement, however, is obviously extremely difficult for the adversary to achieve. As a result, an adversary finds it difficult to execute ballot-stuffing attack.

VI. PERFORMANCE ANALYSIS

This section describes the simulation setup utilized to implement our proposed model (ConTrust), as well as the performance parameters that were employed. Furthermore, the assessment findings were compared to those of the benchmark models Jafarian *et al.* [8] and Aslam *et al.* [10]. The benchmark models were selected based on their recentness and contextual similarity to our proposed model.

A. SIMULATION SETUP

ConTrust model was implemented using python libraries, and a PC with Intel(R) Core (TM) i3-3217U CPU @ 1.80GHz was used for the experiments. To prevent bias and get the best observation and findings, all models were implemented in the same setup context. Moreover, the same weights of 0.5, 0.3, and 0.2 were used in all models for α, β and γ. Furthermore, the following parameter values were used in the simulations:

1) The SIoT environment population was limited to 400 participants (both service requesters and providers) by increasing the population in each scenario.
2) Each service contact comprised two randomly selected parties (requester and provider).
3) Interactions were performed in minutes, and 800 interactions were conducted in 800 minutes, such that each of the 400 participants functioned as a requester or provider in distinct situations.
4) The Percentage of malicious service providers was varied between 10% to 100% in different testing scenario.
5) The two essential parameters d_1 and $\mathcal{T}_{t_1}$ in μ_1, which represent the rate of decay and sensitivity factor in the $\mathcal{Q}\left(r_i, p_j\right)$ function for completed jobs, were assigned initial values of 2 and 100, respectively.
6) The two essential parameters d_2 and $\mathcal{T}_{t_2}$ in μ_2, which represent the rate of decay and sensitivity factor in the $\mathcal{Q}\left(r_i, p_j\right)$ function for failed jobs, were assigned initial values of 5 and 200, respectively.
7) The capability, commitment, and satisfaction thresholds $\mathcal{T}_{\mathcal{K}}$, $\mathcal{T}_{\mathcal{Q}}$, and $\mathcal{T}_{\mathcal{S}}$ in job assignment were set to initial values of 0.5, 0.6, and 0.5, respectively.

We trained our model to include service providers in six distinct categories to measure the trustworthiness outcomes of service providers with varied behavioral traits. These categories include:

Absolutely credible: These are exceptional service providers with exceptional talents that always do their work honestly. The likelihood of these types of service providers in completing a job is 100 percent.

Highly credible:These are great service providers with strong capabilities that always do their work honestly. The likelihood of these service providers completing a job is about 85 percent.

Fairly credible: These are ordinary service providers with basic competencies who may occasionally be neglectful in completing a job. The likelihood of these service providers completing a job is around 65 percent.

Highly mistrusted: These are malicious service providers with rudimentary capabilities who will occasionally purposefully fail jobs. The likelihood of these service providers completing a job is around 45 percent.

Extremely mistrusted: These are ineffective passive service providers with limited capabilities who consistently fail to complete jobs. The likelihood of these types of service providers completing a job is around 25 percent.

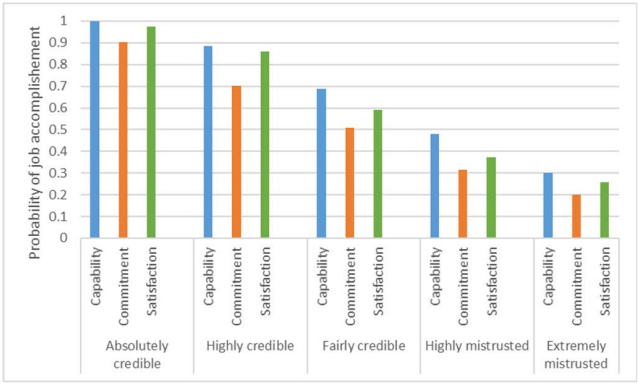

FIGURE 2. Job accomplishment with respect to varying service provider's behaviors.

B. PERFORMANCE METRICS AND EVALUATION

To assess the performance of the ConTrust, several metrics were used, such as average trust scores, probability of job completion, average execution latency, and the resiliency of our model to the identified attacks. The evaluation results were discussed in the following subsections.

1) TRUST EVALUATION

The effective rate of capability, as shown in Figure 2, is roughly proportional to the percentage of completed jobs. The reasoning behind this is that the service requester will gradually realize the full potential of the service provider and the feature-property relationship through direct contact between the two parties. Moreover, the commitment is lower than the capability because the proposed model's punitive process weights unsuccessful jobs more heavily when assessing a service provider's commitment.

Besides, Figure 3 demonstrates that under our trust model, even if the service requester does not have a significant number of contacts over a lengthy period, he or she may nevertheless create the experience of direct connection with other service requesters and form an accurate assessment about a given service provider. As a result, our approach enables the service requester to easily differentiate between different categories of service providers for job assignment.

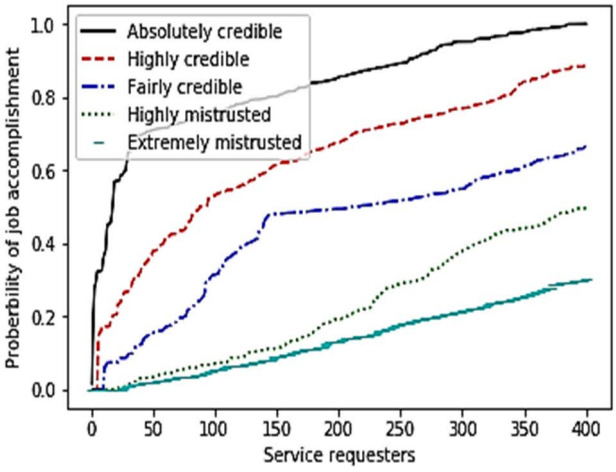

FIGURE 3. Job accomplishment with respect to varying number of previous service requesters in the system.

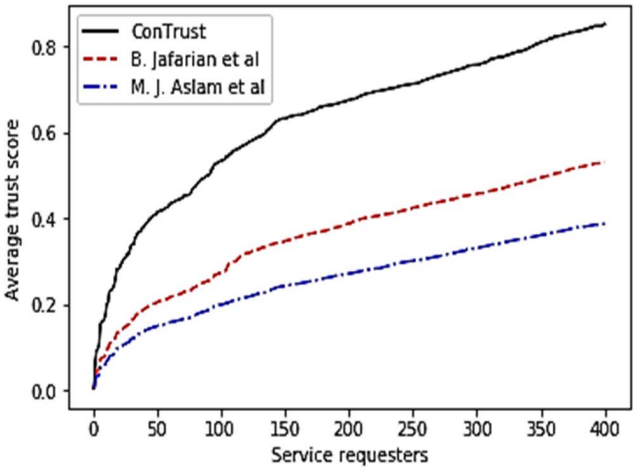

FIGURE 4. Trust score with respect to varying number of previous service requesters in the system.

Figure 4 depicts the findings for all models in terms of trust score, which clearly shows that ConTrust has a considerably higher trust score than the models provided in [8]and [10].

When compared to both benchmark models, simulation results reveal that ConTrust earned a trust score of 49.4 percent more. ConTrust can calculate a reasonable trust score in the context of mistrusted service providers by combining the three essential elements of *Capability, Commitment,*and*Satisfaction*. However, benchmark models are incapable of calculating a fair trust score for service providers. This is due to service providers influenced or manipulated experience feedbacks obtained from service providers that the benchmark model failed to detect accurately. As a result, the trust score of the service provider is incorrectly computed using the benchmark models. Thus, ConTrust can compute the trust of a service provider based on prior experience feedbacks which are based on their performance in terms of Capability, Commitment, and Satisfaction to complete the service requester's demands.

2) OVERALL EXECUTION LATENCY

The execution latency in this model is proportional to the model's average computing cost. Figure 5 depicts the average transaction latency for both models. When compared to the benchmark model, the ConTrust has significantly reduced latency. Furthermore, when the number of participants increased, the latency in the ConTrust model varied minimally, but the latency in the benchmark models changed dramatically. The average latency of 400 participants in our model, on the other hand, is 59.22 percent lower than the benchmark model. This is due to the removal of clustering methods, which require more processing.

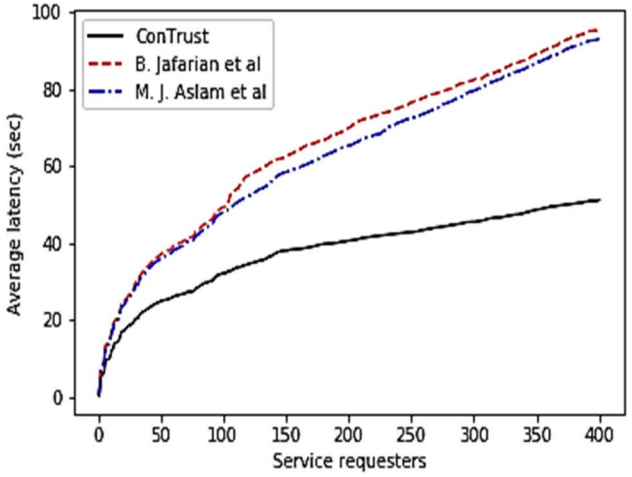

FIGURE 5. Average execution latency with respect to varying number of previous service requesters in the system.

3) RESILIENCY

To mimic the enormous interaction behaviors and job assignments, we vary the fraction of service requesters impacted by malicious service providers from 10% to 100% in this section. During the first phase, all service requesters will create three familiar connections with other objects. In our studies, the degree of social relationship of familiar ties is organized according to the design given in section 5.1. Furthermore, when a service requester initially enters the system, interaction with familiar objects seems to be more probable. As a result, several jobs that happen among familiar objects were pre-programmed so that the service requester could gain an early understanding of the Capability, Commitment, and Satisfaction attributes.

The resilience of our model to the identified attacks is defined in this study as the ratio between the probability of the attack's failure in the system and the percentage of service requesters affected by the same attack. In this experiment, ConTrust's robust performance is compared to the benchmark models of [8] and [10]. The experiment was also carried out to evaluate the resilience of all the models against all the identified attacks provided in section 2.2, and the results of these tests are shown in Figure 6 to 11. According to

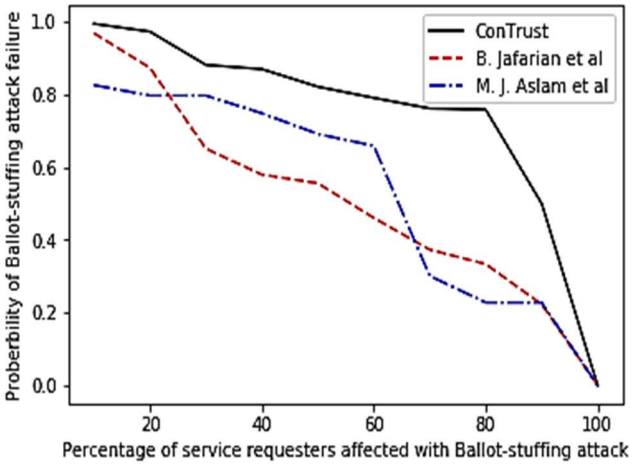

FIGURE 6. Resiliency against ballot-stuffing attack.

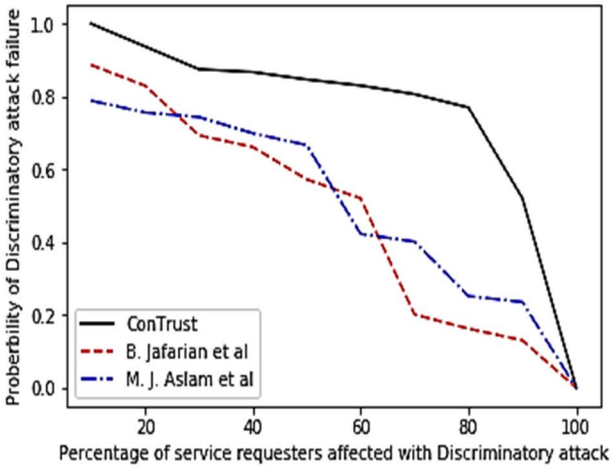

FIGURE 7. Resiliency against discriminatory attack.

the findings, the proposed ConTrust model, which combines the Capability, Commitment, and Satisfaction characteristics, will be better suited for trust assessment, improving resistance to identified attacks as well as job completion success.

Conclusively, if the fraction of prior service requesters affected by the malicious service provider grows, all models will be affected to some extent. When the findings (Figures 6–11) are compared, the opportunistic service attack (Figure 11) has the largest detrimental influence on the ConTrust model. Nonetheless, the ConTrust model has a higher tolerance than the benchmark models. It is proven that the ConTrust model can successfully assist the service requester in identifying trustworthy service providers even in the presence of malicious objects.

C. COMPARATIVE ANALYSIS

According to Table 3, the subjected model studied by M.J. Aslam *et al.* has less trust computation capabilities and may be vulnerable to several other trust-based attacks. On average, the B. Jafarian *et al.* scheme outperforms the

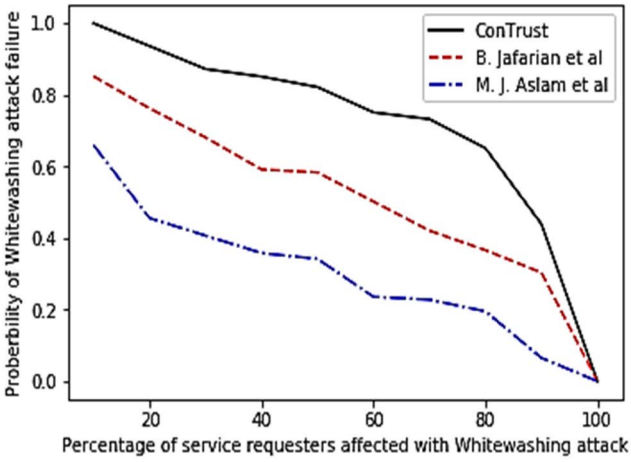

FIGURE 8. Resiliency against whitewashing attack.

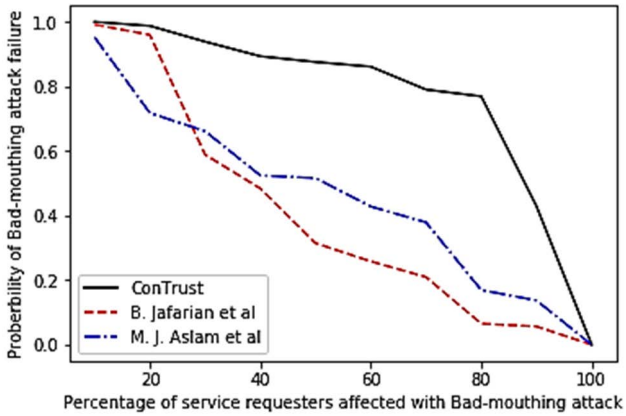

FIGURE 9. Resiliency against bad-mouthing attack.

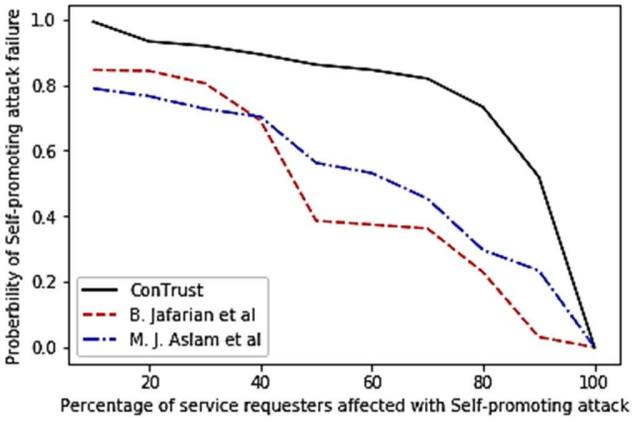

FIGURE 10. Resiliency against self-promoting attack.

M.J. Aslam *et al.* scheme, which likewise uses solely direct experience and familiar objects as sources of trust evaluation. Both systems are asserted to have a primary drawback in that they depend only on direct experience and familiar objects, which may be impacted by self-promoting, opportunistic, and whitewashing attacks, resulting in a biased trust computation.

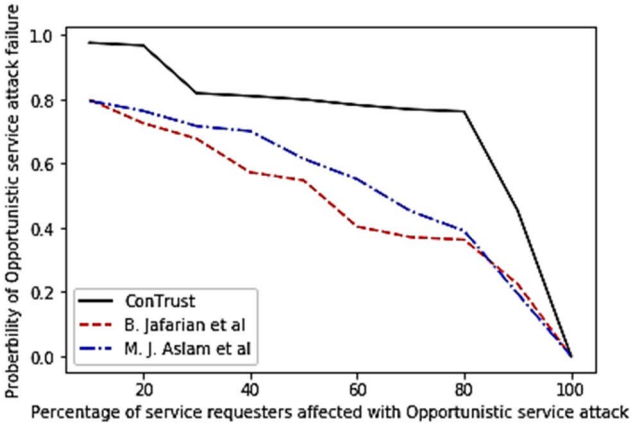

FIGURE 11. Resiliency against opportunistic service attack.

TABLE 3. Comparison of security features.

Security features	B. Jafarian et al.	M.J. Aslam et al.	ConTrust
Resilience to whitewashing attack	NO	NO	YES
Resilience to opportunistic service attack	NO	NO	YES
Resilience to self-promoting attack	NO	NO	YES
Resilience to discriminatory attack	YES	YES	YES
Resilience to bad-mouthing attack	YES	YES	YES
Resilience to ballot-stuffing attack	YES	NO	YES
Strong trust computation	NO	NO	YES
Applicability in a dynamic situation	NO	NO	YES
Sources for trust assessment	Direct experience and familiar objects	Direct experience and familiar objects	Direct experience, familiar and unfamiliar objects
High scalability	NO	NO	YES

Similarly, both methods implemented with a small number of participants in consideration. Thus, when a greater number of participants is involved, the schemes have less influence. However, the proposed ConTrust model is scalable and can be employed in dynamic situations.

VII. CONCLUSION

This paper offers a context-dependent trust management approach (ConTrust) for selecting a trustworthy service provider and assigning jobs in a SIoT environment. A comprehensive trust model in SIoT was created by integrating trust theory with social networks. The combination of capability, commitment, and satisfaction, as well as the feature-property match technique, will improve the efficiency of trust assessment and the resolution of context-dependent

issues. To protect the system from potential attacks, this paper offered flexible capability, commitment, and satisfaction computation techniques.

The proposed trust model remains cognizant of job characteristics, object capacities and truthfulness, as well as the impact of malicious behavior. The experimental findings demonstrate the viability of our proposed ConTrust model and its capacity to ensure the reliability and effectiveness of SIoT operations. In future, the model will be implemented in real physical nodes. Similarly, the model will be expanded to cover other possible forms of trust-related attacks that were not covered in this work.

ACKNOWLEDGMENT

The author would like to acknowledge the support of Prince Sultan University for paying the Article Processing Charges (APC) of this publication.

REFERENCES

[1] N. B. Truong, H. Lee, B. Askwith, and G. M. Lee, "Toward a trust evaluation mechanism in the social Internet of Things," *Sensors*, vol. 17, no. 6, p. 1346, 2017.

[2] D. Hussein, S. N. Han, G. M. Lee, N. Crespi, and E. Bertin, "Towards a dynamic discovery of smart services in the social Internet of Things," *Comput. Electr. Eng.*, vol. 58, pp. 429–443, Feb. 2017.

[3] J. E. Kim, X. Fan, and D. Mosse, "Empowering end users for social Internet of Things," in *Proc. IEEE/ACM 2nd Int. Conf. Internet-Things Design Implement. (IoTDI)*, Apr. 2017, pp. 71–82.

[4] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The social Internet of Things (SIoT)—When social networks meet the Internet of Things: Concept, architecture and network characterization," *Comput. Netw.*, vol. 56, no. 16, pp. 3594–3608, Nov. 2012.

[5] M. Khani, Y. Wang, M. A. Orgun, and F. Zhu, "Context-aware trustworthy service evaluation in social Internet of Things," in *Proc. Int. Conf. Service-Oriented Comput.*, in Lecture Notes in Computer Science: Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics, 2018, pp. 129–145.

[6] L. Wei, J. Wu, C. Long, and B. Li, "On designing context-aware trust model and service delegation for social Internet of Things," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4775–4787, Mar. 2021.

[7] A. Altaf, H. Abbas, F. Iqbal, F. A. Khan, S. Rubab, and A. Derhab, "Context-oriented trust computation model for industrial Internet of Things," *Comput. Electr. Eng.*, vol. 92, Jun. 2021, Art. no. 107123.

[8] B. Jafarian, N. Yazdani, and M. S. Haghighi, "Discrimination-aware trust management for social Internet of Things," *Comput. Netw.*, vol. 178, Sep. 2020, Art. no. 107254.

[9] O. B. Abderrahim, M. H. Elhedhili, and L. Saidane, "CTMS-SIOT: A context-based trust management system for the social Internet of Things," in *Proc. 13th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2017, pp. 1903–1908.

[10] M. J. Aslam, S. Din, J. J. P. C. Rodrigues, A. Ahmad, and G. S. Choi, "Defining service-oriented trust assessment for social Internet of Things," *IEEE Access*, vol. 8, pp. 206459–206473, 2020.

[11] I.-R. Chen, F. Bao, and J. Guo, "Trust-based service management for social Internet of Things systems," *IEEE Trans. Dependable Secure Comput.*, vol. 13, no. 6, pp. 684–696, Nov. 2016.

[12] I.-R. Chen, J. Guo, and F. Bao, "Trust management for SOA-based IoT and its application to service composition," *IEEE Trans. Services Comput.*, vol. 9, no. 3, pp. 482–495, May 2016.

[13] B. T. Mi, X. Liang, and S. S. Zhang, "A survey on social Internet of Things," *Jisuanji Xuebao/Chin. J. Comput.*, 2018.

[14] W. Abdelghani, C. A. Zayani, I. Amous, and F. Sèdes, "Trust management in social Internet of Things: A survey," in *Proc. Conf. e-Bus., e-Services e-Soc.*, in Lecture Notes in Computer Science: Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics, 2016, pp. 430–441.

[15] M. R. Rashmi and C. V. Raj, "A review on trust models of social Internet of Things," in *Emerging Research in Electronics, Computer Science and Technology* (Lecture Notes in Electrical Engineering). Singapore: Springer, 2019, pp. 203–209.

[16] M. M. Rad, A. M. Rahmani, A. Sahafi, and N. N. Qader, "Social Internet of Things: Vision, challenges, and trends," *Hum.-Centric Comput. Inf. Sci.*, vol. 10, no. 1, Dec. 2020.

[17] J. S. Coleman, "The vision of foundations of social theory," *Analyse Kritik*, vol. 14, no. 2, pp. 117–128, Nov. 1992.

[18] M. Nitti, R. Girau, and L. Atzori, "Trustworthiness management in the social Internet of Things," *IEEE Trans. Knowl. Data Eng.*, vol. 26, no. 5, pp. 1253–1266, May 2014.

[19] J. S. Sichman, R. Conte, C. Castelfranchi, and Y. Demazeau, "A social reasoning mechanism based on dependence networks," in *Proc. 11th Eur. Conf. Artif. Intell.*, 1994, pp. 416–420.

[20] N. R. Jennings, "Commitments and conventions: The foundation of coordination in multi-agent systems," *Knowl. Eng. Rev.*, vol. 8, no. 3, pp. 223–250, Sep. 1993.

[21] I. U. Din, M. Guizani, B.-S. Kim, S. Hassan, and M. K. Khan, "Trust management techniques for the Internet of Things: A survey," *IEEE Access*, vol. 7, pp. 29763–29787, 2019.

[22] B. Pourghebleh, K. Wakil, and N. J. Navimipour, "A comprehensive study on the trust management techniques in the Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 9326–9337, Dec. 2019.

[23] A. I. A. Ahmed, S. H. A. Hamid, A. Gani, S. Khan, and M. K. Khan, "Trust and reputation for Internet of Things: Fundamentals, taxonomy, and open research challenges," *J. Netw. Comput. Appl.*, vol. 145, Nov. 2019, Art. no. 102409.

[24] M. A. Rahman and M. S. Hossain, "m-Therapy: A multisensor framework for in-home therapy management: A social therapy of things perspective," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2548–2556, Aug. 2018.

[25] H. Xiao, N. Sidhu, and B. Christianson, "Guarantor and reputation based trust model for social Internet of Things," in *Proc. Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Aug. 2015, pp. 600–605.

[26] N. B. Truong, T.-W. Um, and G. M. Lee, "A reputation and knowledge based trust service platform for trustworthy Social Internet of Things," in *Proc. 19th Int. Conf. Innov. Clouds*, 2016, pp. 104–111.

[27] Y. B. Saied, A. Olivereau, D. Zeghlache, and M. Laurent, "Trust management system design for the Internet of Things: A context-aware and multi-service approach," *Comput. Secur.*, vol. 39, pp. 351–365, Nov. 2013.

[28] Y. Wang, I.-R. Chen, J.-H. Cho, A. Swami, Y.-C. Lu, C.-T. Lu, and J. J. P. Tsai, "CATrust: Context-aware trust management for service-oriented ad hoc networks," *IEEE Trans. Services Comput.*, vol. 11, no. 6, pp. 908–921, Nov. 2018.

[29] V. Mohammadi, A. M. Rahmani, A. M. Darwesh, and A. Sahafi, "Trust-based recommendation systems in Internet of Things: A systematic literature review," *Hum.-Centric Comput. Inf. Sci.*, vol. 9, no. 1, pp. 1–61, Dec. 2019.

RABIA LATIF received the M.S. and Ph.D. degrees in information security from the National University of Sciences and Technology, Pakistan, in 2010 and 2016, respectively. She is currently working as an Assistant Professor with the College of Computer and Information Sciences, Prince Sultan University, Riyadh, Saudi Arabia. She is an Active Member of the Artificial Intelligence Data Analytics Research Laboratory, Prince Sultan University. Her research interests include cloud computing security, healthcare data security, web security, cyber security, and network security. She has several professional certifications on her credit, including CND, CEH, ECSA, VCTA-DCV, VCTA, and NV. Her professional career consists of activities ranging from the conference publication chair, a technical program committee member, and a reviewer for several international journals and conferences.