Journal of Computer Science

Research Article

Latent Feature-Based Trust-Aware Model for Service Delegation in Social Internet of Things (SIoT)

Rahul[1], Venkatesh[1] and Satish B Basapur[2]

[1]*Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bengaluru, India*
[2]*Department of Computer Science and Engineering, RV Institute of Technology and Management, Bengaluru, India*

Article history
Received: 11-03-2025
Revised: 30-05-2025
Accepted: 23-06-2025

Corresponding Author:
Rahul
Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bengaluru, India
Email: gaikwad005@gmail.com

Abstract: The integration of social networking concepts into the Internet of Things (IoT) paradigm has given rise to Social IoT (SIoT) ecosystems, aiming to address challenges related to network navigation, service discovery, and service composition. A fundamental issue in SIoT is the careful selection of trustworthy devices that provide services. A service provider can offer multiple and diverse services, and different service providers may offer the same services with varying parameters, making it difficult for service requesters to navigate and identify the best service provider that meets their requirements. Moreover, heterogeneous devices and dynamic social relationships in SIoT networks pose challenges in recommending reliable service providers. This research focuses on identifying and recommending consistent and trustworthy service providers in SIoT. The proposed trust model evaluates interactions, friendships, community similarity, cooperativeness, hidden features of service providers and their services, and predicts uncertainties associated with service providers while assessing their trustworthiness. A set of research experiments is conducted on an available dataset to demonstrate the effectiveness and efficiency of the proposed method. The trust model leverages device interactions, cooperativeness, trustworthy relationships, usage patterns, and uncertainty features of service providers. The Root Mean Square Error (RMSE) and Mean Square Error (MSE) metrics are used to evaluate the accuracy of service provider recommendations in the SIoT environment. The proposed model achieves lower RMSE and MSE values, indicating improved recommendation performance. Additionally, the Normalized Discounted Cumulative Gain (NDCG) metric is employed to assess the quality and efficiency of the recommended service providers. The proposed trust model achieves an NDCG score of approximately 90%, demonstrating its ability to recommend highly trusted service providers effectively.

Keywords: Social-Internet-of-Things, Trust Aware, Service Recommendations, Feature-Aware

Introduction

The Internet of Things (IoT) is a network of ubiquitously distributed, identifiable, interconnected devices that use widely accepted communication protocols for interactions (Li *et al*., 2015). The resource-constrained IoT devices exchange data and collaborate across various domains. IoT is not a collection of interconnected devices IoT extends beyond a global ecosystem of connected devices; it also encompasses enabling technologies, essential services, and diverse applications (Mishra and Pandya, 2021). IoT can be viewed as a network designed to facilitate interactions where devices or nodes can either request or provide services. Furthermore, these nodes can cooperate to deliver integrated solutions (Wu and Liang, 2021). Since its inception, IoT has witnessed unprecedented growth, inspiring innovations such as Social IoT (SIoT), Industrial IoT, and IoT applications in healthcare.

IoT empowers heterogeneous devices to interact and cooperate while providing or consuming services. Nevertheless, this cooperative framework raises trust-related concerns, necessitating a decentralized, mobile, cost-efficient, low-latency, lightweight, and scalable

trust management model. The fusion of social networks with IoT has led to the emergence of SIoT (Chung and Liang, 2020), distinguished by its diversity of hardware and software components and varied architectural frameworks. Within SIoT, these disparate devices collaborate to accomplish common objectives (Afzal *et al*., 2019). SIoT is a broad paradigm encompassing interactions between individuals, devices, and a combination of both (Lakshmanaprabu *et al*., 2019). It also facilitates the effective discovery of geographically dispersed devices (Khan *et al*., 2021).

SIoT integrates peer-to-peer networking with social relationships among autonomous systems, where nodes serve as either Service Providers (SPs) or Service Consumers (SCs). Each node within the network is more likely to receive appropriate responses to its requests than standalone devices (Lin and Dong, 2018; Amin and Oun Hwang, 2022). The fundamental aim of SIoT is to detach devices from direct human oversight, enabling them to self-organize and share computational resources, data, and functionalities. Each node determines the nature of its relationships with others (Amin *et al*., 2022). In SIoT, relationships can occur between users and devices or exclusively among devices, depending on their respective affiliations. These relationships play a pivotal role in inter-SIoT communication and application development (Hosseinzadeh *et al*., 2024). When devices recognize their inherent social behavior, they begin to establish connections.

Social links or connections among IoT devices are formed based on factors such as specifications, activities, usage patterns or behaviors, installed applications, and the services they offer (Smart *et al*., 2019; Ahmed *et al*., 2019). This social relation can be classified as Manufacture-object, Co-location, Co-work, IoT objects, and Social-object social relationship. The Manufacture-object social relationship refers to IoT devices belonging to the same manufacturer and same batch of manufacturing (Chung and Liang, 2020; Ahmed *et al*., 2019), the IoT objects located in the same work location, city are referred to as co-location social relationship and if IoT cooperates with other IoT devices to accomplish the given task then such relationship is referred as Co-work social relationship. Further, a group of devices belonging to the same owner is referred to as object-ownership social relationship. Moreover, IoT devices contact other devices regularly or irregularly for some reasons.

These social relationships are essential for device interactions and data exchange among the devices. But, peer-to-peer interaction, social interaction, and relationships amongst a set of autonomous systems may cause intrinsic or extrinsic attacks, where devices act as service/access providers (AP/SPs) can exploit or generate spurious attacks on service consumer or requesters/ consumers (ARs or SRs or SCs). Every IoT device or node gets or obtains valid results or services or responses to its demand or requests. Therefore, it is important to define trust and trustworthiness among the devices to provide service or access the services.

The trust is referred to as a deep dependability on other device, confidence on other devices, the device's honesty, the device's sincerity in its functions, justice in device functionality, and confidence in another device to perform a function or transaction. Trust is also referred to as commitment, agreed upon established laws, principles, norms, expectations, (Becherer *et al*., 2024; Sagar *et al*., 2024). The term 'trustworthiness' is represented in terms of the social relationship among the devices or entities. Confidence in other honesty or trust. Trustworthiness of IoT objects depends on the characteristic or attributes of the trustee device (Sagar *et al*., 2024). In SIoT, trust and security are important for IoT device data exchange and interaction.

In SIoT, trust is a procedure that service requester or trustor gives or assign responsibilities or tasks to the service provider or trustee to perform a specified task or functions. The result or output of the trustees or service provider can be used to achieve their objectives. The service requester or trustor examines and evaluates the competence and willingness of service provider or trustor. The service requester trustor or trustee or service provider evaluates the trustworthiness of each other's. The trustor examines and evaluates the trustee's competence, willingness, and trust.

To enhance the trustworthiness of intelligent SIoT objects, trust management has become a fundamental requirement for establishing a reliable and secure network of smart objects. Effective trust management is crucial for improving the security and reliability of cyber-physical systems. Artificial Intelligence (AI) has been adopted to enhance credibility scores in trust management. However, addressing the existing challenges in trust management remains a significant necessity.

The abundance of available services necessitates intelligent and trust-aware recommendations to facilitate smooth navigation and enhance user satisfaction. Service recommendation systems within the SIoT framework play a crucial role in addressing this challenge by providing intelligent recommendations that consider user preferences, social connections, and contextual needs (Lin and Dong, 2017; Amin *et al*., 2022; Hosseinzadeh *et al*., 2024).

This research investigates how explicit and implicit trust and social relationships among the device influence on recommending trustworthy service providers in the SIoT environment. Additionally, it investigates the impact of cooperation between a service requestor and a service provider. Furthermore, this research examines the

contribution of latent pattern/features in process of computing trustworthy service provider and the effectiveness of recommendation systems in the SIoT environment.

Related Work and State-of-the-Art

Related Work

Internet-of-Things (IoT) and SIoT produce huge among of data and are accessible on Internet. It is important to use research paradigms or intelligent mechanism to extract knowledge that meets the requirements of end-users from enormous data. The intelligence mechanisms that extract useful information from enormous data can recommend suitable service or products to users. Further, useful data generated by IoT devices or objects are useful in designing solutions and recommending services.

It is important to examine trust of service provider before recommending the service provider for a particular service delegation. In the academic and research community, it is important to improve accuracy of a service recommendation. A collective filtering service recommendation system incorporating trust of reference user or recommender, local and social influence or authority of recommender or reference users based his./her social network (Lu *et al*., 2020). Similarly, Chen *et al*. (2016) proposed a collaborative/collective filtering-based method that consider the rating and ranking of service provider. Service recommendation-based rating and ranking service provider may leads to recommendation of the misbehaving service provider. It is necessary to avoid the misbehaving service provider (Aalibagi *et al*., 2022), the misbehaving or malicious service provider interrupt the core functionality of SIoT by damaging the reputation of legitimate and well-behaved devices or randomly increasing the score of trustworthiness of misbehaving or malicious service providers (Aalibagi *et al*., 2022). The trust model must predict the efficient, competent, and reliable service provider for a particular service requester/trustor. Trust model must assist SIoT device to avoid the risk of vulnerability to malicious service provider. Aalibagi *et al*. (2022) developed trust model based service providers' centrality and similarity to find trustable service providers.

Wei *et al*. (2022) proposed a reciprocal trust model and examined the characteristics of SIoT tasks or services to enhance the feasibility of trust models. These models are constructed based on the utility of the service petitioner or assistance requester, as well as opinion- and evidence-based trust quantification. In SIoT, service is recommended using social relation between IoT devices and data generated by various IoT devices. Bouazza *et al*. (2022) used data generated by IoT devices and applied filtering and ontology to recommend the trustworthy service provider to users.

The trust or trustworthiness of a service provider directly influences the Service Requester's (SR's) critical decisions regarding entrusting the provider with a particular service. Trust models in the literature consider the requirements of the service petitioner or assistance requester to evaluate the trustworthiness of service providers. However, the correlation between trust models and service delegation remains unclear. It is challenging to trace and access services from quality and credible service providers in large-scale social networks. There are implicit constraints and inherent characteristics of devices that influence the reliability and security issues in SIoT networks. Chen *et al*. (2016) evaluated the trustworthiness of service providers based on the status of energy, past performance, and social relationships among the IoT objects. Similarly, Wei *et al*. (2021) evaluated the trustworthiness of service providers based on competition, willingness, and social relationships among the IoT devices. These trust models are robust against malicious attacks in dynamic real-time SIoT environments. In contrast, service providers can be selected based on service requesters' characteristics, service interests, previously used services, service requester social intimacy, and interaction context among other devices (Pashaei Barbin *et al*., 2020; Wang *et al*., 2015). Another way of computing the trust of service providers is through IoT devices deployed by the government and trusted institutions; these sensor devices can capture surrounding sensitive data as sensitive data standards. With the help of sensitive data standards, the trustworthiness of service or data providers can be derived (Li *et al*., 2021).

SIoT symbolizes the possible social relationship among devices in the network and mirrors trustworthiness, specific features, compatibility, and so on. The trustworthiness of service providers is based on IoT devices' features and social relationships among the devices (Hamrouni *et al*., 2022; Ben Sada *et al*., 2023). The service recommendation techniques in the literature extract and adopt of social connection among social users, and devices and ignore contextual information of reviews on service providers. Ben Sada *et al*. (2023); Lye *et al*. (2020); Kalaï *et al*. (2018) integrated latent features of SIOT device, a device to device interaction, and social relationship among the social users, social users' credits and reviews from trusted surroundings friends, device, reviews from domain experts to find trustworthiness of service provider.

Graph-based Neural Networks (GNN) can portray devices' characteristics and their social connections among the devices and form a group of context-aware communities (Hamrouni *et al*., 2022). The utilization of user feedback and reviews is becoming the recent trend in service delegation recommendations. However, with a large number of services, service providers, and users, some discordant and noisy reviews or information or fake feedback reviews for malicious intentions may sneak into the service recommendation mechanism. Apparently, fake and noisy feedback certainly harms the trustworthy quantification of service providers. Thus, such fake and noisy feedback should be differentiated and discarded (Deng *et al*., 2014). The rise of fake or legitimate tendered services led to complexity while selecting service providers, customizing, and filtering services. The process of sudden rise of fake or legitimate tendered service is referred to as service explosion. Identifying suitable service provides that matches the requirements of the service requester is a tedious task. To mitigate such a problem, a query-based service provider search model is designed in Amin and Oun Hwang (2022), the service provider search model uses the local navigability concept.

State-of-the-Art

Finding a service provider who fits the service requester's requirements can be tedious. The literature proposes collaborative filtering and variants of collaborative filtering-based service recommendation methods (Ayub *et al*., 2020; Yan *et al*., 2021). A recommendation system in Yan *et al*. (2021) integrate collaborative filtering with the LSH forest method to find grad of service. However, these methods consider the static service requester's needs. Over time, the needs of the service requester certainly change, and service requesters' tastes change.

The time-aware service recommendation system integrates the service requester's mutable needs and the service provider's credibility. Credibility is a direct proposition to inferred direct and indirect trust relationships, and it mitigates data sparsity issues (Ngaffo *et al*., 2021). A method in Ayub *et al*. (2020) creates a service requester profile based on both explicit and implicit trust and the service requesters' priority and similarity for the particular service provider recommendations. Similarly, Kang *et al*. (2017) generated the most relevant set of service provider groups based on social connection similarity of service requirement. However, these methods suffer from sparseness, scalability, and cold start problems. Shokeen and Rana (2021) proposed semantic-based service provider recommendation method to mitigate cold-start problem.

The trust score of service providers is computed based on social relationships and ratings. In addition to this, prioritised semantic, likeminded friends connected to other semantic, likeminded friend's feedback on social networks are considered in computing trustworthiness. The trusted service provider can act maliciously to deny the actual service and disturb the network services. Thus, the service provider's trust is quantified using transaction time, availability, and execution time (Aslam *et al*., 2020). Similarly, the best service provider can be identified by obtaining service requesters' predilection, capturing the frequency of service requester's usage and likeness of a service provider, and obtaining devices' social relationships (Rajendran and Jebakumar, 2021; Cheng *et al*., 2019).

Hybrid Feature-Trust Based Recommender System

The hybrid feature-trust based recommender system in the Social Internet of Things (SIoT) environment is designed to optimize service recommendations by integrating both trust and latent feature modelling. It integrates diverse methodologies to enhance its functionality, addressing the complexities of service recommendation systems within the SIoT context. The system combines explicit and implicit trust metrics to create an effective and adaptable service recommendation framework.

Trust-Rank Based Model

The Trust-rank based model in the SIoT environment is designed to create an effective and adaptable service recommendation system by incorporating both implicit ($Tr_{AB}^{implicit}$) and explicit ($Tr_{AB}^{explicit}$) trust metrics. It evaluates the social trust rank of devices, providing valuable insights into trust relationships. This model integrates these trust metrics into the matrix factorization process to enhance personalized service recommendations and mitigate service confusion among devices. The approach balances the influence of explicit and implicit trust using a weighting factor.

Explicit Trust Metric

Basically explicit trust metric T in SIoT evaluates trust based on direct interactions and observable actions like collaborations and feedback. It uses clear evidence within the network for trust measurement. The key factors include.

Interaction Factor (IF): The Interaction Factor (IF_{ij}) is a component of the explicit trust metric used to evaluate trust between node i and node j in the Social Internet of Things (SIoT) environment. It is calculated based on the interactions between nodes, specifically focusing on the feedback and transactional factors associated with these. The Interaction Factor (IF_{ij}) measures interactions the

quality of direct interactions between two devices based on whether transactions are relevant or non-relevant and whether the feedback is positive or negative:

$$IF_{ij} = \frac{\sum_{i=1}^{ton^{tt}} f_{ij}^{l} tf_{ij}^{l}}{\sum_{i=1}^{ton^{tt}} f_{i}^{l} j} \quad (1)$$

Where, (IF_{ij}) interaction factor between device I (trustor) and device j (trustee), $tt\ f_{ij} = 1$: Transaction is relevant, $tt\ f_{ij} = 0$: Transaction is irrelevant, $t\ f_{ij} = 1$: Feedback is satisfactory, $t\ f_{ij} = 0$: Feedback is unsatisfactory.

Friendship Similarity (FS): Friendship Similarity (FS_{ij}) measures the importance of an object among other objects in terms of their interactions, reflecting their social relationships in a specific context. It is determined by the overlap of friends between two nodes, calculated as the ratio of the intersection of their friend sets to the size of one of the friend sets minus one. It Measures the overlap in the social networks of two devices, reflecting the strength of their social relationship. Higher values of FS_{ij} indicate stronger social ties, leading to greater trustworthiness in the SIoT environment:

$$FS(i,j) = \frac{\left|FS_i \cap FS_j\right|}{\left|FS_j\right| - 1} \quad (2)$$

Where: FS (i, j): Friendship similarity between devices i and j, FS_i: Set of friends of device i, FS_j:Set of friends of device j, $|FS_i \cap FS_j|$: Number of common friends between i and j (intersection of FS_i and FS_j). $|FS_i|$: Total number of friends of device i (cardinality of FS_i). While in denominator ($|FS_i| - 1$), is to normalize the similarity score by considering Fi, it excludes i itself. It ensures that similarity is relative to the size of I's friendship network.

Community-of-Interest (CoI): Community-of-Interest (CoI (i, j)) quantifies the similarity between nodes concerning their participation in communities or groups of social interest. Nodes with high CoI are more likely to interact and build trustworthy relationships:

$$Col(i,j) = \frac{\left|C_i \cap C_j\right|}{\left|C_i\right|} \quad (3)$$

Where: CoI (i, j) : Community of Interest trust score between devices i and j, C_i : Set of communities or interest groups that device i belongs to, C_j : Set of communities or interest groups that device j belongs to, $|C_i \cap C_j|$: Number of shared communities between i and j, $|C_i|$: Total number of communities that device i belongs to the value of Community Of Interest factor ranges between 0-1, CoI (i, j) = 1 : Device i and j share all communities, and CoI (i, j) = 0 : Device i and j share no communities.

Cooperativeness (CoP): Cooperativeness (CoP (i, j)) assesses the level of social cooperation between a trustee and a trustor. It measures the balance in their interactions, and the CoP-based trust is calculated using the entropy function as follows:

$$CoP(i,j) = -Tp\log(TP) - (1-Tp)\log(1-Tp) \quad (4)$$

Where: CoP (i, j): Cooperativeness trust score between devices i (trustor) and j (trustee), $T\ p$: Fraction of messages or interactions initiated by device i compared to the total interactions between i (trustor) and j (trustee). This equation uses the entropy function to quantify the cooperativeness between nodes i and j, where $T\ p$ represents the probability of cooperation between the nodes. The explicit trust metric is composed of all four essential factors so while calculating the explicit trust metric is the sum of all the essential factors:

$$Tr_{AB}^{explicit} = w_1 IF(i,j) + w_2 FS(i,j) + w_3 Col(i,j) + w_4 Cop(i,j) \quad (5)$$

Where: IF (i, j): Interaction factor, FS (i, j): Friendship similarity, CoI (i, j): Community-of-interest similarity, CoP (i, j): Cooperativeness trust score., and w_1, w_2, w_3, w_4: Weights for each metric.

Implicit Trust Metric

The Implicit Trust Metric $Tr_{AB}^{implicit}$ in the SIoT environment offers insights into the reputation of SIoT nodes by assessing trustworthiness through implicit factors such as behavior, shared interests, and history of cooperation. It complements the Explicit Trust Metric by providing a broader view of trust relationships that are not solely based on direct interactions.

Hybrid Trust Model

The hybrid trust model in the SIoT environment is designed to capture the complexities of direct and indirect trust relationships within the SIoT device network. It incorporates both implicit and explicit trust metrics to create an effective and adaptable service recommendation system. This hybrid model aims to evaluate the reliability of a node by considering factors beyond direct interactions, Influencing the dynamics of interactions and recommendations between

interconnected devices. The trust score between device *A* and device *B*, can be evaluated as:

$$Tr_{AB} = \beta Tr_{AB}^{explicit} + (1-\beta) Tr_{AB}^{implicit} \quad (6)$$

Where: Tr_{AB}: Final trust score between device *A* (trustor) and *B* (trustee), $Tr_{AB}^{explicit}$: Explicit trust score based on direct interactions, $Tr_{AB}^{implicit}$: Implicit trust score based on indirect factors (e.g., reputation, social connections), and β: Weighting parameter β ranges between 0 to 1. Therefore, from Equation 1 to 6, the final expression is:

$$Tr(i,j) = \beta w_1 \frac{\sum_i = 1 ton^{tt} f_{ij}^{l} t\, f_i^{l}}{\sum_i = 1 ton^{tt} f_{ij}^{l}} + \beta w_2 \frac{\left|FS_i \cap FS_j\right|}{\left|FS_i\right| - 1} + \beta w_3 \frac{\left|C_i \cap C_j\right|}{\left|C_i\right|} + \beta w_4 (-T\, p \log(TP) - (1-Tp)\log(1-Tp)) + (1-\beta) Tr_{AB}^{i} mplicit \quad (7)$$

Latent Feature Modeling

In this subsection, we introduce a method of matrix factorization that combines the Bayesian interface and Gaussian priors for latent feature capturing. In context-based service recommendation for SIoT combines the framework shows the comprehensive model solution related to service rating and latent features. To get the probability of service rating and latent features, and their unpredictability to combines the matrix factorization method with the Bayesian interface and Gaussian priors. Using the matrix factorization method allows us to capture the latent features related to services and devices.

Device-Service Matrix Factorization

The device-service matrix factorization method plays a very important role in latent feature capture related to devices and services. This method is related when considering the device-service matrix, where it's having *m* devices, *n* services, and values of the rating in the range between 0 and 1. To the get modelling process, map the integer rating from 1 to Y_{max} between range from 0 to 1 by using the function $f(x) = {}_{Y}max^{x-\_a}{}_1$. The separate ratings Y_{ij} means judgment of the device *i* for the service *j*. To capture the inherent structure let's introduce $Z\varepsilon Y^{lxn}$ and $U\varepsilon Y^{lxm}$, service feature and latent device matrices respectively. Here Z_j service-specific and U_i device-specific latent feature vectors.

Conditional Distribution and Trust Propagation

In generating trust and latent features, the key element distributed the observed ratings conditionality. Let *C* be the observed ratings matrix, *U* represent the feature latent device matrix, *Z* represent the feature latent service matrix, and σ_Y^2 represent unpredictability related to ratings. Then the conditional distribution is calculated as follows:

$$p(C \mid U, Z, \sigma_y^2) = \prod_i = 1 ton \prod_j = 1 ton \eta(qij \mid g(U_i^T Z_j), \sigma_y{}^2) I_{ij}^{Y} \quad (8)$$

Here, q_{ij} represents the approximated rating for the communication between the device *i* and the service *j*, The indicator function I_{ij}^{Y} if it is 1 then the rated service *j* to the device *i*, and otherwise 0. η is the normal distribution detect the unpredictability in related ratings. The product of all communications guarantee a joint distribution above the all recognized rating matrix.

Equation 8 indicates the assimilation of matrix factorization, where latent features *Zj* and *Ui* contribute to guessing *qij* and trust-related inference, as observe different ratings by trust score identical to device-service communication. In comparing Bayesian inference with conditional distribution, the conditional distribution plays an important role in modelling the observed rating.

Gaussian Priors

The Gaussian priors play an important role in modelling the distribution of service features and latent device vectors, in suggested framework for trust-related service recommendation in SIoT. These priors are used to regulate the latent features to capture inherent uncertainties, and giving the Bayesian foundation for the recommendation model. For latent device feature matrix UεYlxm place zero-mean spherical Gaussian priors on user and feature vectors:

$$p(U \mid \sigma_U^2) = \prod_i = 1 tom \eta = (U_i \mid 0, \sigma_U{}^2 I) \quad (9)$$

Equation 9 indicate that Ui each row vector in the latent device feature matrix following the Gaussian distribution with zero-mean and variance σU2I. The σU2 control the distribution spreading and conditioning the degree of regulations which to be applied to latent device features. As same way, the latent service feature matrix ZεYlxn the Gaussian priors are:

$$p(Z \mid \sigma_Z^2) = \prod_j = 1 tom \eta = (Z_i \mid 0, \sigma_U{}^2 I) \quad (10)$$

Equation 10 indicate that Z_j each column vector in the latent service feature matrix following the Gaussian distribution with zero-mean and variance $\sigma_Z{}^2 I$. Comparing the Gaussian priors concerning Bayesian it maintains the balance of the prior knowledge, and

observed data, and contributing to a more powerful and understandable trust aware service recommendation model in SIoT.

Bayesian Inference

In SIoT, the context based-related service recommendation, the Bayesian inference is an essential method to model the probability of service ratings, latent features, and their uncertainties. The aforementioned integrated method combines the matrix factorization along with Gaussian priors. Indicating Bayesian Inference, the joint probability model is as follows:

$$\begin{aligned} p(U,Z\left|Y,\sigma_y^{\ 2},\sigma_U^2,\sigma_Z^2\right.) &= P(Y\left|U,Z,\sigma_Y^2\right.) \\ &\times P(U\left|\sigma_U^2\right.)\, p(Z\left|\sigma_Z^2\right.) \\ \times\prod_i = 1tom\prod_j = 1tom\eta(r_{ij}\left|g(U_i^t Z_j),\sigma_Y^2\right.)I_{ij}^Y \\ \times\prod_i = 1tom\eta(U_1\left|0\right.)\left|\sigma_Z^2 I\right.) \\ \times\prod_i = 1tom\eta(Z_j\left|0\right.)\left|\sigma_Z^2 I\right.) \end{aligned} \tag{11}$$

In Equation 11, U and Z are noted as the latent device matrices and service feature matrices, rating matrix (observed). σ_Y^2 noise rating variance, σ_U^2 device features variance on Gaussian priors, and σ_Z^2 service features variance on Gaussian priors. The term $p(Y|U,Z,\sigma_Y^2)$ indicates conditional distribution related to the observed ratings, gathering predicted ratings $g(U_i^T Z_j)$ and the noise rating variance σ_Y^2 The product of i and j with indicator function I_{ij}^Y that ensures the evaluation of the distribution one and only for observed ratings. The $p(U|\sigma_U^2)$ and $p(Z|\sigma_Z^2)$ Gaussian priors enforce the regulations on the latent feature matrices, guide the learning process and contribute to constant and understandable recommendation model. Through the Bayesian approach, the suggested model gets a balance between the prior knowledge, observed data, understanding of latent features, service ratings, and their uncertainties in SIoT.

Figure 1 shows the step by step recommendation process. First, based on the historical interaction between services and devices, the device-service rating matrix is constructed. Subsequently, using comprehensive trust method (Both implicit and explicit trust metrics) to calculate the trust value of each device. Following the process of trust assessment, matrix factorization, combine with Gaussian priors and Bayesian inference, this process is applied to capture the latent features related to services and devices. This process deteriorating the device-service rating into latent features matrices. The embodiment of Bayesian inference giving a feasible framework for make the predictions, then Gaussian priors assign rules to avoid overfitting in sparse data. The trust value based on real-time interactions between the nodes ensures the trust values related with change the trust dynamic in SIoT. Finally, device-service rating matrix that shows latent features and their uncertainties the trust-based service recommendation method.

Materials and Methods

In this section, we discuss the methodology of the proposed work includes a description of regard dataset and method of integrating the proposed trust model technique. In the initial phase, the proposed service recommendation integrated the trust model, significantly recognise the trust that contact latent features that will be capture by matrix factorization. Before dissipation device-service matrix the trust score as additional factors. In process of feature extraction, the model is trained to assess the trustworthy devices. This methodology is constant with direct trust shape the latent features from matrix factorization.

Dataset

The proposed model using the FilmTrust dataset, in this dataset, mainly focus on ratings, it has trust values between users. The dataset having valuable information related to users' trust and un-trust. Then users can assess the best-rated reviews given by other users. The dataset discussed in Guo *et al*. (2013), and key item and its value are shown in Table 2. The 23,714 users and item pool of 300,014 items with 914,414 ratings, it's an average of 42.14 ratings per user. The dataset having 35,631 true relationships, includes 17,514 users who trust others 17,814 users who are trusted. Then the average rating in dataset is 3.99.

Table 1: The FilmTrust dataset

Item	Value
Users	1,508
Items	2,071l
Ratings	914,414
Range of ratings	[0.5- 4.0]
Trusters	709
Trustees	814
Trust relations	35,631
Density	1.41%

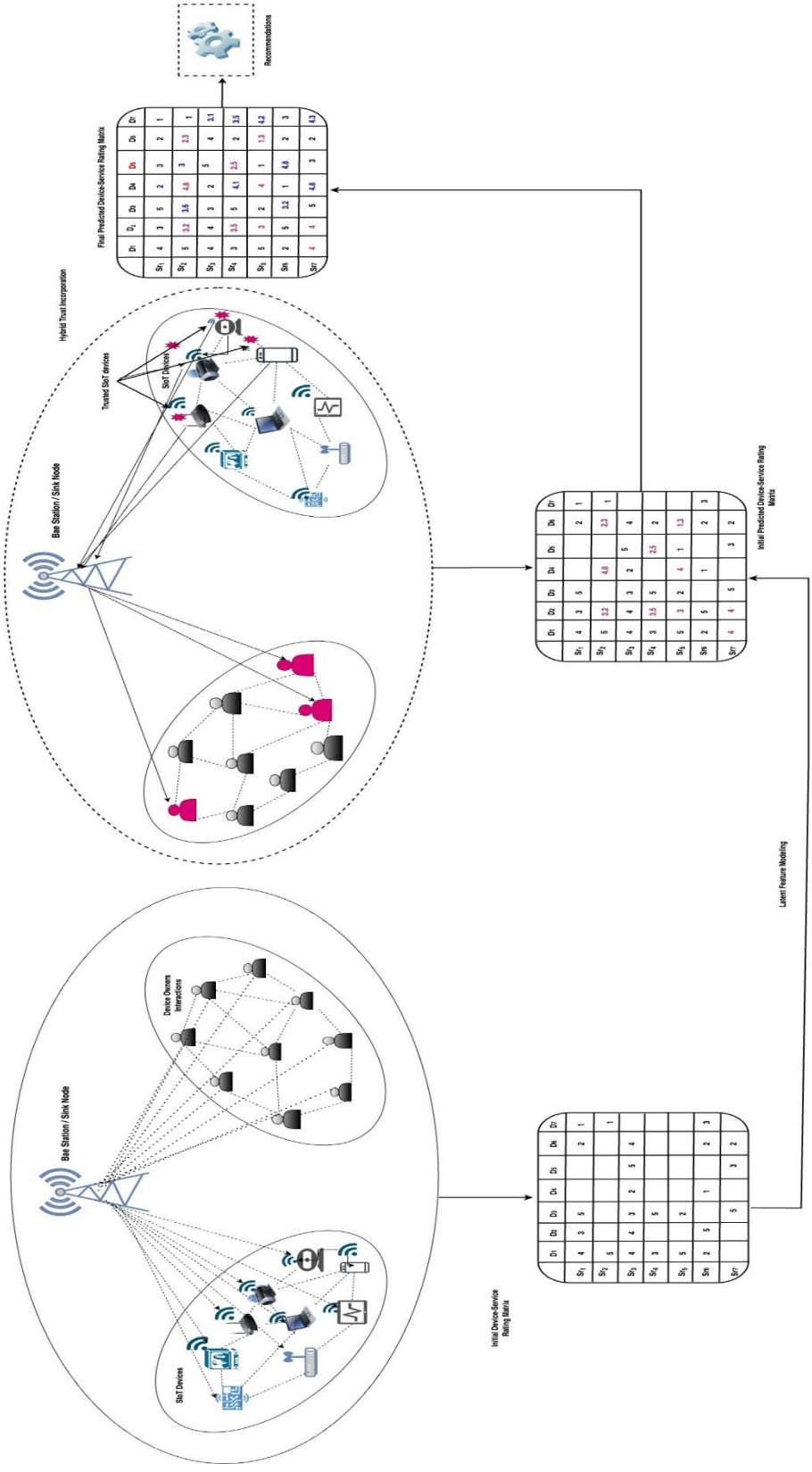

Fig. 1: Process of recommendation

Integration Model of Trust

Mutual Trust Computation in the SIoT Environment

In the dynamic nature of the SIoT, the trustee devices are the main concept, that differentiate SIoT from social networks and static IoT networks. Like IoT nature, SIoT introduces various aspect of trustee-influence (both explicit and implicit) trust factors. The explicit trust originates from predicted relationships, such as Co-location, Co-ownership, parental object relationships, and social object relationships. The devices, similar to reputed friends, ordinary users, and ordinary in social networks, assume the main role of trusted friends. Our proposed model not only include predicted trust it also includes actual interaction between the devices. These interactions have exchanged the data, enveloping both send and receive actions. The fundamental of the proposed method is to calculate the bilateral trust among the nodes. Figure 2 shows the bilateral trust computation includes a web of trust in SIoT nature. Figure 2 highlighting trustee devices and interconnected relationships. It shows the interactions in real-time and explicit relationships, our method offers a comprehensive understanding of the complex network of trustee devices of interdependent devices.

Trust Model With Comprehensive Integration

In this subsection, we demonstrate the integration of trust model into the overall scheme of proposed service recommendation process. This enclose many components, contains the manipulation of both explicit trust and implicit trust, a fusion of trust related metrics collected from the dataset, and the integration of matrix factorization method into the trust scores. We apply the algorithms to calculate the scores of both trusts (Explicit and Implicit) for devices belonging to SIoT network. The Explicit Trust Calculation (ETC) covers interactions, direct observations, and feedback, while Implicit Trust Calculation (ITC) covers collected interest, behavior, and previous history of the node. The metrics related to trust getting from the dataset, we taking features such as Cooperativeness (CoP), Community-of-Interest (CoI), Interaction Factor (IF), and Friendship Similarity (FS). All these metrics get the appearance of trust and communication between devices. The trust (explicit and implicit) scores play an important role in our matrix factorization method. Before deteriorating device-service matrix, we cover trust scores as extra factor. This plan integration technique allows to assigning of a weight to the trustworthy devices in the features extraction method, calculating the trust on latent features. This method gives adapting recommendations depends on real-time interaction. To confidants, the model is robustness and anticipate overfitting, Gaussian priors applied to vectors of service and device feature. The priors especially relating to trust and regulating the learning process. Therefore, our model having the advantage Bayesian inference model to joint probability of latent features, rating relate to services, and uncertainties. This integration method gives a trust relation information from priors and observed ratings. The graphical representation of the trust model is shown in Figure 2.

Scenario Case: Addressing Service Confusion Selection in Smart Office SIoT

In SIoT many devices are interconnected to each other SIoT relationships, as like parental, co-work, co-location, or ownership relationships. In figure 3, three SIoT device D1, D3, and D5 play important role in creating smart living experience.

The trust metrics (implicit/explicit) related to these devices becomes crucial in solving the problem. Implicit trust is based on device behaviours and interactions between the devices, while then explicit trust is based on direct and observable. The devices have a device-service interconnected matrix, scaling from 0 to 5, given by devices of different smart office services. Installing new devices in SIoT environment the big challenge of service confusion. The new devices added D6, D7, and D8 utilization of speciated services.

The proposed method using a trust weighting sum method with latent feature method, which cover hybrid matrix factorization, Bayesian Inference, and Gaussian priors, is planned to un-cover latent features related to services and devices. The trustee devices to boost service recommendation of the devices D6, D7, and D8. Therefore, thinking about the problem of the proposed method, trust metrics are guide by the matrix factorization, given the related recommendations to confused devices D6, D7, and D8. Figure 3 shows the service recommendation in smart office. The devices having in red play an important role in manage the different smart office functionalities and the red devices also gives the service recommendation by exchanging and updating newly added devices, showing their importance related to trust in the SIoT network.

The Limitations of the Proposed Methods

The proposed trust model depends on past transaction data that may not be available for new or non-interactive devices. Data privacy breaches may arise while analyzing past interaction data and social relationships of devices. The trust model performance may change depending on the dataset quality and the number of samples in the dataset used for training and evaluation. The proposed trust model performance may change if SIoT has an extremely dynamic device and complexity.

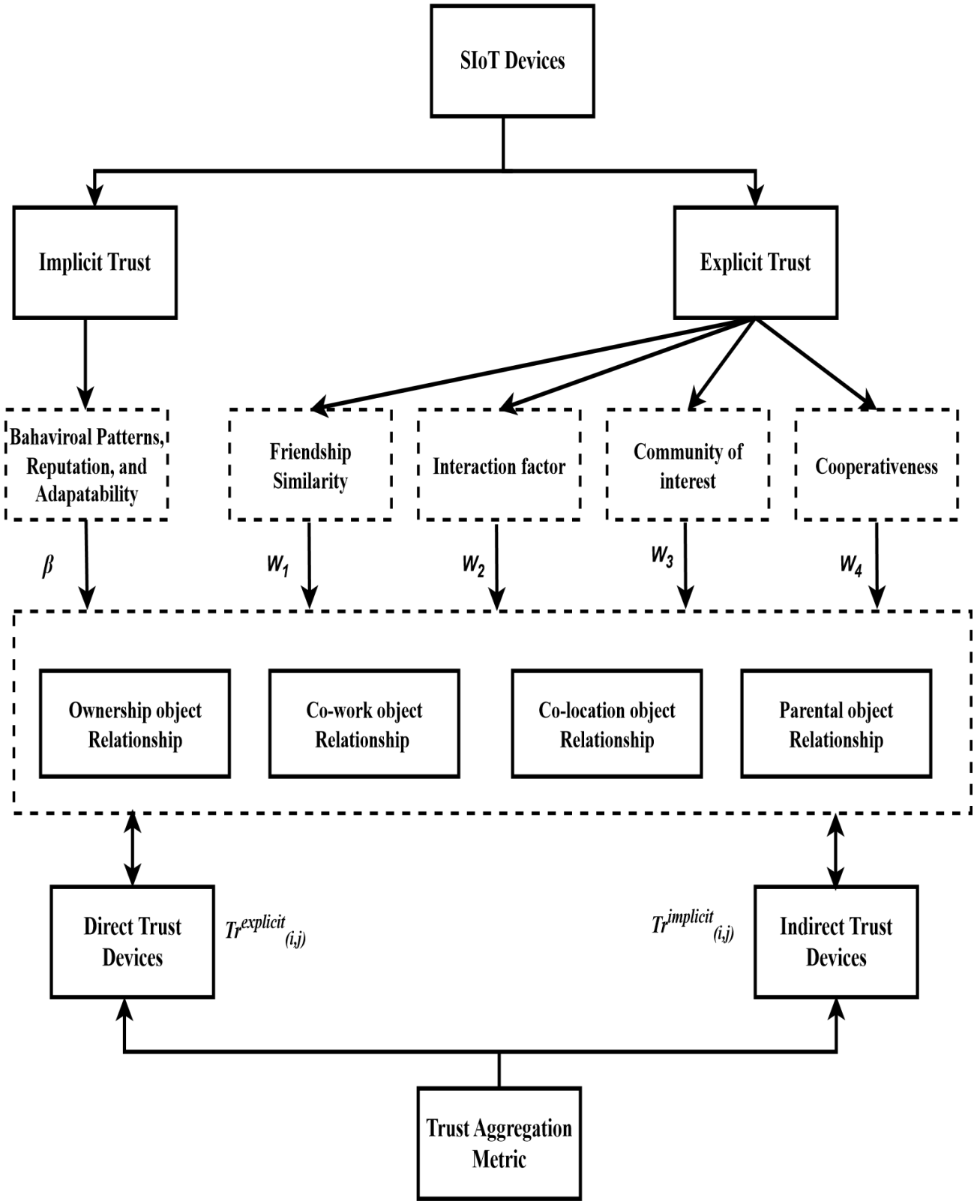

Fig. 2: Trust model of SIoT devices

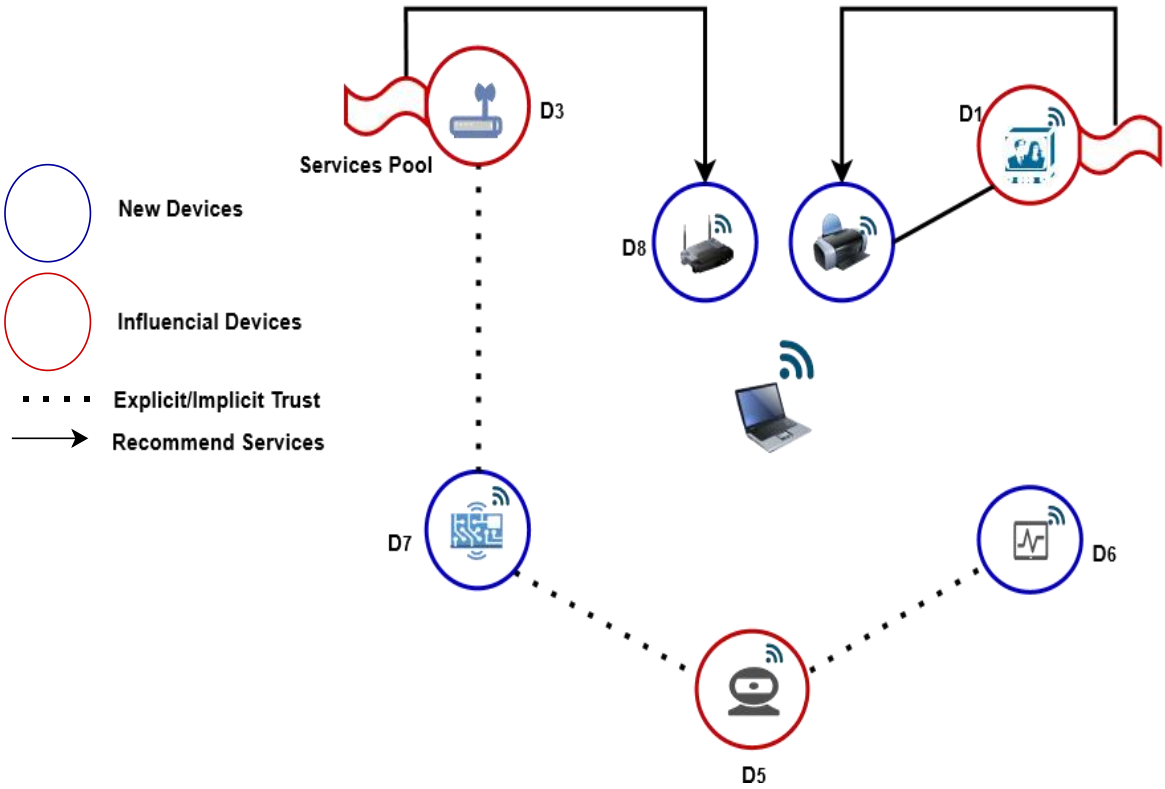

Fig. 3: Scenario case of SIoT service recommendation in smart office environment

Evaluation

Metrics

To conduct an overall evaluation of proposed model, we conduct a fivefold cross verification approach. Within every fold, dividing dataset into 20% for testing and 80% for training. The evaluation of the metrics given in our evaluation work are NDSG, MAE and RMSE. Both the MAE and RMSE measuring the correlation among predictions and ratings. Then both DCG and NDCG use powerful evaluation of framework effectiveness, in recommendations systems to assessing the original raked list of the recommendations system by thinking recommended item's position in list and their relevance. These metrics are explained as follows:

Mean Absolute Error (MAE): Calculate the average magnitude of errors between the actual ratings and predicted ratings. To get the complete accuracy of recommendations the MAE metric is used. Then MAE is calculated as:

$$MAE = \frac{1}{n}\sum_{i=1ton}\left|Ar_i - A_i\right| \tag{12}$$

Root Mean Squared Error (RMSE): As with MAE, to get the accuracy of recommendations by calculating square root of the average square difference between actual ratings and predicted ratings. As compare to MAE this metric is dismissed as the larger errors. Then RMSE is calculated as:

$$RMSE = \sqrt{\frac{\sum_{1ton}(\left|Ar_i - A_i\right|)}{n}} \tag{13}$$

Normalized Discounted Cumulative Gain (NDCG): It's the most essential metrics in the recommendation system, by assess the quality of the recommended items by thinking rank position and relevance of the recommendations items. The *NDCG* is defined as:

$$NDCG@k = \frac{DCG@k}{\left|IDCG@k\right|} \tag{14}$$

Where *NDCG@k* represent the *NDCG* value at the position *k*, *DCG@k* denotes the *DCG* at the position *k*, and *IDCG@k* denotes the IDCG at the position *k*. To calculate the *DCG@k* the sum the grading relevance of the recommendation item up to the position *k*. The *DCG@k* is calculated as:

$$DCG@k = \sum_{i=1tok}\frac{\left|rell_i\right|}{\log_2(i+1)} \tag{15}$$

Where $rell_i$ = Graded relevance of item at the position *i*. The IDCG@k represents the constant DCG value at the

position *k*, getting by sorting the relevance value in descending order. Then *NDCG@k* ranges between 0 and 1. The value 1 means high quality recommendations its having high relevance and good rank items in the list and the value 0 means low quality recommendation its having low relevance and bad rank items in list.

Recommendation Methods

To address the important challenges of social networks in dynamic nature, we discuss in this section four different recommendation methods. The first approach, TSSR (Shokeen and Rana, 2021) approach discuss the semantic social recommendation based on semantic technique. To calculate semantic and trusted friends depending on direct and indirect friend relations. The second method, RSCF (Son *et al*., 2020) method discuss the context-aware trust recommendation system of SIoT and presents a resilient method that advantage asymmetrical implicit trust network and propagation of the trust. The third method, SoReg (Ma *et al*., 2008) method discuss the important challenges of the popular recommendation system by collecting information about social networks by using social regulations in terms of matrix factorization. Finally, SocialMF (Jamali and Ester, 2010) method discuss the matrix factorization method elaborate with propagation of the trust.

Parameter Tuning

Developing the performance of our service recommendation model to correctly adjust the important parameter in proposed model. The parameters are trust weight β, noise level σ, and the conditionality d. The β, assumes the important role, in finding trust values identified by SIoT relationships. A higher the value of β, indicates that own trust or trust in particular relationships (e.g PoR, WoR), while the lower value of β indicates preference individually. In proposed model experiments, explores the different values of the β these values strike on recommendation performance. To get the optimal results when set $\beta = 0.5$ for 95 and 85% trained data. We carefully assign β parameter with recommendation methods. We fine-tune the value of the priors for service variables and device, set $k = 5$ for Gaussian priors. Finally, the noise level σ determined the anxiety in the observed ratings. We setting σ to 0.4, to ensure a correct data distribution representation for Robust Bayesian inference. This parameter tuning method collectively effectiveness and reliability of the proposed model.

Results and Discussion

This section mention the results of proposed method based on RMSE and MAE matrices and compares them with other methods. Finding the performance of the recommendations system in SIoT. The matrices such as RMSE and MAE get the different roles. Due to its quadratic nature, the RMSE get larger error than smaller ones because of this RMSE assign higher deviations between actual and predicted values when the deviations are higher-order. On the other side, the MAE treats all errors equal, providing differences between actual values and predicted values. Figures 4 and 5 shows the MAE and RMSE values respectively.

We calculated the performance of two dimensionality values of different iterations. That are d = 5 and d-10. Figures 4(a) and 4(b) shows the performance of the proposed model to the dimensions d = 5 and d = 10, depending on MAE values upon different iterations. The proposed model shows the best performance throughout the calculation. In the first iteration, as shown in Figure 4(a), the proposed method having the lower MAE values compare to different methods, it shows that its having high accurate predictions. How- ever, the SoReg gets the higher values of 0.98 of MAE, implying the prediction accuracy is lower compared to another method. The SoReg only decides on user rating matrix items for the matrix factorization and finding the user's own tastes that making recommendations, discard the remaining influencing factors. However, then d = 10, as depicted in Figure 4(b), in initial stage equal performance in all methods. The iteration progressed, to values for two dimensionality values, and the proposed method kept its competitive edge, Figure 4(a-b) shows the decreasing values of the MAE with respect to competing methods. The proposed method compared with TSSR, it's an excellent and modern approach among the baseline methods. In every iteration, TSSR consistently achieves higher MAE values than the proposed method. The proposed method showing its effectiveness in predominant the more advance existing method. This constant improvement in accuracy up with iterations that focus the effectiveness of the proposed method in advantages social interaction and information about trust for elaborate the service recommendation in dynamic SIoT. On the other side, Figure 5(a-b) shows the values of the RMSE noted in the calculation for d = 5 and d = 10 respectively, shows square of average squared error, showing the variation of the magnitude between actual and predicted values. For a better model per- performances to get the least RMSE values with fewer errors among the prediction values. All methods in first iterations begins with high values and afterwords decreases to get more practical values. As shown in Figure 5(a) for d = 5 starting with iteration 30, the proposed model started to better performance compare with other baseline models as iterations progressed. This shows that the proposed model, constantly get better performance than other methods, when compare with TSSR. The proposed method shows the least RMSE values. As shown in Figure 5(b) for d = 10, the proposed model gets the better performance when SoReg method advise the least prediction accuracy comparing with other methods.

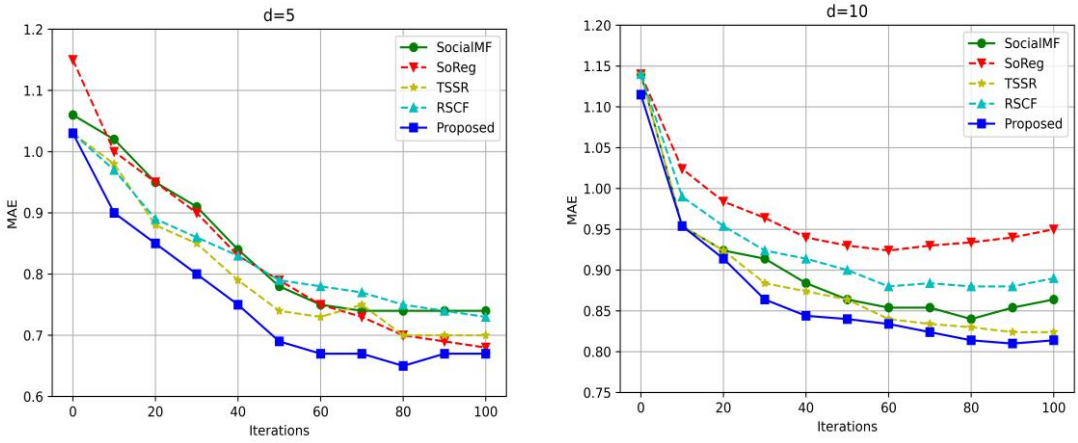

Fig. 4: Performance evaluation of proposed model with different recommendation methods based on MAE

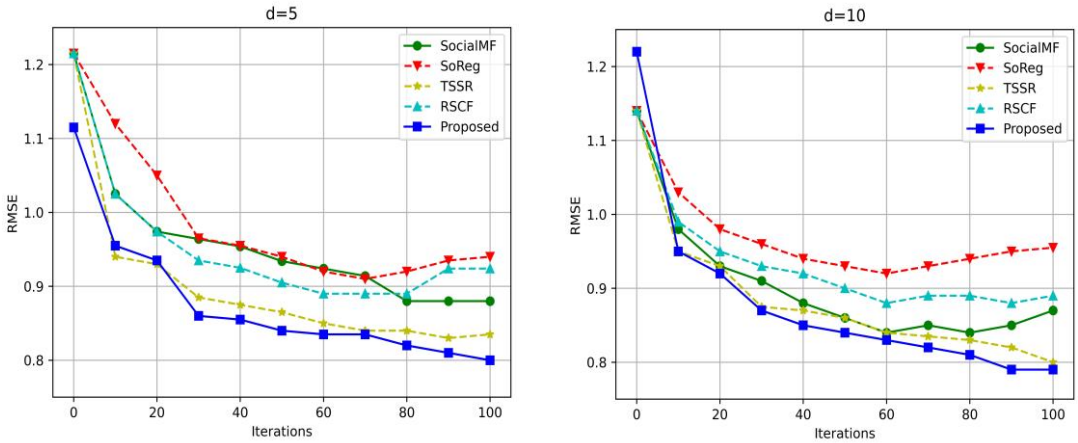

Fig. 5: Performance evaluation of proposed model with different recommendation methods based on RMSE

The MAE providing accurate errors offers a prediction accuracy assessment that is forthright. For larger errors, RMSE is more susceptible. The MAE gives a clear picture of overall accuracy regarding recommendations. The MAE having lower values of the proposed model across iterations indicating that it delivers more reliable and accurate predictions, professed effectiveness in sustaining both large and small errors when the SIoT in dynamic nature. Consequently, the proposed method gets better performance than other approaches in the circumstances of RMSE and MAE.

The calculation of recommendations performance using the metric NDCG, the proposed model is comparing with TSSR approach due to other method having less of data. Figure 6 shows the calculated NDCG values of various recommendation category with top-k recommendations. The proposed model gets better performance than TSSR noted the NDCG values among all the calculated recommendations category. The proposed model having higher NDCG scores, showing that its enhanced ability to get more relevant and accurate recommendations, Especially when the increases the list of the size of the recommendation. These differences indicate the effectiveness of proposed method in elaborate its potential, good recommendations for good performances in recommendation system when SIoT is in dynamic nature. However, it is observed that the NDCG values are lower for k = 5 and k = 10, respectively, comparing to k = 15 and k = 20. This is the matrices to increase space for the recommendation system to showing related items in top positions when the value of the k increases. In ranked list, the NDCG considering both the relation of the items and their positions. Therefore, it includes related items in higher positions, related to the NDCG score becomes high. However, the proposed method shows important improvement comparing to TSSR on the context of NDCG metric.

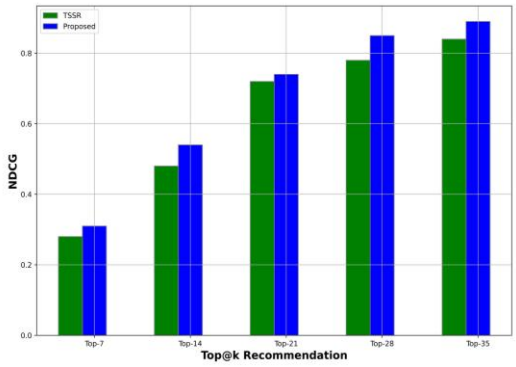

Fig. 6: Performance evaluation of proposed model with TSSR baselines based on NDCG

For the device interactions, having significant improvement in recommendations. The proposed model delivers many related recommendation and strengthens the symbiotic and collaborative relationships between devices in SIoT. In the SIoT devices act as trustees and play an important role in this method. The influence related to recommendation becomes more noticed. The increased reliability of particular devices that comprehensive enhancement of the recommendation service, improving a more reliable and effective ecosystem of the device connections.

The Implications of the Findings

Identifies reliable and consistent service providers in Social Internet of Things (SIoT) environments by evaluating various factors such as device interactions, social relationships, cooperativeness, and hidden service features. The proposed trust model achieves lower Root Mean Square Error (RMSE) and Mean Square Error (MSE) values, illustrating better and more accurate service provider recommendations. The model offers more robust and dependable trust evaluations even in dynamic and heterogeneous SIoT networks. The model achieves approximately 90% in Normalized Discounted Cumulative Gain (NDCG), highlighting its effectiveness in recommending top-quality and trusted service providers.

Conclusion and Future Work

This research focuses on identifying and recommending consistent and trustworthy service providers in the SIoT environment. The proposed trust model evaluates multiple factors, including interaction patterns, friendship and community similarities, cooperativeness, hidden features, and uncertainties associated with service providers. Through comprehensive experiments conducted on publicly available datasets, the effectiveness and efficiency of the proposed method have been demonstrated.

Performance evaluation using RMSE and MSE metrics indicates that the proposed approach achieves lower error rates in recommending service providers. Additionally, the cumulative gain (NDCG) score, which measures the efficiency of recommendations, confirms that the model successfully identifies the most trusted service providers, achieving an accuracy of approximately 90%.

By integrating social interactions, cooperativeness, credibility, readiness, and latent features of devices, the proposed model effectively enhances trust evaluation in SIoT-based recommendation systems. The research findings highlight the significance of key trustworthiness factors in service provider selection, addressing critical gaps in existing literature. The experimental results further validate the efficacy and practical applicability of the proposed method, making a valuable contribution to the field of SIoT trust modeling and recommendation systems.

In future work, the trust model should incorporate dynamically updated trust values in real time as relationships evolve. It should also integrate privacy-preserving techniques to prevent privacy breaches. Additionally, the model can be extended and optimized for large-scale, dynamic, and heterogeneous SIoT environments. Deep learning techniques can be employed to enhance the accuracy of trust value prediction for devices.

Acknowledgment

Thank you to the teachers and research scholars for their support in the publication of this research article. We are grateful for the resources and platform provided by the Department of Computer Science and Engineering, which have enabled us to share our findings with a wider audience. We appreciate the efforts of the reviewers and editorial team in reviewing and editing our work, and we are thankful for the opportunity to contribute to the field of research through this publication.

Funding Information

The authors have not received any financial support or funding to report.

Authors Contributions

Rahul: Main Conceptual Idea, outline/framework, interpretation writing the manuscript.

Venkatesh: Planned, methodology, results, critical feedback, analyzed correction in manuscript verification, future directions.

Satish B Basapur: Theoretical framework, reviewed the final version of the manuscript.

Ethics

I undersigned that this article has not been published elsewhere. The authors declare no conflict of interest.

References

Aalibagi, S., Mahyar, H., Movaghar, A., & Stanley, H. E. (2022). A Matrix Factorization Model for Hellinger-Based Trust Management in Social Internet of Things. *IEEE Transactions on Dependable and Secure Computing*, *19*(4), 2274–2285. https://doi.org/10.1109/tdsc.2021.3052953

Afzal, B., Umair, M., Asadullah Shah, G., & Ahmed, E. (2019). Enabling IoT platforms for social IoT applications: Vision, feature mapping, and challenges. *Future Generation Computer Systems*, *92*, 718–731. https://doi.org/10.1016/j.future.2017.12.002

Ahmed, A. I. A., Ab Hamid, S. H., Gani, A., khan, S., & Khan, M. K. (2019). Trust and reputation for Internet of Things: Fundamentals, taxonomy, and open research challenges. *Journal of Network and Computer Applications*, *145*, 102409. https://doi.org/10.1016/j.jnca.2019.102409

Amin, F., & Oun Hwang, S. (2022). Automated Service Search Model for the Social Internet of Things. *Computers, Materials & Continua*, *72*(3), 5871–5888. https://doi.org/10.32604/cmc.2022.028342

Amin, F., Majeed, A., Mateen, A., Abbasi, R., & Hwang, S. O. (2022). A Systematic Survey on the Recent Advancements in the Social Internet of Things. *IEEE Access*, *10*, 63867–63884. https://doi.org/10.1109/access.2022.3183261

Aslam, M. J., Din, S., Rodrigues, J. J. P. C., Ahmad, A., & Choi, G. S. (2020). Defining Service-Oriented Trust Assessment for Social Internet of Things. In *IEEE Access* (Vol. 8, pp. 206459–206473). https://doi.org/10.1109/access.2020.3037372

Ayub, M., Ghazanfar, M. A., Mehmood, Z., Alyoubi, K. H., & Alfakeeh, A. S. (2020). Unifying user similarity and social trust to generate powerful recommendations for smart cities using collaborating filtering-based recommender systems. *Soft Computing*, *24*(15), 11071–11094. https://doi.org/10.1007/s00500-019-04588-x

Becherer, M., Hussain, O. K., Zhang, Y., den Hartog, F., & Chang, E. (2024). On Trust Recommendations in the Social Internet of Things – A Survey. *ACM Computing Surveys*, *56*(6), 1–35. https://doi.org/10.1145/3645100

Ben Sada, A., Naouri, A., Khelloufi, A., Dhelim, S., & Ning, H. (2023). A Context-Aware Edge Computing Framework for Smart Internet of Things. *Future Internet*, *15*(5), 154. https://doi.org/10.3390/fi15050154

Bouazza, H., Said, B., & Zohra Laallam, F. (2022). A hybrid IoT services recommender system using social IoT. *Journal of King Saud University - Computer and Information Sciences*, *34*(8), 5633–5645. https://doi.org/10.1016/j.jksuci.2022.02.003

Chen, Z., Ling, R., Huang, C., & Zhu, X. (2016). A scheme of access service recommendation for the Social Internet of Things. *International Journal of Communication Systems*, *29*(4), 694–706. https://doi.org/10.1002/dac.2930

Cheng, W. K., Ileladewa, A. A., & Tan, T. B. (2019). A Personalized Recommendation Framework for Social Internet of Things (SIoT). *International Conference on Green and Human Information Technology (ICGHIT)*, 24–29. https://doi.org/10.1109/icghit.2019.00013

Chung, K. C., & Liang, S. W.-J. (2020). An Empirical Study of Social Network Activities via Social Internet of Things (SIoT). *IEEE Access*, *8*, 48652–48659. https://doi.org/10.1109/access.2020.2978151

Deng, S., Huang, L., & Xu, G. (2014). Social network-based service recommendation with trust enhancement. *Expert Systems with Applications*, *41*(18), 8075–8084. https://doi.org/10.1016/j.eswa.2014.07.012

Guo, G., Zhang, J., & Yorke-Smith, N. (2013). A novel Bayesian similarity measure for recommender systems. *Proceedings of the 23rd International Joint Conference on Artificial Intelligence (IJCAI)*, 2619–2625.

Hamrouni, A., Khanfor, A., Ghazzai, H., & Massoud, Y. (2022). Context-Aware Service Discovery: Graph Techniques for IoT Network Learning and Socially Connected Objects. *IEEE Access*, *10*, 107330–107345. https://doi.org/10.1109/access.2022.3212370

Hosseinzadeh, M., Mohammadi, V., Lansky, J., & Nulicek, V. (2024). Advancing the Social Internet of Things (SIoT): Challenges, Innovations, and Future Perspectives. *Mathematics*, *12*(5), 715. https://doi.org/10.3390/math12050715

Jamali, M., & Ester, M. (2010). A matrix factorization technique with trust propagation for recommendation in social networks. *Proceedings of the Fourth ACM Conference on Recommender Systems*, 135–142. https://doi.org/10.1145/1864708.1864736

Kalaï, A., Zayani, C. A., Amous, I., Abdelghani, W., & Sèdes, F. (2018). Social collaborative service recommendation approach based on user's trust and domain-specific expertise. *Future Generation Computer Systems*, *80*, 355–367. https://doi.org/10.1016/j.future.2017.05.036

Kang, D.-H., Choi, H.-S., Choi, S.-G., & Rhee, W.-S. (2017). SRS: Social Correlation Group based Recommender System for Social IoT Environment. *International Journal of Contents*, *13*(1), 53–61. https://doi.org/10.5392/ijoc.2017.13.1.053

Khan, W. Z., Arshad, Q.-A., Hakak, S., & Khan, M. K. (2021). Trust Management in Social Internet of Things: Architectures, Recent Advancements, and Future Challenges. *IEEE Internet of Things Journal*, *8*(10), 7768–7788. https://doi.org/10.1109/jiot.2020.3039296

Lakshmanaprabu, S. K., Shankar, K., Ilayaraja, M., Nasir, A. W., Vijayakumar, V., & Chilamkurti, N. (2019). Random forest for big data classification in the internet of things using optimal features. *International Journal of Machine Learning and Cybernetics*, *10*(10), 2609–2618. https://doi.org/10.1007/s13042-018-00916-z

Li, S., Xu, L. D., & Zhao, S. (2015). The internet of things: a survey. *Information Systems Frontiers*, *17*(243), 243–259.

Li, T., Huang, G., Zhang, S., & Zeng, Z. (2021). NTSC: a novel trust-based service computing scheme in social internet of things. *Peer-to-Peer Networking and Applications*, *14*(6), 3431–3451. https://doi.org/10.1007/s12083-021-01200-8

Lin, Z., & Dong, L. (2018). Clarifying Trust in Social Internet of Things. *IEEE Transactions on Knowledge and Data Engineering*, *30*(2), 234–248. https://doi.org/10.1109/tkde.2017.2762678

Lu, L., Yuan, Y., Chen, X., & Li, Z. (2020). A Hybrid Recommendation Method Integrating the Social Trust Network and Local Social Influence of Users. *Electronics*, *9*(9), 1496. https://doi.org/10.3390/electronics9091496

Lye, G. X., Cheng, W. K., Tan, T. B., Hung, C. W., & Chen, Y.-L. (2020). Creating Personalized Recommendations in a Smart Community by Performing User Trajectory Analysis through Social Internet of Things Deployment. *Sensors*, *20*(7), 2098. https://doi.org/10.3390/s20072098

Ma, H., Yang, H., Lyu, M. R., & King, I. (2008). SoRec. *Proceedings of the 17th ACM Conference on Information and Knowledge Management*, 931–940. https://doi.org/10.1145/1458082.1458205

Mishra, N., & Pandya, S. (2021). Internet of Things Applications, Security Challenges, Attacks, Intrusion Detection, and Future Visions: A Systematic Review. *IEEE Access*, *9*, 59353–59377. https://doi.org/10.1109/access.2021.3073408

Ngaffo, A. N., El Ayeb, W., & Choukair, Z. (2021). A time-aware service recommendation based on implicit trust relationships and enhanced user similarities. *Journal of Ambient Intelligence and Humanized Computing*, *12*(2), 3017–3035. https://doi.org/10.1007/s12652-020-02462-5

Pashaei Barbin, J., Yousefi, S., & Masoumi, B. (2020). Efficient service recommendation using ensemble learning in the internet of things (IoT). *Journal of Ambient Intelligence and Humanized Computing*, *11*(3), 1339–1350. https://doi.org/10.1007/s12652-019-01451-7

Rajendran, S., & Jebakumar, R. (2021). Object Recommendation based Friendship Selection (ORFS) for navigating smarter social objects in SIoT. *Microprocessors and Microsystems*, *80*, 103358. https://doi.org/10.1016/j.micpro.2020.103358

Sagar, S., Mahmood, A., Sheng, Q. Z., Zhang, W. E., Zhang, Y., & Pabani, J. K. (2024). Understanding the Trustworthiness Management in the Social Internet of Things: A Survey. *Computer Networks*, *251*, 110611. https://doi.org/10.1016/j.comnet.2024.110611

Shokeen, J., & Rana, C. (2021). A trust and semantic based approach for social recommendation. *Journal of Ambient Intelligence and Humanized Computing*, *12*(11), 10289–10303. https://doi.org/10.1007/s12652-020-02806-1

Smart, P., Madaan, A., & Hall, W. (2019). Where the smart things are: social machines and the Internet of Things. *Phenomenology and the Cognitive Sciences*, *18*(3), 551–575. https://doi.org/10.1007/s11097-018-9583-x

Son, J., Choi, W., & Choi, S.-M. (2020). Trust information network in social Internet of things using trust-aware recommender systems. *International Journal of Distributed Sensor Networks*, *16*(4). https://doi.org/10.1177/1550147720908773

Wang, Y., Li, L., & Liu, G. (2015). Social context-aware trust inference for trust enhancement in social network based recommendations on service providers. *World Wide Web*, *18*(1), 159–184. https://doi.org/10.1007/s11280-013-0241-5

Wei, L., Wu, J., Long, C., & Li, B. (2021). On Designing Context-Aware Trust Model and Service Delegation for Social Internet of Things. *IEEE Internet of Things Journal*, *8*(6), 4775–4787.
` https://doi.org/10.1109/jiot.2020.3028380

Wei, L., Yang, Y., Wu, J., Long, C., & Lin, Y.-B. (2022). A Bidirectional Trust Model for Service Delegation in Social Internet of Things. *Future Internet*, *14*(5), 135. https://doi.org/10.3390/fi14050135

Wu, X., & Liang, J. (2021). A blockchain-based trust management method for Internet of Things. *Pervasive and Mobile Computing*, *72*, 101330. https://doi.org/10.1016/j.pmcj.2021.101330

Yan, B., Yu, J., Yang, M., Jiang, H., Wan, Z., & Ni, L. (2021). A novel distributed Social Internet of Things service recommendation scheme based on LSH forest. *Personal and Ubiquitous Computing*, *25*(6), 1013–1026. https://doi.org/10.1007/s00779-019-01283-4