Servitrust: Reliable Local Services Through Trust Metrics

[1]Mrs. Sujatha S, [2]Ragul K, [3]Karthick S, [4]Saidivakar A, [5]Nithish Kumar M

[1]Assistant Professor, [2]Student, [3]Student, [4]Student, [5]Student

[1]Department of Information Technology,

[1]Adhiyamaan College of Engineering, Hosur, India

Abstract: The rapid growth of on-demand local service platforms has made users more reliant on digital systems to find service providers such as plumbers, electricians, and technicians. However, most existing platforms depend on star ratings and subjective reviews, which may not accurately reflect service reliability and long-term trust. Servitrust offers a trust-based local service discovery and matching system that focuses on real trust the system calculates a dynamic trust score for each service provider using objective factors including service completion, rate punctuality, repeat customer interactions, cancellation history, and complaint records. Based on this trust score service providers are ranked and recommended to users, ensuring fair visibility for reliable providers. The platform allows users to request services based on location and category while automatically suggesting the most trustworthy providers in real time. By prioritizing transparency and data-based trust evaluation, servitrust enhances customer satisfaction, reduces misleading reviews, and encourages responsible service behavior. The system is suitable for residential communities, campuses, and smart city environments.

Keywords: Trust Score, Local Service Platform, Dynamic Rating System, Complaint Validation, Service Lifecycle Management, Transparency.

I. INTRODUCTION

The rapid growth of digital technology has changed how people access everyday services. From booking rides to ordering food, online platforms have made many daily tasks simpler. However, users still face significant challenges when looking for reliable local service providers such as plumbers, electricians, carpenters, and technicians. In many areas, finding services relies on personal recommendations, informal contacts, or unverified online listings. Even though digital service marketplaces exist, they often do not fully address issues related to trust, safety, and service quality. One major problem with the local service landscape is the lack of a transparent and structured system for reliability. Most platforms focus on convenience, pricing, and quick booking, but they do not offer a way to assess the long-term performance and consistency of service providers.

Star ratings and customer reviews are common, but these methods can be biased, manipulated, or based on limited interactions. A provider might get high ratings from a few users but may not consistently offer quality service. Likewise, negative feedback may not always reflect true performance due to misunderstandings or unfair complaints. As a result, users often find it difficult to confidently choose a trustworthy provider. Trust becomes crucial in local service situations since these services require direct physical interactions between customers and providers. Unlike purely digital transactions, local services often involve access to homes or personal spaces, making reliability and accountability key. Without a structured way to evaluate trust, users may face poor service quality, inconsistent performance, slow responses, or even safety risks.

Meanwhile, dedicated and hardworking service providers may not receive the recognition they deserve if the platform does not accurately showcase their performance history. To tackle these challenges, this research proposes ServiTrust, a trust-based local service discovery platform aimed at improving transparency, accountability, and reliability. The main idea behind ServiTrust is to use a dynamic trust score system that evaluates service providers based on multiple performance factors, not just basic ratings. The trust score is calculated using elements such as verified service completion, user ratings, feedback quality, complaint validation, and service consistency. By continuously updating this score after every completed service, the system ensures that provider rankings reflect real-world performance. ServiTrust also introduces role-based access control for users, service providers, and administrators to maintain system integrity and secure operations. Complaints filed by users are verified by administrators before impacting the provider's trust score, ensuring fairness and preventing system misuse. Through this structured and data-driven approach, ServiTrust seeks to create a reliable local service ecosystem where users can make informed decisions with confidence. Overall, the proposed system aims to enhance trust in digital service marketplaces by incorporating transparency, accountability, and dynamic evaluation into the service discovery process.

II. OBJECTIVE

The main goal of this research is to create a trust-based local service discovery system that improves reliability, transparency, and accountability in selecting service providers. The proposed system, ServiTrust, aims to overcome the shortcomings of current service marketplace platforms by introducing a clear and data-driven trust evaluation process. By combining service history, user feedback, complaint validation, and performance consistency into a dynamic trust score, the system wants to give users a more trustworthy and secure way to book local services. The platform is designed to boost user confidence and ensure fair recognition for truly reliable service providers.

Specific Objectives:
- To develop a secure and scalable local service discovery platform that connects users with verified service providers.
- To design and implement a dynamic Trust Score mechanism based on user ratings, service completion records, complaint validation, and service consistency.
- To ensure role-based access control for users, service providers, and administrators for secure system operations.
- To provide a structured complaint management system that validates complaints before they affect a provider's trust score.
- To enable real-time tracking of service requests from creation to completion for better transparency.
- To implement filtering and ranking mechanisms that show service providers based on trust score and performance metrics.
- To create a user-friendly interface that makes service booking, feedback submission, and request monitoring easy.
- To improve accountability and reduce the risk of fake reviews or manipulated ratings by allowing review submissions only after service completion.
- To build a centralized backend system using secure REST APIs and database integration for reliable data management.

III. LITERATURE REVIEW

Recent research on digital service platforms has increasingly focused on improving trust management, reputation modeling, and reliability assessment. As online marketplaces and service-based applications grow quickly, traditional star-rating systems have shown they cannot accurately reflect long-term provider performance. Static ratings often depend on personal opinions and are prone to manipulation, which reduces transparency and fairness in service selection. To tackle these issues, several recent studies have suggested new trust evaluation frameworks that combine various performance indicators.

A major study published in 2022 introduced a multi-factor trust evaluation framework designed for decentralized service environments. This framework uses behavioural metrics, historical transaction records, and credibility assessments to calculate a dynamic trust value. Unlike static rating methods, this approach continuously updates trust scores based on service consistency and anomaly detection. By

incorporating multiple factors, the model offers better resistance against reputation manipulation. However, this framework mainly targets distributed computing and blockchain environments. It does not adequately address centralized complaint validation processes or administrative oversight, which are crucial in local service marketplaces where accountability and user safety are vital.

In 2023, another study proposed a deep-learning-based reputation evaluation model for online service platforms. This model uses historical performance data, user behaviour, and sentiment analysis of feedback to predict provider reliability more accurately. The study shows that machine learning techniques can improve recommendation accuracy and identify fraudulent or biased reviews more effectively than traditional averaging methods. While the approach enhances predictive trust scoring, it needs significant computational resources and large datasets. Additionally, the model mainly focuses on predictive analytics and does not fully include real-time service lifecycle tracking or structured complaint handling, which are important in practical service marketplace applications.

More recently, a trust-aware service recommendation framework was developed for smart service environments. This framework combines user ratings, service completion rates, cancellation history, and performance indicators to calculate a composite trust score. The study emphasizes the importance of using multiple operational factors to ensure fair provider visibility and ranking accuracy. While the framework allows for dynamic recalculation of trust scores, it lacks a detailed administrative validation mechanism for checking complaints. In real-world local service platforms, properly assessing complaints and confirming service completion greatly influence trust reliability and user confidence.

Overall, recent research shows that there has been significant progress in dynamic trust modeling and reputation-aware recommendation systems. However, many existing approaches either depend on decentralized structures, require heavy computational resources, or focus on feedback-driven analytics without including centralized lifecycle tracking and complaint validation. There is still a clear need for a scalable and transparent trust-based framework that combines verified service completion, administrative complaint validation, and real-time performance monitoring within a centralized service marketplace.

IV. EXISTING SYSTEM

Existing local service marketplace platforms connect users with nearby service providers through digital booking systems. These platforms let users search for services by categories like plumbing, electrical work, carpentry, and appliance repair. Basic features include profiles for providers, service descriptions, pricing details, availability status, and customer ratings. While these systems make things more convenient and accessible compared to traditional word-of-mouth, they still have several issues with reliability and trust evaluation. Most current platforms depend on star-based rating systems and user reviews to show service quality. Although ratings give users a quick reference, they are often subjective and based on individual experiences. In many cases, ratings do not reflect the long-term consistency of services or the overall reliability of providers. Additionally, reviews can be manipulated, biased, or submitted without strict checks on whether the service was completed.

This reduces the credibility of the evaluation system and may mislead users when choosing providers. Another significant issue is the lack of a dynamic trust calculation model. Existing systems usually present average ratings without factoring in key performance indicators, such as service completion rate, response time, complaint history, and consistency in performance. As a result, provider rankings may not accurately depict real performance over time. Moreover, complaint management processes on many platforms lack transparency and structured validation. Complaints often do not impact provider reputation unless administrators manually review them. There is also limited protection against false or malicious reporting. In summary, while current systems focus on booking efficiency and service accessibility, they do not establish a clear and structured trust-based framework. This gap points to the need for a more reliable and transparent approach to evaluating local services.

V. PROPOSED SYSTEM

The proposed system, ServiTrust, is a trust-based local service discovery platform aimed at addressing the shortcomings of current service marketplaces. It focuses on improving transparency, accountability, and reliability by introducing a structured trust evaluation system. Unlike traditional platforms that rely solely on static ratings, ServiTrust combines dynamic performance metrics and validated feedback for evaluating providers. Here are the key features of the proposed system:

5.1 Dynamic Trust Score Mechanism

The main part of ServiTrust is a model for calculating a dynamic trust score. The score is based on various factors such as user ratings, verified service completion, complaint validation, and service consistency. It updates automatically after each completed service, ensuring that provider rankings reflect real-time performance instead of static averages.

5.2 Verified Feedback and Complaint Validation

Users can submit ratings and feedback only after a service is successfully completed. This prevents fake or unauthorized reviews. Complaints made by users are also verified by administrators before they impact a provider's trust score. This validation process ensures fairness while maintaining accountability.

5.3 Transparent Service Lifecycle Tracking

ServiTrust provides a clear service workflow, including stages like request creation, provider acceptance, service execution, and completion. Users can track the status of their service requests in real time. This transparency builds user confidence and improves communication between users and providers.

5.4 Secure and Role-Based Access Control

The system uses role-based access for users, service providers, and administrators. Secure authentication methods protect data and control access to system features. This control strengthens system integrity and prevents unauthorized actions.

Overall, the proposed system sets up a trust-driven framework that improves reliability in local service discovery and fosters a safer, more accountable digital service environment.

VI. RESEARCH METHODOLOGY

The research methodology explains the step-by-step process used to design, develop, and evaluate the ServiTrust system. It includes planning, analyzing requirements, designing the architecture, implementing the system, and validating the trust-based framework. The approach is detailed below:

6.1 Requirement Analysis

The first stage involved identifying the limitations of current local service platforms and understanding user needs. We defined functional requirements like service discovery, request management, review submission, complaint handling, and trust score calculation. We also considered non-functional requirements such as security, scalability, usability, and transparency. This phase ensured that the system's goals matched real-world challenges in the service marketplace.

6.2 System Design and Architecture Planning

Using the identified requirements, we created a three-tier architecture. This architecture includes a presentation layer (Android application), a business logic layer (Spring Boot backend), and a data layer (MySQL database). We structured the system workflow, data flow, and interactions among users, providers, and administrators. We also defined the logic for computing trust scores during this stage.

6.3 Technology Selection and Development Tools

We selected appropriate technologies to ensure the system's reliability and scalability. We developed the frontend using Kotlin and Jetpack Compose for a modern user interface. The backend was built with Spring Boot REST APIs and JPA for database interaction. We chose MySQL for structured data storage. Retrofit facilitated communication between the mobile application and the backend server.

6.4 Trust Score Model Formulation

We developed a rule-based trust scoring model to assess service provider performance. This model includes parameters like user ratings, completion rates, verified complaints, and cancellation histories. The trust score updates dynamically after each relevant event. We assigned weight values to each parameter to ensure a balanced and fair evaluation.

6.5 System Implementation

We implemented the system in incremental steps. We developed and integrated core functionalities such as user registration, provider profile management, the service request lifecycle, review submission, and complaint validation. We tested the APIs with controlled input scenarios to ensure correct trust score updates and consistent data.

6.6 Testing and Validation

We tested the system with various user scenarios to check its functionality, accuracy, and reliability. Functional testing confirmed that both request flow and trust score updates worked correctly. We also tested edge cases such as repeated complaints, invalid reviews, and cancellation scenarios to ensure robustness. The results showed that the trust mechanism accurately reflects provider performance.

VII. SYSTEM ARCHITECTURE

The system architecture of ServiTrust uses a three-tier client-server model to ensure modularity, scalability, and secure communication between components. This design divides the system into three main layers: the Presentation Layer, the Application Layer, and the Data Layer. Each layer has specific responsibilities while working together to deliver a dependable trust-based service platform. The Presentation Layer includes the Android mobile app developed with Kotlin and Jetpack Compose. This layer manages all user interactions and displays the graphical interface. It offers role-based access for Users, Service Providers, and Administrators. Users can search for providers by service type, view trust scores, create service requests, submit reviews, and file complaints. Service providers can handle incoming requests, update service statuses, and track their trust performance. Administrators can verify complaints and oversee system-level activities. All interactions in this layer securely transmit data to the backend using REST APIs integrated through Retrofit.

The Presentation Layer ensures a responsive and user-friendly experience while maintaining secure communication. The Application Layer is built with Spring Boot and serves as the main logic processor of the system. This layer manages authentication, authorization, validation, and business logic. It processes incoming requests from the mobile app, applies set rules, and carries out necessary operations like creating service requests, updating request statuses, verifying complaints, and recalculating trust scores. The trust score engine is included in this layer, updating provider rankings based on factors such as service completion rate, user ratings, verified complaints, and cancellation history. The backend also controls access based on user roles to ensure only authorized users can perform specific actions. By centralizing business logic in this layer, the system maintains consistency and scalability.

The Data Layer is powered by MySQL, a relational database management system that stores structured data such as user profiles, provider details, service requests, reviews, complaints, and trust history records. Spring Data JPA is used for object-relational mapping, allowing smooth interaction between Java objects and database tables. This layer ensures data integrity, transactional consistency, and reliable storage of trust-related metrics. Each update in service status or complaint verification triggers database updates, which are then reflected in the recalculated trust score.

The communication process starts when a user takes action in the mobile app. The request is sent to the backend via REST API. The backend processes the request, interacts with the database if needed, recalculates trust metrics when necessary, and sends the response back to the app. The user interface then updates dynamically based on the received response. This structured architecture ensures real-time data synchronization, secure processing, and effective separation of responsibilities. Overall, the three-tier trust-based system architecture offers a solid foundation for ServiTrust, ensuring reliability, maintainability, and transparency in local service discovery.
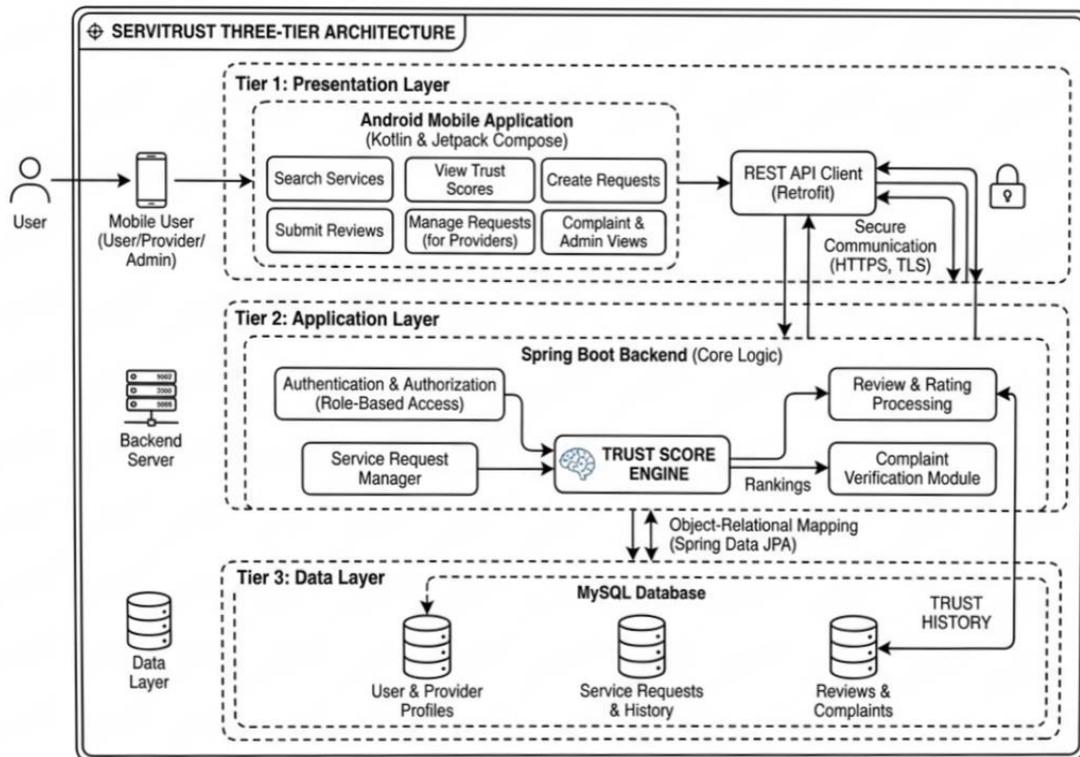
Fig. 1: ServiTrust Three-Tier Trust-Based Architecture

VIII. MODULE DESCRIPTION

The ServiTrust system includes several functional modules that work together to ensure secure operations, transparent service management, and ongoing trust evaluation. Each module has a specific role and integrates smoothly with the other components of the system. The detailed modules are described below:

8.1 User Authentication and Profile Management

This module manages secure registration, login, and profile upkeep for users, service providers, and administrators. It uses role-based access control to ensure that each user group can access only the features they are allowed to use. Passwords are stored securely with encryption to protect user credentials. The module also controls sessions, providing secure login persistence within the mobile application. Service providers can update their professional details, such as service category, availability, and experience, while users maintain their personal information and service history. This module is the foundation of system security and identity management.

8.2 Service Discovery and Intelligent Provider Listing

This module helps users search for services by type, category, and location. It pulls relevant providers from the database and ranks them dynamically based on trust score and performance metrics. The ranking system ensures that providers with higher reliability and better service history appear at the top. Filtering options make it easier for users to make quick, informed decisions. This module improves transparency by showing provider trust scores with service information.

8.3 Service Request Lifecycle and Tracking

This module handles the entire lifecycle of a service request. Users can create requests by providing service details and location. Providers receive notifications about incoming requests and can choose to accept or reject them. Once accepted, the request moves through defined stages, including Accepted, In Progress, and Completed. Users can track the real-time status of their requests through the mobile app. This organized workflow ensures accountability and clear communication between users and providers.

8.4 Review and Feedback Management

After a service is successfully completed, users can submit ratings and written feedback. Reviews are limited to completed services to avoid fake or unauthorized entries. The system checks review eligibility before acceptance. Feedback is saved in the database and helps calculate the dynamic trust score. This module ensures authenticity and strengthens the credibility of the evaluation system.

8.5 Trust Score Calculation and Performance Monitoring

This is the main module of ServiTrust. It calculates a dynamic trust score for each provider using multiple weighted parameters, including average rating, service completion rate, verified complaints, and cancellation frequency. The trust score is updated automatically whenever a relevant event occurs. This ongoing recalculation keeps provider rankings aligned with real-time performance and reliability.

8.6 Complaint Management and Administrative Oversight

This module allows users to file complaints after service completion. Administrators review and validate complaints before they affect the provider's trust score. This process prevents misuse and ensures fairness. Administrators also oversee system activity, manage user accounts, and ensure compliance with platform rules. The validation process boosts transparency and accountability across the system.

IX. RESULTS AND DISCUSSION

9.1 Experimental Setup

To assess the effectiveness of the proposed ServiTrust system, we created a structured experimental environment to mimic real-world interactions between users and service providers. The system ran on a Spring Boot REST backend, connected to a MySQL database, with an Android mobile application serving as the front-end interface. The evaluation focused on measuring system reliability, trust score accuracy, complaint handling efficiency, and ranking transparency.

We developed a set of simulated service providers with various service histories, ratings, cancellation records, and complaint statuses. Multiple user accounts generated service requests across different categories like plumbing, electrical repair, and appliance servicing. Each request went through defined lifecycle stages, including Requested, Accepted, Completed, and Cancelled.

After the service was completed, users could submit ratings and feedback. Complaints were registered and processed through administrative validation before they influenced the provider's trust score. We compared the performance of the proposed trust-based ranking mechanism to a traditional rating-only system to examine improvements in fairness and transparency. All tests were carried out under consistent system configurations to ensure a fair comparison and reliable results.

9.2 Performance Metrics

We conducted a comparative evaluation between the Traditional Rating-Based System and the Proposed ServiTrust System using various performance indicators such as trust score reliability, review authenticity, complaint impact, adaptability, and system efficiency

Table 1: Performance Comparison Between Traditional System and Proposed ServiTrust System Metric

Metric	Traditional Rating-Based System	Proposed ServiTrust System
Provider Ranking	Based only on average star rating	Based on rating, completion rate, complaint validation and consistency
Review Control	Reviews can be manipulated	Reviews allowed only after service completion
Complaint Handling	Often manual and delayed	Admin-validated complaint impact
Trust Score Update	Static, slow adjustment	Dynamic, event-driven recalculation
Performance Transparency	Limited visibility of history	Complete service lifecycle tracking

- Provider Ranking Accuracy

In traditional platforms, provider ranking mainly relies on average star ratings. This method does not take into account service completion rates, cancellations, or complaint records. During testing, it was found that providers with high ratings but frequent cancellations still ranked at the top in systems that only considered ratings. In contrast, the ServiTrust model recalculated trust scores dynamically using several weighted factors. Providers with consistent performance and fewer complaints were ranked higher. This led to fair and reliable ordering of service providers.

- Review Authenticity

Traditional systems often allow open review submission, which raises the risk of fake ratings. In the proposed system, review submissions were strictly limited to completed services, and duplicate reviews for the same request were not allowed. Testing confirmed that this limitation removed unauthorized feedback and improved the credibility of provider ratings.

- Complaint Validation Impact

In many existing systems, complaints can directly harm a provider's reputation without verification. In ServiTrust, complaints only affect the trust score after administrative validation. This stops false complaints from unfairly hurting a provider's ranking. Experimental observations showed balanced trust adjustments without sudden drastic score drops.

- Dynamic Trust Score Adaptability

The traditional rating-based model updates slowly and does not reflect real-time changes in service quality. The proposed ServiTrust model recalculates the trust score immediately after service completion, review submission, or validated complaint. This event-driven recalculation method ensures that provider rankings accurately reflect current performance.

- System Efficiency and Responsiveness

The backend REST APIs showed stable performance during simultaneous request simulations. The average API response time stayed within acceptable limits, and trust score recalculation occurred instantly after triggering events.

9.3 Overall Discussion

The experimental evaluation shows that the ServiTrust system significantly improves transparency, accountability, and reliability in local service discovery. By using dynamic trust metrics instead of just star ratings, the system ensures fair provider ranking and reduces the risk of manipulation. The trust score engine stands out as the key strength of the proposed model, as it continuously adjusts to real service outcomes. The structured workflow and verified review process further enhance the system's

integrity. In summary, the results confirm that ServiTrust offers a more secure, transparent, and performance-driven alternative to traditional rating-based service platforms.

X. CONCLUSION

The ServiTrust system offers a clear and trust-focused method for improving reliability in local service discovery platforms. Traditional service marketplaces mainly rely on fixed rating systems. These often fail to reflect long-term performance and can be easily manipulated or influenced by biased feedback. To solve these issues, ServiTrust introduces a trust score model that uses various objective factors, including service completion rates, cancellation rates, verified complaints, and authenticated user reviews. The system recalculates trust scores in real time after every important service interaction. This immediate updating allows provider rankings to show current performance instead of outdated averages. Validating administrative complaints increases fairness and prevents misuse of the rating system. Additionally, allowing reviews only for completed services boosts credibility and reduces fraudulent feedback.

Experimental results show that the ServiTrust framework greatly enhances transparency, accountability, and ranking accuracy compared to traditional rating systems. Its structured tracking of the service lifecycle and role-based access control improve system integrity and user trust. Overall, ServiTrust creates a scalable and secure trust-driven service environment suitable for residential communities, academic campuses, and smart city settings. Future work may include the integration of machine learning models for predictive trust analysis and expanding support across different web platforms, which would further enhance reliability and user satisfaction in digital service marketplaces.

XI. ACKNOWLEDGEMENT

XII. REFERENCES

[1] W. Z. Khan, Q. U. A. Arshad, S. Hakak, M. K. Khan, and S.-U. Rehman, "Trust management in social Internet of Things: Architectures, recent advancements, and future challenges," IEEE Internet of Things Journal, vol. 8, no. 10, pp. 7768–7788, 2021.

[2] R. A. Saleh, M. Driss, and I. Almomani, "CBiLSTM: A hybrid deep learning model for efficient reputation assessment of cloud services," IEEE Access, vol. 10, pp. 35321–35335, 2022.

[3] S. Zhang, D. Zhang, Y. Wu, and H. Zhong, "Service recommendation model based on trust and QoS for social Internet of Things," IEEE Transactions on Services Computing, vol. 16, no. 5, pp. 3736–3750, 2023.

[4] J. Golbeck, "Trust and nuanced profile similarity in online social networks," ACM Transactions on the Web, vol. 3, no. 4, 2009.

[5] H. Xia, F. Tao, and Y. Cheng, "A trust-aware service recommendation method based on collaborative filtering," Knowledge Based Systems, vol. 86, pp. 91–99, 2015.

[6] M. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," Decision Support Systems, vol. 43, no. 2, pp. 618–644, 2007.

[7] P. Resnick, K. Kuwabara, R. Zeckhauser, and E. Friedman, "Reputation systems," Communications of the ACM, vol. 43, no. 12, pp. 45–48, 2000.

[8] Y. Wang and J. Vassileva, "Trust and reputation model in peer-to-peer networks," in Proceedings of the IEEE International Conference on Peer-to-Peer Computing, 2003, pp. 150–157.