

## Article

# Exploring Trust Dynamics in Online Social Networks: A Social Network Analysis Perspective

Stavroula Kridera and Andreas Kanavos \* 

Department of Informatics, Ionian University, 49100 Corfu, Greece; kridera@ionio.gr

\* Correspondence: akanavos@ionio.gr

**Abstract:** This study explores trust dynamics within online social networks, blending social science theories with advanced machine-learning (ML) techniques. We examine trust's multifaceted nature—definitions, types, and mechanisms for its establishment and maintenance—and analyze social network structures through graph theory. Employing a diverse array of ML models (e.g., KNN, SVM, Naive Bayes, Gradient Boosting, and Neural Networks), we predict connection strengths on Facebook, focusing on model performance metrics such as accuracy, precision, recall, and F1-score. Our methodology, executed in Python using the Anaconda distribution, unveils insights into trust formation and sustainability on social media, highlighting the potent application of ML in understanding these dynamics. Challenges, including the complexity of modeling social behaviors and ethical data use concerns, are discussed, emphasizing the need for continued innovation. Our findings contribute to the discourse on trust in social networks and suggest future research directions, including the application of our methodologies to other platforms and the study of online trust over time. This work not only advances the academic understanding of digital social interactions but also offers practical implications for developers, policymakers, and online communities.

**Keywords:** data mining; machine-learning techniques; predictive modeling; social network graph analysis; trust dynamics; online social networks



**Citation:** Kridera, S.; Kanavos, A. Exploring Trust Dynamics in Online Social Networks: A Social Network Analysis Perspective. *Math. Comput. Appl.* **2024**, *29*, 37. <https://doi.org/10.3390/mca29030037>

Academic Editor: Leonardo Trujillo

Received: 24 March 2024

Revised: 6 May 2024

Accepted: 10 May 2024

Published: 15 May 2024



**Copyright:** © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

## 1. Introduction

The advent of the digital era has ushered in an unprecedented transformation in human connectivity, with online social networks at the forefront of this paradigm shift. These platforms have become central to our personal, professional, and civic lives, establishing trust as a critical yet complex pillar within this digital ecosystem. Trust in online environments transcends mere transactional interactions, embedding itself into the fabric of virtual communities and influencing the formation, depth, and resilience of online connections [1]. Despite the extensive body of research exploring the dynamics of online communities, the nuanced mechanisms through which trust is formed, maintained, and eroded in these digital spaces remain underexplored. This gap presents a compelling opportunity for interdisciplinary inquiry, combining the theoretical depth of social sciences with the analytical breadth of advanced machine-learning (ML) techniques to unveil the intricacies of digital trust [2].

Trust in online social networks is defined as the confidence users place in one another and the platform, influenced by the perceived reliability, integrity, and competence of the parties involved. This concept extends beyond simple reliability, embedding deeply in the expectations of reciprocal behavior and the ethical use of shared information within digital communities.

Drawing from a rich tapestry of disciplines—economics, psychology, sociology, and computer science—this study embarks on an exploratory journey into the multifaceted nature of trust within online social networks. Trust influences not only the propensity for information sharing and community engagement but also the overall cohesion and

sustainability of digital platforms. By employing a diverse array of ML models, including KNN, Logistic Regression, SVM, Naive Bayes, and others, we aim to predict the strength and quality of user connections on platforms exemplified by Facebook, advancing the empirical study of trust dynamics in social media settings [3].

Our investigation also delves into the structural and algorithmic underpinnings of social networks, utilizing graph theory and predictive modeling to navigate the ethical and practical challenges inherent in trust analysis. Issues such as privacy concerns, misinformation, and online deception are critically examined, reflecting the complex interplay between technology and trust in digital communities. Through this comprehensive approach, we contribute to the scholarly dialogue on digital trust, highlighting the role of computational methods in dissecting the complex social interactions that characterize online networks [4].

Unique to this research is our methodological innovation that integrates diverse machine-learning models not merely as analytical tools but as integral components of understanding trust dynamics within the nuanced context of social interactions. We introduce novel machine-learning applications, such as the use of ensemble methods and deep learning techniques, specifically adapted to dissect and quantify trust within vast and unstructured social media data. This novel approach allows for a more nuanced capture and analysis of trust signals, which are often subtle and context-dependent.

The significance of this study extends beyond academic interest, addressing critical real-world issues such as the enhancement of digital trustworthiness and the design of more effective social media governance frameworks. By providing empirical insights into how trust forms and evolves in online environments, our research supports the development of algorithms that can effectively detect and mitigate issues of mistrust, fraud, and misinformation. Additionally, the findings have important implications for the design of digital platforms, offering guidelines that can help foster healthier and more trustworthy online communities [5].

In an era where online interactions increasingly influence the contours of society, understanding the mechanisms of trust becomes paramount. This research offers a meticulous examination of trust's underlying mechanisms, informed by both theoretical considerations and robust empirical analyses [6]. By setting a new standard for interdisciplinary research, this study promotes a collaborative discourse among technologists, social scientists, and platform users, aiming to co-develop digital ecosystems that prioritize trust.

Our findings promise to inform the ongoing evolution of digital platforms, guiding the development of more inclusive, secure, and trust-oriented online communities. As we navigate through the complexities of trust prediction within social networks, this paper is structured to provide a comprehensive overview of the field, detailing our methodologies for trust prediction, describing the implementation of our models, evaluating their performance, and concluding with a discussion of our findings and directions for future research. This rich dialogue not only advances our academic understanding of trust in online social networks but also sparks a broader conversation on leveraging emerging technologies to foster trust among digital communities [7].

### 1.1. Trust Dynamics in Social Networks

This research delves into the dynamics of trust within online social networks, particularly focusing on Facebook. Utilizing various machine-learning models, we explore the complex nature of trust, which encompasses several dimensions:

- **Definitions of Trust:** We clarify different academic and practical definitions of trust, providing a broad understanding that caters to diverse social networking contexts.
- **Types of Trust:** Trust is categorized into cognitive-based trust (rooted in beliefs and experiences) and affect-based trust (founded on emotional bonds [8,9]), each playing a vital role in social interactions.
- **Mechanisms of Trust Formation:** We analyze how trust is built, maintained, and broken within social networks, highlighting the role of communication patterns, shared experiences, and mutual friends in influencing trust levels.

By employing a range of machine-learning tools, from Logistic Regression to Neural Networks, we assess the predictive power of these models in identifying and quantifying trust relationships on Facebook, thus providing insights into how digital interactions translate into trust metrics.

### 1.2. Key Contributions and Implications

This subsection outlines the contributions of our study, emphasizing the unique aspects and potential impacts of our research:

- **Innovative Methodologies:** We present novel machine-learning techniques specifically developed to address the challenges of modeling trust in the complex environment of social networks.
- **Empirical Insights:** Our study provides empirical data and analyses that deepen the understanding of trust dynamics and their implications for online communities.
- **Practical Implications:** The findings have significant practical implications, offering guidelines for designing digital platforms that foster trust and community engagement.

The remainder of this paper is structured as follows: Section 2 reviews related work, setting the stage for our analysis. Section 3 outlines the methodologies employed for trust prediction. Section 4 delves into the implementation details of our models. Section 5 presents a rigorous evaluation of these models' performance. Finally, Section 6 encapsulates our findings and proposes directions for future research.

## 2. Related Work

Trust's exploration spans numerous disciplines, underscoring its foundational role in both personal and economic spheres. Economists like Arrow have highlighted how trust acts as a crucial enabler of economic transactions, serving as a lubricant that reduces friction in the marketplace, a principle that extends into the realm of online transactions and interactions, showcasing the enduring relevance of trust in economic activities within digital platforms [10]. Psychologists investigating the roots of trust in individual behavior and cognition, like Rotter, have revealed how perceptions of trustworthiness significantly influence human interactions, a dynamic that remains pivotal in online settings where digital personas and interactions frame these perceptions [11].

Sociologists have mapped trust onto the fabric of societal structures, arguing for its essential role in the smooth functioning of societies and facilitating cooperative behaviors, with Coleman's work providing a broad framework for understanding societal trust [12]. Theories like Granovetter's "strength of weak ties" [13] and Burt's "structural holes" [14] offer valuable insights into the complexities of trust in digital landscapes, suggesting that indirect connections through network structures significantly impact trust formation and information flow in online environments.

The digital revolution, marked by the rise of social networks, has transformed human interaction, introducing novel dynamics into trust formation and management. These platforms have expanded our social circles and the speed of connection formation, bringing unique challenges in how trust is established and maintained without traditional face-to-face cues. The role of online identities and reputation systems in trust dynamics has become increasingly significant, as Donath outlined, influencing how individuals present themselves online and how they are perceived by others, therefore impacting the trust placed in them [15].

While the foundational work across disciplines provides a robust framework for understanding trust, there are notable limitations in the existing research. For instance, economic models of trust often oversimplify the complexities of interpersonal trust in digital interactions, focusing predominantly on transactional aspects without fully capturing the social and psychological nuances. Similarly, psychological and sociological studies, while insightful, frequently rely on traditional face-to-face contexts and may not fully translate to online environments where cues and interactions differ significantly.

Our research addresses limitations in trust research by:

- **Adapting Psychological Constructs for Online Contexts:** We refine psychological theories of trust to better suit digital interactions, applying machine-learning techniques to detect subtleties in online communication that influence trust.
- **Enhancing Sociological Models with Real-time Data:** We integrate real-time interaction data into sociological models, improving their applicability to dynamic online social networks where trust relationships evolve rapidly.
- **Incorporating Ethical Data Practices:** In response to concerns about privacy and data ethics in machine-learning models, our methodology emphasizes transparent and responsible data usage, ensuring that trust predictions are both accurate and ethically sound.

Moreover, while machine learning has advanced the analysis of trust by enabling the processing of large-scale data, these models often require substantial and sometimes invasive data collection, raising concerns about privacy and the ethical use of data. The predictive accuracy of these models can also vary dramatically depending on the diversity of the dataset and the dynamic nature of online interactions, which are continually evolving. This variability can lead to challenges in generalizing findings across different platforms or demographic groups. Additionally, much of the existing research has not thoroughly addressed the rapid evolution of online platforms and how these changes affect trust dynamics, leaving a gap in our understanding of these phenomena as they occur in real time.

These gaps underscore the need for ongoing research that not only adapts existing theories to the modern digital context but also develops new methodologies that can more accurately reflect the complex and evolving nature of trust online. Our study aims to fill some of these gaps by implementing advanced machine-learning techniques tailored to the unique characteristics of online social interactions, providing insights that are critical for the design of more trustworthy digital environments.

The incorporation of machine learning into trust analysis marks a significant advancement, transitioning from traditional sociological and psychological analyses to data-driven approaches. This shift, facilitated by the work of researchers like DuBois [16], employs vast datasets inherent to social networks, allowing for nuanced insights into trust relationships at scale. Techniques ranging from supervised learning to advanced methodologies like ensemble methods [17] and deep learning [18] have enhanced the capability to predict and understand trust dynamics within complex network structures, reflecting a major leap in quantifying and analyzing trust through algorithmic lenses.

Our research builds upon these foundations, employing a wide spectrum of machine-learning models to delve into trust dynamics within Facebook's social network. By exploring models ranging from KNN to Gradient Boosting, we aim to provide a comprehensive understanding of how trust forms and evolves online, addressing the nuanced nature of trust. This approach not only highlights the potential of leveraging machine learning for trust prediction but also sheds light on the challenges in digital trust analysis, such as data privacy and misinformation. As we contribute to the dialogue on digital trust, our work signals a call for multidisciplinary research, integrating insights from technology, social sciences, and ethics to unravel the complexities of trust in our interconnected world.

### 3. Methodologies for Trust Prediction in Social Networks

In addressing the unique challenges of predicting trust in unstructured social media data, we have adapted conventional machine-learning models to better suit the complex and dynamic nature of our dataset. These adaptations include advanced feature engineering to capture contextual and temporal dynamics, tailored hyperparameter tuning to manage high-dimensional data, and customized validation techniques to ensure robust model evaluation. This section details the specific modifications made to each model, highlighting our methodological innovations that enhance their predictive accuracy and relevance to social media analytics.

Although various state-of-the-art machine-learning methods have been demonstrated to be effective in the domain of trust prediction, this paper specifically addresses gaps in

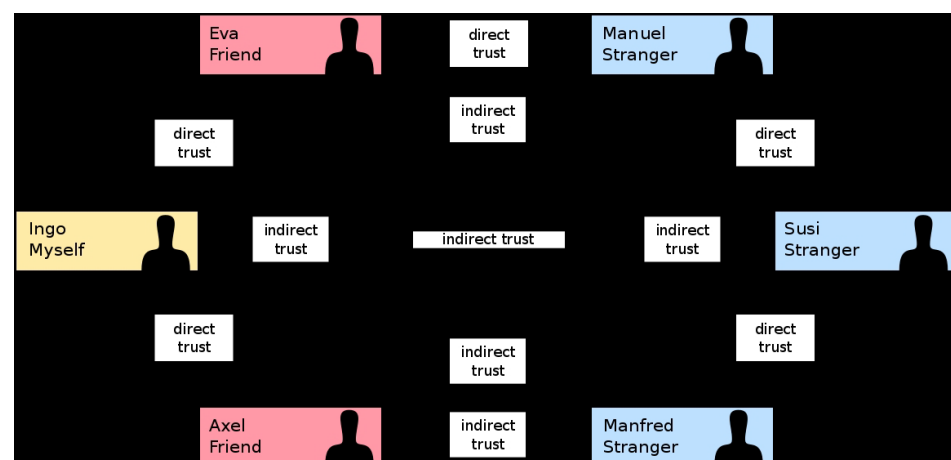
adapting these technologies to dynamic trust scenarios in social networks. Unlike existing approaches that often rely on static snapshots of data, our methodologies are uniquely tailored to capture and analyze the evolving nature of trust as interactions occur over time. We introduce modifications to traditional models to handle temporal data, enabling them to adapt to the changing landscape of social interactions and trust relationships. Furthermore, we integrate ensemble methods and deep learning techniques to improve the robustness and accuracy of trust predictions in dynamic social environments, addressing the limitations of overfitting and underfitting in rapidly changing data contexts.

### 3.1. Graph-Based Prediction Models

Graph-based models are fundamental in the realm of trust prediction within social networks, leveraging the Web of Trust (WoT) and Friend of a Friend (FOAF) concepts to intricately map the web of interpersonal relationships. These models conceptualize the social network as a graph, with individuals represented as nodes and the trust relationships between them depicted as edges. This graphical representation aids in the intuitive understanding of the complex network of trust among users, providing a clear visual framework to analyze the intricacies of interpersonal connections and trust dynamics.

Despite their utility, graph-based models often presuppose that each individual operates within a well-defined network of trust. This assumption may not accurately reflect the diverse and fluid landscapes of online communities, where trust networks can be sparse or even non-existent for some users. These scenarios challenge the models' effectiveness, highlighting a gap between the idealized representations of trust networks and the actual, often fragmented, trust landscapes encountered in digital environments. Nevertheless, the trust propagation and inference mechanisms these models employ are crucial for predicting trust relationships, especially in contexts where direct connectivity between users is limited [19].

Figure 1 vividly illustrates the Web of Trust concept, emphasizing how trust relationships serve as the threads that connect users within the tapestry of a social network. This visualization is instrumental in showcasing the models' capability to encapsulate the dynamics of trust among users, providing a visual narrative that highlights both the density and the complexity of trust networks. The depiction of users as nodes interconnected by trust relationships (edges) not only brings to light the structural aspects of trust networks but also underscores the potential of graph-based models to explore and analyze the multi-faceted nature of trust within online communities. Through this figure, the abstract concept of the Web of Trust is rendered tangible, offering a compelling illustration of how trust permeates through the network, binding users together in a complex web of relationships that underpin the social fabric of online platforms.



**Figure 1.** Illustration of the Web of Trust concept, depicting users as nodes connected by varying colors and sizes of links that represent different levels and types of trust relationships.



Within the evolving landscape of trust prediction methodologies, various innovative approaches have significantly expanded our understanding and capability to infer and model trust within social networks. The Friend of a Friend (FOAF) concept, for example, is instrumental in extrapolating trust between users by identifying contexts or topics that underlie trust relationships, highlighting the role of shared interests and connections in trust formation [20]. This approach to trust prediction underscores the importance of contextual relevance in the establishment of trust.

A notable strategy highlighted in [21] suggests that individuals are more inclined to trust recommendations from their direct connections, emphasizing the critical role of immediate social ties in trust-based decisions. This insight into the mechanics of trust underscores the significance of proximal relationships within the digital domain, where the physical cues of trustworthiness are absent.

Further advancements in trust modeling, such as the incorporation of implicit user feedback into trust network construction, offer a nuanced view of how interactions contribute to trust dynamics [5]. The TidalTrust algorithm leverages the concept of trust transitivity to infer trust levels among users, suggesting a model where trust between indirectly connected individuals can be estimated based on mutual connections' trust ratings [22].

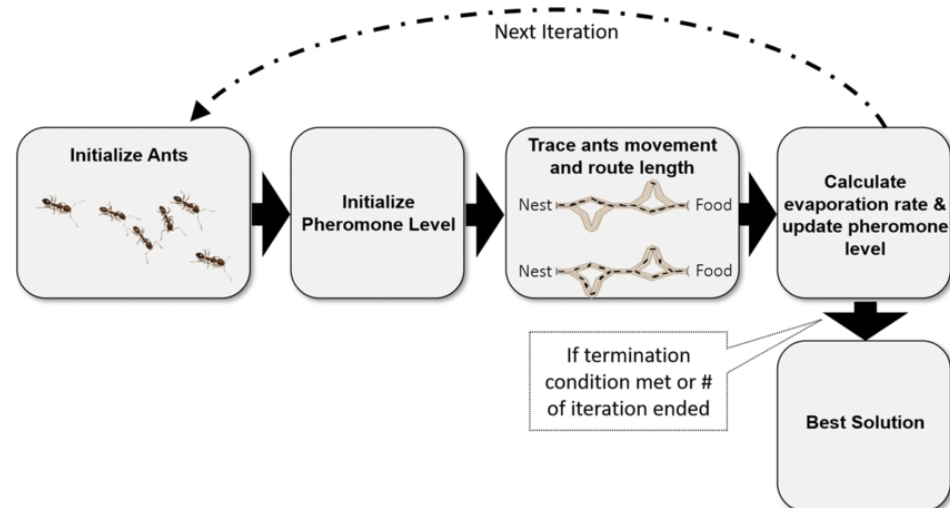
Progressing beyond the examination of individual trust connections, the development of network-based trust prediction models like Appleseed introduces a sophisticated approach to trust analysis, particularly in its application to the Semantic Web [23]. These models refine the trust prediction process by focusing on trust assessments within specific user groups, offering a detailed examination of trust dynamics at a granular level. Additionally, evaluating the similarity of user trust networks, treating the challenge of recommendation as a graph similarity issue, further enhances the precision of trust predictions by examining the structural intricacies of trust networks [22].

The exploration of trust through trust chains and graphs adds a complex layer to trust prediction, enabling the computation and assessment of trust levels across extensive networks. The utilization of a trust certification graph as a structural guide for assessing trust relationships marks a significant advancement in understanding the architecture of trust networks [24].

SocialTrust introduces a refined approach to trust prediction by weighting user feedback through algorithms akin to Google's PageRank, integrating social interactions into the evaluation of trust [25]. Additionally, semantic trust inference mechanisms leverage ontology design and role-based reasoning to distill trust relationships based on category-specific trust dynamics [7].

Heuristic algorithms for trust network discovery, emphasizing social context awareness, represent innovative strategies to navigate and uncover trust networks within the complexities of social interactions, enhancing the accuracy of trust predictions through context-aware structures [21].

Within this spectrum of methodologies, recommendation systems that utilize matrix factorization models have become increasingly popular, shifting the focus towards item recommendation rather than mere score prediction [26]. Additionally, collaborative filtering systems that incorporate the Ant Colony Optimization (ACO) algorithm represent a notable advancement in leveraging social trust for recommendation purposes [27]. In these systems, users are evaluated based on the trust relationships within their network, with the ACO algorithm being employed to assign weights and assess similarity levels among users. This approach not only enhances the personalization of recommendations but also underscores the integral role of trust in shaping user interactions and preferences, as depicted in Figure 2.



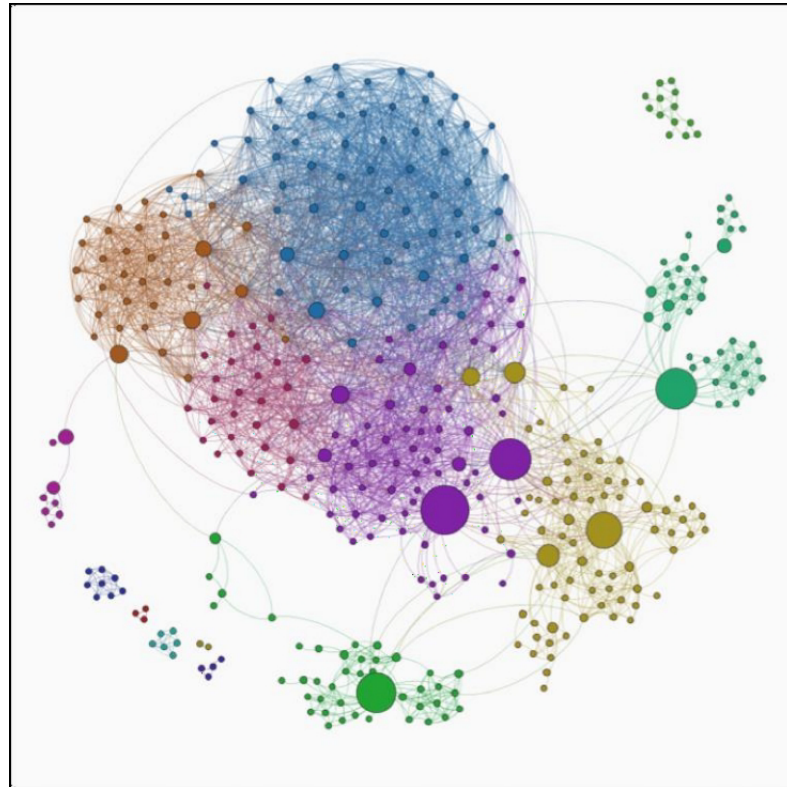
**Figure 2.** Application of the Ant Colony Optimization (ACO) algorithm for leveraging social trust in recommendation systems.

The domain of trust prediction continues to evolve, incorporating a diverse array of methodologies that enrich the analysis and modeling of trust within social networks. One notable approach, TrustRank, adapts the PageRank algorithm to specifically assess the trustworthiness of nodes in a social network. By distributing trust scores across connections, TrustRank provides a systematic way to evaluate the trust landscape within digital communities [28]. Building on this foundation, local trust propagation methods refine TrustRank’s approach by focusing on the immediate trust dynamics between users. These methods adjust trust ratings based on the perceived trustworthiness of adjacent users, offering a more granular perspective on trust within the network [29].

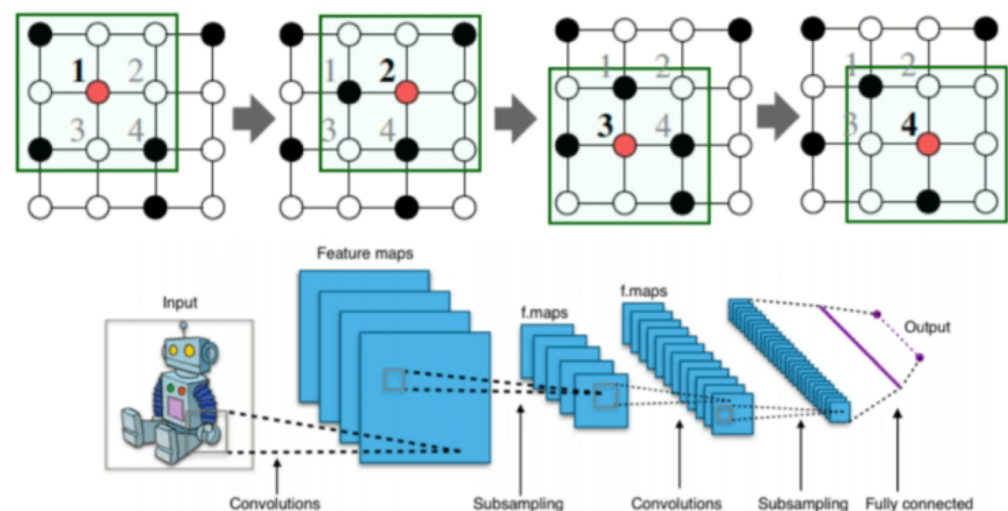
Further enhancing trust prediction, the analysis of social influence considers the impact of user interactions and the extent to which individuals influence each other’s trust decisions within the network. This approach leverages social influence metrics to inform trust assessments, recognizing the powerful role of social interactions in shaping trust perceptions [30].

Additionally, the identification of user communities within social networks marks a crucial advancement in trust prediction [31]. By targeting groups with shared interests or characteristics, these methods enable a nuanced estimation of trust levels within specific communities. This strategy leverages the collective reputation and perceived trustworthiness of community members to assess trust, as vividly illustrated in Figure 3. This visualization captures the essence of communal trust assessment, highlighting how shared traits and interests within communities can inform and refine trust evaluations.

The integration of Convolutional Graph Neural Networks (CGNNs) signifies a groundbreaking development in trust prediction models [32]. By employing deep learning techniques, GCNNs effectively learn node representations by analyzing the structure and connectivity patterns within the network. This sophisticated modeling approach significantly enhances the accuracy and depth of trust predictions, as depicted in Figure 4. Here, the application of GCNNs demonstrates their potential to capture and analyze complex trust relationships, offering insights into the structural and relational nuances of trust networks.



**Figure 3.** This graph illustrates the complexity of trust interactions within a network, using circles of varying colors and sizes to represent different user groups and trust intensities. Each color signifies a distinct trust group, while the size indicates the group's influence or trust level within the network, offering insights into how trust propagates in social media settings.



**Figure 4.** Application of Convolutional Graph Neural Networks (GCNN) in the modeling of trust relationships within a social network [33].

Complementary to GCNNs, trust-based random walks present a dynamic methodology for exploring trust across networks. This technique simulates the diffusion of trust through network graphs using random walks, estimating nodes' trustworthiness based on visit frequency. This approach offers a probabilistic perspective on trust distribution and influence, providing a novel lens through which to view and analyze trust dynamics across extensive social networks [34].



### 3.2. Prediction Models Based on Interactions

Trust prediction models grounded in user interactions employ a variety of approaches to decode the intricacies of engagement within social networks [2,4]. These methodologies offer a nuanced exploration of trust dynamics, emphasizing the role of direct and indirect interactions in trust formation and evolution:

- **Dissemination of Trust:** This strategy posits that trust, much like information, proliferates through social connections. It is based on the observation that users are likely to develop trust following positive interactions. Techniques such as random walks, matrix factorization, and graph-based methods are utilized to disseminate trust scores across the network. This diffusion process relies on user interactions as a primary source for mapping the trust landscape, suggesting that trust can be quantitatively spread and measured throughout the social fabric.
- **Collaborative Filtering:** Traditionally pivotal in recommender systems, collaborative filtering finds a parallel application in trust prediction by scrutinizing patterns of user interactions. It pinpoints trust relationships by matching users with analogous interaction patterns, effectively using the aggregated experiences of similar users as a proxy to infer trust connections. This method capitalizes on the premise that shared behaviors and preferences can serve as a basis for establishing trust.
- **Patterns of Interaction:** This approach zeroes in on the qualitative aspects of interactions, such as frequency, recency, sentiment, and consistency, to unearth potential indicators of trust. Advanced machine-learning models, including decision trees, support vector machines, and neural networks, are deployed to analyze these interaction attributes and predict trust relationships. By focusing on the depth and nature of user engagements, this method aims to extract trust signals from nuanced behavioral patterns.
- **Temporal Dynamics:** Acknowledging the fluidity of trust, this model incorporates both the current and historical context of interactions to understand trust evolution. It examines the stability and variations in trust levels over time, offering insights into how trust relationships develop, wane, or persist. This dynamic approach to trust prediction recognizes that the significance of interactions can change, providing a comprehensive view that encompasses the temporal dimension of user relationships.

The efficacy of these interaction-based models is contingent on several factors, including the specific features of the social network, the richness of the interaction data, and the goals of the trust prediction endeavor. Hybrid models that integrate multiple interaction-based strategies or contextual data are gaining traction, seeking to bolster the precision and applicability of trust predictions.

Contrasting with graph-based models, which may not fully capture the depth of genuine user interactions, interaction-based models prioritize the analysis of direct engagements between users. Initial research highlighted the potential of categorizing trust prediction models based on user behaviors and interactions [35]. Subsequent studies have introduced nuanced models that distinguish between the trust a community places in an individual versus the trust an individual has in the community [36], and methods that focus on communication patterns, such as conversation trust, which evaluates the frequency and duration of interactions [37]. Another approach quantifies subjective trust values among connected users based on their social engagements [38], underscoring the critical role of direct interactions in revealing trust indicators that structural analyses might overlook.

### 3.3. Hybrid Prediction Models

Hybrid trust prediction models represent a significant advancement in the field of trust prediction by synthesizing the insights derived from both the structural configurations and the interactional dynamics of social networks. By examining the intricate web of users' past interactions along with the overarching network architecture, these models endeavor to forecast trust relationships with a level of accuracy previously unattainable.

- **TDTrust Model:** The TDTrust model, unveiled by Ghafari in 2018, stands as a quintessential example of this hybrid methodology. It is designed to meticulously capture the multifaceted nature of trust relationships by amalgamating interaction data with insights into the network's structural aspects. This dual-focused approach aims at delivering predictions of trust relationships with a significantly enhanced level of precision, highlighting the model's ability to navigate the complexities inherent in trust dynamics [39].
- **Tensor Decomposition Approach:** Pushing the boundaries further, the tensor decomposition approach offers an innovative lens through which the trust framework is analyzed. Employing a three-dimensional tensor decomposition technique, this method paves the way for direct and structured exploration of trust relationships. It adeptly integrates various dimensions of user data and network structure into the analysis, providing a multifaceted approach to trust prediction that acknowledges the layered complexity of social interactions and network configurations.
- **SETTrust:** This model takes an unsupervised approach to trust prediction, weaving social exchange theory into the fabric of its methodology [40]. It operates on the foundational belief that trust relationships are essentially transactions where relationships burgeon when the perceived benefits surpass the costs involved. By embedding this cost-benefit analysis into its core, SETTrust offers profound insights into the mechanics of trust formation and sustainability within social networks.
- **Trust Link Detection System:** This system is specifically designed to navigate the nuanced terrain of subjective trust and reputation among users [41]. By calculating subjective trust based on historical interactions and gauging reputation through the aggregation of community-based trust evaluations, the system adopts a comprehensive approach to understanding trust relationships. This methodology acknowledges the importance of both individual user experiences and collective community perceptions in crafting a multi-layered picture of trust within social networks.

In essence, hybrid models, by marrying varied data sources and theoretical insights, afford a panoramic view of the trust landscape within social networks. They adeptly recognize that trust emanates from a confluence of factors—ranging from direct user interactions to the broader sociocultural context—therefore facilitating a more detailed and accurate prediction of trust relationships. Through this holistic approach, hybrid models not only advance the field of trust prediction but also enhance our understanding of the intricate interplay of elements that foster or diminish trust in digital social spaces.

### 3.4. Types of Prediction Algorithms

The section delves into the categorization of trust prediction algorithms into supervised and unsupervised methodologies, focusing on their distinct approaches to modeling and predicting trust within social networks.

#### 3.4.1. Supervised Methods

Supervised trust prediction models are pivotal in leveraging labeled data to train algorithms for accurate trust relationship forecasting. These methods utilize an array of features and sophisticated algorithms to derive trust insights from user attributes and interactions:

- **Attribute-Based Models:** Utilizing user attributes and interactions, these models apply classifiers to infer trust relationships. By analyzing demographics, profile characteristics, and textual content, they offer nuanced predictions of trust levels, emphasizing the importance of personal and behavioral data in trust assessment [35].
- **Cluster-Based Approaches:** By grouping users with similar attributes or interaction patterns, these personalized models enhance the specificity of trust predictions. Classifiers trained within these clusters provide tailored trust assessments, showcasing the value of segmentation in understanding trust dynamics [42].

- **Reputation-Focused Models:** Prioritizing user reputation, these models employ binary classification to evaluate and predict trust. By analyzing user ratings and interactions, they assess the impact of reputation on trust, highlighting the significance of community feedback in trust inference [43].
- **Hybrid Techniques:** Combining Dempster–Shafer theory with neural networks, these models improve trust inference through a blend of evidential reasoning and deep learning. This approach underlines the synergy between traditional belief theories and modern machine learning in enhancing trust prediction accuracy [44].
- **Feature-Rich Classifiers:** Employing classifiers with a broad spectrum of features, including demographics, profile details, and content analysis, these models aim to capture the complex dynamics of trust in social networks. They illustrate the importance of a multifaceted approach in accurately modeling trust relationships [45].
- **User-Rating Based Algorithms:** Focusing on user ratings on review platforms, these models infer trust relationships by highlighting the role of rating similarity. This approach underscores the predictive value of shared opinions and experiences in trust formation [46].
- **Graph-Based Feature Analysis:** Integrating graph-based features with user ratings, these studies employ decision tree algorithms for trust prediction. They demonstrate how combining structural network analysis with user feedback can enrich trust prediction models [47].
- **Multi-Class Classifier Framework:** Utilizing multi-class classifiers and integrating RESTful architecture and SVM techniques, this framework exemplifies the application of complex machine-learning strategies in social network trust prediction, highlighting the role of advanced classification methods [48].
- **Demographic-Focused Classifier:** The DCAT classifier, by incorporating demographic data and textual content analysis, focuses on enhancing trust prediction accuracy. This model reveals the predictive power of demographic information in trust assessment [40].
- **Time-Based Prediction Models:** Addressing trust prediction as a time-link problem, these approaches examine temporal interaction patterns to predict trust dynamics over time. They spotlight the importance of historical interaction data in forecasting trust evolution [49].
- **Trust Management Frameworks:** In pervasive computing environments, these models enable devices to evaluate the trustworthiness of others based on historical interactions, showcasing the application of trust prediction beyond social networks into device interactions [50].
- **Reputation Features Model:** Focusing on reputation features for supervised trust prediction, this probabilistic model addresses the initial trust establishment challenge, emphasizing the critical role of reputation in trust prediction [51].
- **Topic-Centric Trust Estimator:** Evaluating trustworthiness based on topic similarity measures on Twitter, this model highlights the role of content relevance in trust assessment, showcasing the importance of topical alignment in trust dynamics [52].
- **Multi-Dimensional Trust Prediction:** The CommTrust approach, evaluating trust based on user comments, addresses overly positive reputation issues. It underscores the complexity of trust inference and the need for multi-dimensional analysis in trust prediction [53].

While supervised methods offer detailed and robust trust inference capabilities, they contend with challenges such as data sparsity and the need for extensive labeled data sets, potentially limiting their effectiveness in rapidly changing social network environments.

### 3.4.2. Unsupervised Methods

Unsupervised trust prediction models, which do not rely on labeled data, infer trust relationships by identifying inherent patterns within the social network. These models apply various techniques for a dynamic and adaptive approach to trust prediction:

- **hTrust:** This model exploits homophily in trust prediction by identifying users with similar rating behaviors. It considers the similarity in items rated, rating values for similar items, and overall rating patterns to predict trust [54].
- **sTrust:** Leverages social state theory alongside the PageRank algorithm to prioritize users of higher social status as more trustworthy within the network. This model infers that social influence and status can be significant indicators of trustworthiness, providing a unique angle to trust prediction by incorporating the hierarchical structure of social interactions [55].
- **Trust Transfer Model:** Introduces the innovative concept of trust transference across different contexts, allowing trust established in one domain to inform trust predictions in another. This approach acknowledges the multifaceted nature of trust and its applicability across various scenarios, making it a versatile tool for trust prediction in diverse environments [56].
- **Trust-aware Recommendation Systems:** Addresses the challenge of enhancing the accuracy of rating predictions by constructing dynamic trust networks between users. By analyzing similarity values and trust declarations, this system adapts to the evolving nature of trust within social networks, therefore refining the quality of recommendations based on updated trust dynamics [57].
- **Trust-ACO:** Applies Ant Colony Optimization to delineate trusted paths and cycles within the network, focusing on identifying the most reliable routes for service discovery. This method combines probabilistic trust rules with an understanding of social familiarity, showcasing how optimization algorithms can be tailored to navigate the complexities of trust in social networks [58].
- **Social Trust-based Prediction:** Utilizes matrix factorization to explore the influence of established trust metrics on the prediction of pairwise trust relationships. This method systematically identifies which trust metrics are most indicative of accurate trust predictions, enhancing the precision of trust inference in social networks [59].
- **eTrust:** Concentrates on dynamic trust prediction for users on product review websites, employing matrix factorization techniques to model trust as it evolves through user interactions. This model is particularly adept at capturing changing trust dynamics, reflecting the transient nature of user preferences and trust over time [60].
- **Joint Multiple Factorization Method:** Investigates trust prediction as a link prediction challenge, using joint multiple factorization to assess similarities at the user group level across correlated graphs. This approach leverages the shared behaviors and tastes within social circles to predict trust, emphasizing the collective aspect of trust dynamics [61].
- **Feature Recognition-based Approach:** An unsupervised method that identifies key features associated with trust, aiding in the comprehension of how trust is formed and maintained within social networks. This approach highlights the importance of feature selection in understanding and predicting trust dynamics accurately [62].
- **Ranking System for User Reputation:** Evaluates trust through the lens of user reputation and social connections, offering a novel perspective on trustworthiness based on the aggregation of community-based reputation insights. This system provides a framework for assessing trust relationships by leveraging collective reputation data [63].
- **Trust-awareness for Personalized QoS:** Implements trust-awareness to optimize personalized Quality of Service (QoS) delivery. By measuring user reputation and identifying groups of similar trusted users, this approach tailors service delivery to align with the trust-based preferences of the user community, ensuring reliable and personalized service experiences [64].
- **Method for Correlation between Social Media and Financial Data:** Enhances the understanding of the correlation between social media activity and financial data, particularly in the stock market context. By analyzing Twitter data related to stocks,

this method identifies significant correlations that can inform investment and financial decisions, illustrating the broader applicability of trust and sentiment analysis [65].

- **Study on Trust Dynamics:** Delves into the computational modeling of distrust within social networks, offering insights into not just trust but also its counterpart, distrust. This research contributes to a more comprehensive understanding of trust dynamics, recognizing the importance of both trust and distrust in shaping social interactions [66].
- **Influence of Social Status on Trust:** Investigates how the perceived social status of users within a network affects trust relationships. This study provides valuable insights into the sociological aspects of trust, underscoring the impact of social hierarchy on trust formation and sustainability within social networks [67].

Unsupervised models, with their inherent flexibility and adaptability, are invaluable for predicting trust relationships across various contexts and dynamics within social networks.

As we explore the evolutionary trends in trust prediction, it is crucial to consider not only the technological advancements but also the ethical implications of deploying AI in social spaces. Future research could explore the integration of blockchain to ensure transparency and immutability in trust transactions or the role of AI ethics in managing bias in trust predictions. These directions could profoundly influence the design and functionality of future digital platforms, enhancing their capability to foster trusted environments.

## 4. Implementation

### 4.1. Data Preprocessing

Effective data preprocessing is a critical foundation for optimizing the performance of machine-learning models in trust prediction. This stage prepares the data for analysis, ensuring it is clean, relevant, and appropriately structured.

- **Exploratory Analysis and Cleaning:** Initial exploratory analysis is vital for understanding the dataset's characteristics, including identifying key variables that may influence trust, detecting anomalies, and discerning underlying patterns. Cleaning is a meticulous process that rectifies common data issues such as missing values, outliers, and inaccuracies, which, if left unaddressed, could skew the model's outcomes. Techniques like imputation for missing values or outlier detection and removal can significantly enhance data quality and reliability.
- **Feature Engineering and Selection:** This process involves the creation of new features that better encapsulate the nuances of trust within social networks, alongside the selection of the most impactful features. Effective feature engineering might include deriving new variables from existing data that highlight the frequency, recency, and type of interactions indicative of trust. Feature selection, possibly through methods like principal component analysis (PCA) or models with embedded feature importance evaluation, helps reduce the dimensionality of the data. This step is pivotal in concentrating the model's attention on the most informative aspects of the data, which can lead to improved prediction accuracy and model interpretability. We developed specialized features to better capture the dynamic nature of trust in social networks. These features include time decay functions for interaction metrics and sentiment aggregation over dynamic time windows tailored to the evolving context of social media data. These methods address the complexities of trust dynamics more effectively than conventional feature engineering practices.
- **Normalization and Encoding:** Normalizing numerical features ensures that all variables contribute equally to the model's decision process, preventing features with larger scales from dominating the prediction. Encoding categorical variables into a numerical format through techniques such as one-hot encoding or target encoding is crucial for incorporating these variables into machine-learning algorithms effectively. These steps are instrumental in preparing the data for analysis, ensuring compatibility with various machine-learning algorithms that require numerical input.



- **Dataset Division:** Properly dividing the dataset into training and testing sets or utilizing cross-validation techniques is essential for evaluating the model's performance accurately. This division guarantees that the model is both trained and assessed on different subsets of the data, offering an unbiased estimation of its predictive power. Techniques like k-fold cross-validation further enhance model evaluation by ensuring that every data point is used for both training and validation across different iterations, thereby providing a more comprehensive assessment of the model's generalization capabilities.

#### 4.1.1. Data Identification

The data identification phase is the critical first step in data preprocessing, where the dataset is thoroughly examined to understand its structure and key characteristics. This foundational analysis informs all subsequent preprocessing decisions.

- **Feature Analysis:** Involves examining feature types (e.g., numeric, categorical) and their distributions to determine their potential impact on model performance.
- **Handling Anomalies:** Focuses on identifying and addressing missing values, outliers, and other anomalies that could compromise the accuracy and reliability of the predictive models.

This stage is essential for laying the groundwork for effective data preprocessing, ensuring the dataset is optimally prepared for machine-learning model training and evaluation.

#### 4.1.2. Label Encoding

Transforming categorical variables into a machine-readable format is crucial in data preprocessing. This step is especially important in social networks, where categorical data often contains key insights into user demographics and interactions.

- **Integer Mapping:** Categorical values are transformed into integers, facilitating algorithmic processing by assigning a unique integer to each category.
- **Alternative Encodings:** One-hot encoding is considered to mitigate ordinal implications, creating binary columns for each category and ensuring that machine-learning models do not infer an unintended order among categories.

This encoding process ensures that the rich categorical information within the dataset is retained and effectively utilized in the subsequent modeling process.

#### 4.1.3. Data Formatting

Achieving uniformity in data format is essential for the compatibility and efficiency of machine-learning models. This step ensures that all data points are presented in a consistent format, facilitating model training and prediction accuracy.

- **Scaling Techniques:** The application of Min-Max scaling or Z-score normalization adjusts feature scales to a common range, crucial for models sensitive to feature magnitude.
- **Normalization:** Transforming skewed data distributions into more uniform or normal distributions enhances model performance by addressing data bias and variance issues.

Data formatting, by standardizing the scale and distribution of features, significantly contributes to the model's ability to learn from the data effectively.

#### 4.1.4. Dataset Splitting

Dataset splitting is a pivotal step in preparing data for machine learning, crucial for both training models and evaluating their performance accurately.

- **Training Set Utilization:** The training set plays a key role in model development, offering a diverse array of examples from which the model learns. The breadth of the training data directly impacts the model's ability to understand and predict complex trust relationships, with larger datasets typically leading to better generalization.

- **Testing Set Evaluation:** The testing set is essential for objectively assessing the model's effectiveness on unseen data. This independent evaluation ensures that the performance metrics accurately represent the model's predictive capabilities in real-world scenarios.

A strategic approach to dataset splitting enhances model training, evaluation, and the overall reliability of trust predictions within social networks.

#### 4.2. Machine-Learning Algorithms

The task of predicting trust levels in social networks, particularly the strength of interpersonal bonds, is intricate due to the complex dynamics of trust. Each machine-learning algorithm brings distinct advantages to this challenge, suited for different aspects of trust prediction. Here is a detailed analysis of the selected algorithms:

- **Logistic Regression:** This model excels in situations where the relationship between the trust level and the features is approximately linear. Its transparency and simplicity make it ideal for initial analyses, providing clear insights into how each feature influences the likelihood of trust.
- **K-Nearest Neighbors (KNN):** KNN's instance-based learning is particularly effective for trust prediction in densely connected social networks. It can adaptively infer trust levels based on the similarity and proximity of users, capturing local patterns within the network's structure.
- **Random Forest:** By aggregating decisions from multiple trees, Random Forest mitigates the risk of overfitting, making it robust across diverse data distributions. Its ensemble nature allows it to handle the complexity and non-linearity of trust relationships, offering detailed insights into feature importance.
- **Extra Trees:** Similar to Random Forest but with added randomness in feature selection, Extra Trees can uncover more subtle trust signals within the data. This approach is particularly beneficial when traditional feature selection methods might overlook intricate patterns indicative of trust.
- **Support Vector Machine (SVM):** SVM's capacity to find the optimal hyperplane for class separation makes it adept at distinguishing between varying levels of trust. Its kernel trick allows for modeling complex, non-linear trust relationships that might be present in social networks.
- **Naive Bayes:** This probabilistic model, with its assumption of feature independence, is especially suited for text-based user interaction analysis. It can efficiently process large volumes of text data, such as user comments or messages, to predict trust based on communication patterns.
- **AdaBoost:** By focusing iteratively on challenging instances, AdaBoost refines the model's ability to predict trust in ambiguous or borderline cases. This adaptive boosting of weak learners is valuable for enhancing model performance in predicting nuanced trust levels.
- **Decision Tree:** Decision Trees offer a straightforward visualization of how different features contribute to trust predictions. The model's hierarchical structure mirrors decision-making processes, making it intuitive for understanding trust determinants.
- **Gradient Boosting:** This technique sequentially corrects errors from previous models, making it highly effective for complex datasets with intricate trust dynamics. Gradient Boosting's iterative refinement is key for achieving high accuracy in trust-level predictions.
- **Neural Networks:** With their deep learning capabilities, Neural Networks are unparalleled in modeling the intricate and abstract patterns of trust within social networks. Their layered architecture enables the capture and analysis of complex relationships and interactions that define trust levels.

Each of these algorithms offers a toolkit for tackling the multifaceted nature of trust prediction in social networks, with choices often dictated by the specific characteristics of

the dataset, the complexity of trust relationships, and computational considerations. The selection and application of these models necessitate a balanced consideration of accuracy, interpretability, and computational efficiency to effectively model and predict trust levels within social networks.

#### *4.3. Performance Evaluation and Experimental Procedure*

##### *4.3.1. Performance Evaluation*

The effectiveness of machine-learning models in predicting trust relationships was meticulously assessed using a range of key metrics: confusion matrices, accuracy, precision, recall, and F1-score. These metrics provided a comprehensive view of model performance, revealing strengths and areas needing improvement in predicting trust dynamics within social networks. A notable consideration in this evaluation was the balance between precision and recall, highlighting the need for a nuanced approach in model selection based on specific trust prediction requirements.

Evaluating model performance extends beyond numerical scores; it involves understanding the balance between metrics such as precision and recall, which can reflect differing priorities in trust prediction contexts. For instance, a model with higher precision but lower recall might be preferred in applications where falsely predicting trust is more detrimental than missing potential trust relationships. This nuanced view helps in tailoring model selection to the specific requirements of trust prediction tasks in social networks.

##### *4.3.2. Experimental Procedure*

The experimentation phase was characterized by a rigorous exploration of the parameter space for each machine-learning model, with a special focus on neural networks due to their complex architectures. Automated tuning techniques like grid search and Bayesian optimization were employed to efficiently identify optimal configurations, significantly impacting the models' ability to accurately predict trust. This iterative process of parameter optimization was crucial in refining the models' sensitivity to the subtle cues indicative of trust relationships within the web of social interactions.

The parameter tuning process, particularly for complex models like neural networks, presented significant challenges due to their deep architectures and vast parameter space. Navigating this space to find optimal configurations required a meticulous approach, often employing automated tuning techniques like grid search or Bayesian optimization. These methods proved instrumental in identifying parameter settings that significantly enhanced model performance, showcasing the critical role of systematic parameter optimization in trust prediction.

Our parameter tuning approach utilizes a hybrid method combining grid search and evolutionary algorithms, specifically adapted to the challenges of social media data. This adaptive tuning process is designed to optimize model parameters dynamically, accommodating the fluid characteristics of trust interactions in online environments.

A comparative analysis against existing trust prediction implementations provided valuable insights into the relative strengths and proposed innovative strategies for enhancing trust prediction methodologies. This benchmarking exercise was instrumental in advancing the domain, offering a broader perspective on state-of-the-art methodologies and highlighting future innovation areas.

##### *4.3.3. Implementation Tools*

The practical implementation of this study leveraged Python and the Anaconda Spyder IDE, utilizing libraries such as pandas for data manipulation, matplotlib for visualization, scikit-learn for machine learning, and keras for neural networks. These tools were chosen for their robustness and the specific features they offer that support trust prediction research, such as scikit-learn's machine-learning algorithms and keras's deep learning frameworks. Despite facing challenges like handling large datasets and optimizing training times, strategies like data chunking and parallel computing enabled effective management

and utilization of these tools, ensuring a seamless research workflow and reproducibility of results.

## 5. Experimental Evaluation

This section presents a comprehensive and comparative evaluation of machine-learning models developed to predict trust levels within social networks. Our analysis spans one specific dataset to provide a broad perspective on the models' predictive capabilities. This dataset, from Facebook, delves into the dynamics of social ties, exploring their impact on users' mental well-being and the nature of communication within Facebook friendships.

The effectiveness of the models across these datasets is quantitatively assessed using a suite of key performance metrics: accuracy, precision, recall, and F1-score. Each metric sheds light on different facets of the models' performance:

- **Accuracy:** Offers a general measure of the models' overall performance by calculating the proportion of correctly predicted instances.
- **Precision:** Assesses the models' ability to correctly identify positive instances, crucial for minimizing false positives in trust prediction.
- **Recall (Sensitivity):** Measures the models' capability to capture all relevant instances, emphasizing the importance of minimizing false negatives.
- **F1-Score:** Provides a balanced metric that harmonizes precision and recall, serving as a critical measure for evaluating the models' efficiency in predicting trust levels accurately.

Through the detailed scrutiny of these metrics, this evaluation aims to offer valuable insights into the strengths and weaknesses of each machine-learning model in capturing the nuanced dynamics of trust relationships within social networks. By comparing the models' performance across the Facebook dataset, this section elucidates their efficacy and applicability in diverse social media environments, highlighting areas where models excel or fall short in the complex task of trust prediction.

Given the challenges associated with establishing a concrete ground truth in trust dynamics within social networks, these metrics are calculated based on a derived ground truth, which integrates both observed user behaviors and expert annotations.

The derivation of ground truth involves:

- **User Behaviors:** Quantitative data from user interactions (likes, comments, shares) that imply trust are used to label data points as 'trusted' or 'not trusted'.
- **Expert Annotations:** Subject matter experts provide labels for a subset of data, which helps in calibrating the trust inference model, particularly in ambiguous cases.

In our experiments, we utilize established machine-learning models; while these methods are commonly used, the novelty in our research lies in the custom adaptations made to effectively address the challenges posed by unstructured social media data, which is central to trust analysis in online social networks.

The following adaptations highlight how we tailored standard approaches to fit the unique requirements of our trust prediction study:

### 1. Feature Engineering:

- **Contextual Relevance:** We adapted feature selection to emphasize contextually relevant information extracted from user interactions, which are critical for assessing trust. This includes linguistic cues and patterns of communication that standard models might not prioritize without domain-specific adjustments.
- **Temporal Dynamics:** Understanding that trust dynamics evolve over time, we incorporated temporal features that capture changes in user behavior and interaction frequency, which standard applications of these models might overlook.

### 2. Model Customization:

- **Hyperparameter Tuning:** We specifically tuned the model parameters to handle the sparse and high-dimensional nature of social media data, which differs significantly from the structured datasets these models typically handle.

- Bias-Variance Tradeoff Adjustments: Given the noisy nature of social media data, adjustments were made to the complexity of the models to optimize for the bias-variance tradeoff, enhancing their predictive performance on this particular type of data.
3. Validation Techniques:
- Stratified Sampling: To address the non-uniform distribution of trust indicators across the dataset, we used stratified sampling techniques in our cross-validation process to ensure that each fold is representative of the overall dataset.
  - Performance Metrics Adjustment: We selected and adjusted performance metrics that are particularly suited to the uneven class distributions and the specific nuances of trust prediction in social media contexts.

To ensure the robustness and applicability of our models, we employed advanced cross-validation techniques tailored to the specifics of social network data. We implemented stratified and time-series cross-validation to handle the non-i.i.d nature of our data, enhancing the reliability of our findings and ensuring that our models are validated against realistic scenarios of social media interactions.

### 5.1. Exploring Mental Well-Being through Facebook Interaction Analysis

#### 5.1.1. Dataset

This study employs a dataset derived from Facebook user interactions to explore the implications of social ties on mental well-being [68]. These data are pivotal as they reflect the dynamic and complex nature of interpersonal relationships within a digital context, providing a unique lens through which we can analyze psychological health influences.

The dataset includes a variety of interaction metrics such as message exchange frequency, comment interactions, wall posts, and emotional tone analysis of communications, which are critical for understanding the depth and quality of social ties [69–71]. By analyzing these data points, the developed predictive model assesses the strength of these ties and correlates them with indicators of psychological well-being. This allows for a nuanced exploration of how robust social connections enhance or deteriorate mental health, offering insights into the preventive or aggravating factors of mental health issues in digital social settings.

Moreover, the dataset's comprehensive nature enables the examination of both direct and indirect interactions, providing a holistic view of an individual's social network influence on their mental state. This is essential for developing targeted interventions that could potentially mitigate mental health risks associated with weak or negative social ties on platforms like Facebook.

#### 5.1.2. Potential Applicability to Other Datasets

Our study has tailored machine-learning models specifically for a single dataset to deeply analyze trust dynamics within an online social network. The methodologies, particularly in feature engineering and model adaptation, are designed with general principles that can be adapted to other datasets. These include the capability to capture temporal dynamics and contextual nuances, which are prevalent in various social media environments. Adjustments could be made to accommodate different data structures or user interaction patterns found in other social networks or digital communities. This flexibility allows the proposed methods to be potentially applicable in a broader context, albeit with necessary modifications to suit specific data characteristics.

#### 5.1.3. Ground Truth Justification

In our study, the ground truth for trust relationships is derived based on a combination of user interactions and publicly available data from social networks. We understand the critical importance of robust ground truth data for validating the effectiveness of machine-



learning models in predicting trust. To this end, our ground truth is constructed through the following methods:

- **User-Generated Data:** Trust labels are assigned based on user interactions such as likes, comments, and shares, which are indicative of positive trust indicators in social dynamics.
- **Expert Annotations:** For a subset of data, trust labels are corroborated by expert reviewers familiar with the context and dynamics of the social network, ensuring that the trust definitions align with practical user experiences.
- **Consistency Checks:** We apply consistency checks across different data points to validate the reliability of the trust definitions, enhancing the integrity of our ground truth.

We recognize the limitations associated with manually defined ground truths and are committed to continuously refining our data collection and validation methods. Future iterations of our research will explore the integration of more automated and objective measures to establish ground truth, potentially through real-time feedback mechanisms and enhanced user engagement analytics.

By employing these methods, we aim to provide a sufficiently reliable basis for evaluating our machine-learning models, ensuring that our findings contribute meaningful insights into trust dynamics within online social networks.

#### 5.1.4. Data Points Utilized

The predictive model incorporates diverse data points to map the intricacies of social interactions, including:

- Exchange frequency of messages and comments
- Posting activity on each other's walls
- Emotional positivity in received messages
- Use of words expressing familiarity
- Time elapsed since the last interaction

#### 5.1.5. Attachment Strength Calculation

To quantify the attachment strength between individuals on Facebook, we employ a formula based on established psychological and sociological research that correlates various dimensions of online interactions with users' mental well-being [68]:

$$\begin{aligned} \text{Attachment Strength} = & -0.76 \times (\text{Number of days since last communication}) + \\ & + 0.111 \times (\text{Number of words expressing intimacy}) + \\ & + 0.135 \times (\text{Degree of positive emotions}) + \\ & + 0.299 \times (\text{Number of wall posts}) + \\ & + 0.299 \times (\text{Number of messages}) + \\ & + 0.299 \times (\text{Number of comments}) \end{aligned} \quad (1)$$

This formula incorporates communication frequency, emotional content, and the visibility of interactions to assess the strength of Facebook ties and their correlation with users' mental well-being. The coefficients in the formula were derived from empirical studies that quantitatively assess the impact of specific types of interaction on perceived social support and relationship quality. For instance:

- $-0.76$  for days since last communication emphasizes the decline in relationship strength over time without interaction, highlighting the importance of recent engagements.
- $0.111$  and  $0.135$  for words expressing intimacy and positive emotions, respectively, underscore the significant impact of emotional depth and positivity in maintaining strong social bonds.

- 0.299 for active interaction metrics (wall posts, messages, comments) reflects their role in sustaining and enhancing visible and frequent engagement, essential for robust social ties.

These coefficients were selected based on regression analysis outcomes that showcase how different interaction dimensions contribute to relationship strength in social networks.

#### 5.1.6. Model and Results

The Logistic Regression model was utilized to predict the strength of these bonds. The execution yielded significant insights, as presented in Table 1, triggering the implementation of our experimental procedures:

**Table 1.** Facebook Data Analysis: Social Ties and Mental Well-being.

ID	Days Since Being Friends	Comment Frequency	Post Frequency	Number of Messages	Vader Positivity	Days Since Last Communication	Attachment Strength
ID1	1900.041667	0	1	0	0	1900.041667	1
ID2	805.583333	1	0	797	0.18654	344.541667	0.897659
ID3	1685.541667	3	0	599	0.22022	483.625000	0.770177
ID4	1561.208333	6	0	575	0.23542	1017.625000	0.751014
ID5	1902.375000	95	0	0	0	1902.375000	0.666496
ID6	1913.958333	8	0	0	0	1913.958333	0.179817
ID7	1558.750000	5	0	0	0	1558.750000	0.179773
ID8	1323.875000	3	0	0	0	1323.875000	0.179653
ID9	1561.500000	5	0	0	0	1561.500000	0.179644
ID10	969.541667	0	0	0	0	969.541667	0.179568

The dataset derived from this experiment, capturing the essence of Facebook social interactions, serves as a valuable input for our subsequent experimental analysis. This approach underscores the potential of social media data to reflect aspects of mental well-being, guided by the strength and nature of online social ties.

Within our dataset, instances where ‘Post Frequency’ and ‘Number of Messages’ are zero indicate user pairs that did not engage in direct messaging or public posting activities during the observation period. However, these zeroes are significant as they represent a type of social tie characterized by passive interactions or connections where interactions may occur through other channels not captured by these specific metrics, such as likes or views. This understanding is crucial for analyzing the broader spectrum of social interactions that contribute to the overall strength of social ties and mental well-being. These zero-entry instances are included in our analysis to provide a comprehensive view of the diverse interaction patterns within the network, ensuring that our trust prediction models and insights reflect the full range of user behaviors observed on the platform.

#### 5.2. Performance Evaluation of Predictive Models

Table 2 provides a consolidated evaluation of the machine-learning models used to predict trust levels in social networks, detailing their performance across four key metrics: accuracy, precision, recall, and F1-score. These metrics are critical in assessing the overall effectiveness of the models, providing insights into their capabilities to accurately and efficiently predict trust among users.

**Accuracy Analysis:** KNN, Random Forest, and Gradient Boosting exhibit superior accuracy, suggesting their effectiveness in capturing the complex patterns of trust within social networks. The high accuracy of KNN (0.93) can be attributed to its ability to form localized decision boundaries, which is crucial in the nuanced domain of trust prediction. Conversely, Gaussian Naive Bayes demonstrates the lowest accuracy (0.55), likely due to its assumption of feature independence, which may not hold in the interdependent contexts of social networks.

**Table 2.** Performance Metrics.

Model	Accuracy	Precision	Recall	F1-Score
KNN	0.93	0.92	0.96	0.94
Random Forest	0.91	0.89	0.93	0.91
Gradient Boosting	0.91	0.89	0.93	0.91
ADABOOST	0.90	0.86	0.96	0.91
SVM	0.89	0.85	0.96	0.90
Extra Trees	0.87	0.86	0.89	0.87
Decision Tree	0.86	0.83	0.89	0.86
Logistic Regression	0.80	1.00	0.60	0.75
Neural Networks	0.80	1.00	0.60	0.75
Gaussian Naive Bayes	0.55	0.75	0.14	0.23

**Precision Analysis:** Logistic Regression and Neural Networks achieved perfect precision scores (1.0), highlighting their precision in identifying genuine trust relationships. This result for Neural Networks, in particular, underscores the models' capacity to leverage complex feature interactions, enhancing the precision of trust predictions. Gaussian Naive Bayes shows the lowest precision (0.75), reinforcing the challenges it faces in the nuanced trust prediction landscape.

**Recall Analysis:** KNN, SVM, and AdaBoost achieve the highest recall scores (0.96), indicating their robustness in comprehensively detecting trust instances across the dataset. This suggests that models with flexible decision boundaries, such as SVM, are particularly adept at capturing the varied manifestations of trust. The significantly lower recall of Gaussian Naive Bayes (0.14) further highlights its limitations in effectively capturing trust relationships.

**F1-Score Analysis:** KNN stands out with the highest F1-score (0.94), confirming its efficacy in balancing both precision and recall in trust prediction. This metric further differentiates models like Gradient Boosting and AdaBoost, which exhibit strong performance across both precision and recall, indicating their capability to manage the tradeoff between identifying relevant trust instances and minimizing false trust predictions.

### 5.3. Case Studies of Trust Relationships Identified by Machine-Learning Models

In our analysis, machine-learning models have demonstrated the capability to autonomously detect and learn from dynamic trust relationships within the social network. Below are case studies that highlight specific instances where our models have successfully identified meaningful trust dynamics:

#### 1. Case Study 1: Detection of Influential Trust Hubs

- **Background:** Utilizing the graph-based analysis, our models identified central nodes within the network, which were verified as influential trust hubs based on their high engagement and frequent interactions.
- **Model Insights:** The model leveraged user engagement metrics such as frequency of interactions and the breadth of user connections to pinpoint these hubs.
- **Outcome:** This identification helps in understanding how trust propagates through the network and the roles these hubs play in disseminating information and influencing community trust levels.

#### 2. Case Study 2: Recovery of Trust Post-Misinformation

- **Background:** After an incident of misinformation, our models were able to track the recovery of trust levels among users by analyzing changes in interaction patterns over time.
- **Model Insights:** By applying time-series analysis, the models observed gradual increases in positive interactions, signaling a restoration of trust.

- Outcome: This case study demonstrates the model's ability to not only detect disruptions in trust but also to monitor the recovery phase, offering valuable insights for managing trust in digital communities.

These examples underscore the practical applications of our machine-learning approaches in automatically learning and adapting to the nuances of trust dynamics within social networks.

#### 5.4. Discussion

The detailed evaluation underscores the nuanced capabilities of various models in predicting trust within social networks. KNN's consistent performance across all metrics highlights its adaptability and comprehensive capture of trust dynamics, suggesting that instance-based learning is particularly suited to the multifaceted nature of trust. The challenges faced by Gaussian Naive Bayes across metrics underscore the importance of model selection, emphasizing that assumptions inherent in certain models may not align with the complexities of social trust.

Moreover, the perfect precision achieved by Logistic Regression and Neural Networks, despite their varied accuracy and recall, points to the importance of understanding model-specific strengths and weaknesses in relation to the prediction task. The ability of models like Random Forest and Gradient Boosting to maintain high performance across metrics illustrates the value of ensemble methods in addressing the intricacies of trust prediction.

The findings of this study illuminate the critical role of tailored algorithmic approaches in trust prediction within social networks. The contrasting performances, particularly the strengths of KNN and the weaknesses of Gaussian Naive Bayes, provide valuable insights for future research directions, emphasizing the need for models that can navigate the complex, interconnected patterns of trust relationships.

This enriched discussion provides a deeper understanding of how each algorithm fares in trust-level prediction within social networks, emphasizing the importance of selecting the right model based on the specific characteristics and challenges of trust prediction tasks. The inclusion of numerical values alongside a thorough analysis offers a comprehensive view that is crucial for informing future advancements in the field.

#### 5.5. Methodological Reflections and Limitations

This study employs traditional data processing techniques and established machine-learning models, which, while robust and well-understood, may not fully capture the complex and evolving dynamics of social networks specific to trust prediction. Recognizing these limitations is crucial for advancing the field and guiding future research directions.

Traditional machine-learning methods, such as those used in this study, often rely on static snapshots of data that may not adequately reflect the temporal and relational complexities inherent in social networks. Social networks are dynamic, with evolving relationships and trust dynamics that can change over short periods. Future research could benefit from employing methods that capture these dynamics more effectively, such as temporal network analysis or models that account for changing network topology.

Moreover, while our approach ensures reproducibility and accessibility, it might overlook some nuances of trust that are uniquely manifest in social network interactions. For instance, the propagation of trust or influence might not be adequately modeled by off-the-shelf algorithms, which typically do not account for the layered and multifaceted nature of social interactions.

To address these challenges, integrating more sophisticated analytical techniques tailored to the specific characteristics of social networks could enhance the accuracy and depth of trust predictions. Advanced techniques such as deep learning, which can learn complex patterns from large-scale data, or graph neural networks, which are designed specifically to handle network structures, could offer more nuanced insights into trust dynamics.

## 6. Conclusions and Future Work

This study embarked on an extensive exploration of trust within social networks, initiating a detailed literature review covering the structure and characteristics of social networks, definitions and forms of trust, its correlation with social networks, and the methodologies for determining trust. Following the theoretical groundwork, a practical implementation was undertaken, utilizing a diverse array of machine-learning models to assess the strength of user relationships on Facebook, therefore underscoring the pivotal role of artificial intelligence in deciphering user behavior and network structures.

Among the models evaluated, KNN demonstrated remarkable performance across multiple metrics, establishing itself as a robust tool for trust prediction. On the contrary, the Naive Bayes algorithm fell short of expectations, underlining the importance of model selection based on the intricate dynamics of social trust. Neural networks, while showing promising results, hinted at the potential for even greater accuracy with the availability of larger datasets, suggesting that dataset size significantly influences model performance.

The experimental outcomes revealed through accuracy, precision, recall, F1-score, and confusion matrices affirm the complexity of modeling trust relationships. These results not only provide a comparative analysis of various models but also highlight the nuanced understanding required to predict trust levels accurately. The minimum and maximum accuracy values presented in the tables underscore the variability in model performance, prompting a need for further optimization and testing on more extensive datasets.

Looking ahead, several avenues for extending this research present themselves. A promising direction involves leveraging Convolutional Graph Neural Networks and applying random walk techniques to model social networks more intricately through graph representations [72,73]. Simplification strategies for these complex graph structures could facilitate more efficient processing without compromising the integrity of the network's information.

Moreover, enriching the dataset with additional records and features could enhance the models' reliability and lead to more insightful conclusions [74]. Utilizing APIs from popular social media platforms like Facebook, Twitter, and Instagram offers a method to capture a broader array of data, potentially unlocking new dimensions in trust prediction.

Further experimentation with a wider range of machine-learning models and exhaustive exploration of parameter combinations could refine the predictive capabilities [75,76]. Notably, the exploration of advanced neural network architectures and their parameter settings promises to push the boundaries of what is currently achievable in trust prediction.

The dynamic nature of trust, evolving over time, suggests the potential application of time-series prediction models to capture these changes. Incorporating sentiment analysis, particularly for comments and posts, could offer a modern approach to understanding the nuances of user interactions and their impact on trust [77]. Tools such as TextBlob, Vader, NTLK, BERT, and Spacy, supported by the Python language, are instrumental in performing sentiment analysis, highlighting the role of natural language processing in this domain [78].

To further validate the robustness and versatility of our approaches, future research will involve testing these models across multiple datasets. We plan to collaborate with other researchers, access different types of social media platforms, and utilize publicly available datasets. Such efforts will help ascertain the adaptability of our tailored models in various settings and contribute to their refinement. Additionally, we acknowledge that variations in data availability, privacy concerns, and the need for hyperparameter tuning present significant challenges. These will be systematically addressed in future studies to enhance the transferability of our machine-learning solutions.

**Author Contributions:** Conceptualization, S.K. and A.K.; Data Curation, S.K. and A.K.; Writing—Original Draft, S.K. and A.K.; Methodology, S.K. and A.K.; Review and Editing, S.K. and A.K. All authors have read and agreed to the published version of the manuscript.



**Funding:** This research received no external funding.

**Data Availability Statement:** No new data were created or analyzed in this study. Data sharing is not applicable to this article.

**Conflicts of Interest:** The authors declare no conflicts of interest.

## References

1. Drakopoulos, G.; Kanavos, A.; Paximadis, K.; Ilias, A.; Makris, C.; Mylonas, P. Computing Massive Trust Analytics for Twitter using Apache Spark with Account Self-assessment. In Proceedings of the 16th International Conference on Web Information Systems and Technologies (WEBIST), Budapest, Hungary, 3–5 November 2020; pp. 403–414.
2. Sherchan, W.; Nepal, S.; Paris, C. A survey of trust in social networks. *ACM Comput. Surv.* **2013**, *45*, 1–33. [\[CrossRef\]](#)
3. Bishop, C.M. Neural networks and their applications. *Rev. Sci. Instrum.* **1994**, *65*, 1803–1832. [\[CrossRef\]](#)
4. Ghafari, S.M.; Beheshti, A.; Joshi, A.; Paris, C.; Mahmood, A.; Yakhchi, S.; Orgun, M.A. A Survey on Trust Prediction in Online Social Networks. *IEEE Access* **2020**, *8*, 144292–144309. [\[CrossRef\]](#)
5. Kim, Y.A.; Le, M.; Lauw, H.W.; Lim, E.; Liu, H.; Srivastava, J. Building a Web of Trust without Explicit Trust Ratings. In Proceedings of the 2008 IEEE 24th International Conference on Data Engineering Workshop, Cancun, Mexico, 7–12 April 2008; pp. 531–536.
6. He, C.; Zeng, J.; Zhang, G.; Liu, S. Generalized opinion dynamics model for social trust networks. *J. Comb. Optim.* **2022**, *44*, 3641–3662. [\[CrossRef\]](#)
7. Nepal, S.; Sherchan, W.; Bouguettaya, A. A Behaviour-Based Trust Model for Service Web. In Proceedings of the 2010 IEEE International Conference on Service-Oriented Computing and Applications (SOCA), Perth, WA, Australia, 13–15 December 2010; pp. 1–4.
8. Kanavos, A.; Kafeza, E.; Makris, C. Can We Rank Emotions? A Brand Love Ranking System for Emotional Terms. In Proceedings of the IEEE International Congress on Big Data, New York, NY, USA, 27 June–2 July 2015; IEEE Computer Society: Los Alamitos, CA, USA, 2015; pp. 71–78.
9. Kanavos, A.; Perikos, I.; Hatzilygeroudis, I.; Tsakalidis, A.K. Emotional community detection in social networks. *Comput. Electr. Eng.* **2018**, *65*, 449–460. [\[CrossRef\]](#)
10. Arrow, K.J. *Economic Welfare and the Allocation of Resources for Invention*; Springer: Berlin/Heidelberg, Germany, 1972.
11. Rotter, J.B. Interpersonal trust, trustworthiness, and gullibility. *Am. Psychol.* **1980**, *35*, 1. [\[CrossRef\]](#)
12. Coleman, J.S. Social capital in the creation of human capital. *Am. J. Sociol.* **1988**, *94*, S95–S120. [\[CrossRef\]](#)
13. Granovetter, M.S. The strength of weak ties. *Am. J. Sociol.* **1973**, *78*, 1360–1380. [\[CrossRef\]](#)
14. Burt, R.S.; Celotto, N. The network structure of management roles in a large matrix firm. *Eval. Program Plan.* **1992**, *15*, 303–326. [\[CrossRef\]](#)
15. Donath, J.; Boyd, D. Public displays of connection. *Technol. J.* **2004**, *22*, 71–82. [\[CrossRef\]](#)
16. DuBois, T.; Golbeck, J.; Srinivasan, A. Predicting Trust and Distrust in Social Networks. In Proceedings of the 2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing, Boston, MA, USA, 9–11 October 2011; pp. 418–424.
17. Breiman, L. *Random Forests*; Chapman & Hall: London, UK, 2001.
18. Goodfellow, I.; Bengio, Y.; Courville, A. *Deep Learning*; MIT Press: Cambridge, MA, USA, 2016.
19. Liu, Y.; Ying, X. A Review of Social Network Sites: Definition, Experience, and Applications. Available online: <https://file.scirp.org/pdf/18-2.1.31.pdf> (accessed on 24 March 2024).
20. Golbeck, J.; Parsia, B.; Hendler, J.A. Trust Networks on the Semantic Web. In Proceedings of the International Workshop on Cooperative Information Agents, Helsinki, Finland, 27–29 August 2003; pp. 238–249.
21. Zhang, Y.; Yu, T. Mining Trust Relationships from Online Social Networks. *J. Comput. Sci. Technol.* **2012**, *27*, 492–505. [\[CrossRef\]](#)
22. Hang, C.W.; Singh, M.P. Trust-Based Recommendation Based on Graph Similarity. Available online: <https://www.csc2.ncsu.edu/faculty/mpsingh/papers/mas/aamas-trust-10-graph.pdf> (accessed on 24 March 2024).
23. Ziegler, C.; Lausen, G. Spreading Activation Models for Trust Propagation. In Proceedings of the IEEE International Conference on e-Technology, e-Commerce and e-Service, Taipei, Taiwan, 28–31 March 2004; pp. 83–97.
24. Zuo, Y.; Hu, W.; O’Keefe, T. Trust Computing for Social Networking. In Proceedings of the 2009 Sixth International Conference on Information Technology, New Generations, Las Vegas, NV, USA, 27–29 April 2009; pp. 1534–1539.
25. Caverlee, J.; Liu, L.; Webb, S. Socialtrust: Tamper-Resilient Trust Establishment in Online Communities. In Proceedings of the ACM/IEEE Joint Conference on Digital Libraries (JCDL 2008), Pittsburgh, PA, USA, 16–20 June 2008; pp. 104–114.
26. Liu, G.; Wang, Y.; Orgun, M.A.; Liu, H. Discovering Trust Networks for the Selection of Trustworthy Service Providers in Complex Contextual Social Networks. In Proceedings of the 2012 IEEE 19th International Conference on Web Services, Honolulu, HI, USA, 24–29 June 2012; pp. 384–391.
27. Guo, G.; Zhang, J.; Zhu, F.; Wang, X. Factored similarity models with social trust for top-N item recommendation. *Knowl. Based Syst.* **2017**, *122*, 17–25. [\[CrossRef\]](#)

28. Cai, M.; Wang, Y.; Gong, Z. An Extension of Social Network Group Decision-Making Based on TrustRank and Personas. *Int. J. Comput. Intell. Syst.* **2020**, *13*, 332–340. [\[CrossRef\]](#)
29. Kim, Y.A.; Song, H.S. Strategies for predicting local trust based on trust propagation in social networks. *Knowl. Based Syst.* **2011**, *24*, 1360–1371. [\[CrossRef\]](#)
30. Tang, J.; Sun, J.; Wang, C.; Yang, Z. Social Influence Analysis in Large-Scale Networks. In Proceedings of the 15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, Paris, France, 28 June–1 July 2009; pp. 807–816.
31. Fogel, J.; Nehmad, E. Internet social network communities: Risk taking, trust, and privacy concerns. *Comput. Hum. Behav.* **2009**, *25*, 153–160. [\[CrossRef\]](#)
32. Kumar, S.; Mallik, A.; Khetarpal, A.; Panda, B.S. Influence maximization in social networks using graph embedding and graph neural network. *Inf. Sci.* **2022**, *607*, 1617–1636. [\[CrossRef\]](#)
33. Graph Neural Network and Some of GNN Applications. Available online: <https://neptune.ai/blog/graph-neural-network-and-some-of-gnn-applications> (accessed on 17 April 2024).
34. Jamali, M.; Ester, M. *TrustWalker*: A Random Walk Model for Combining Trust-Based and Item-Based Recommendation. In Proceedings of the 15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, Paris, France, 28 June–1 July 2009; pp. 397–406.
35. Liu, H.; Lim, E.P.; Lauw, H.W.; Le, M.T.; Sun, A.; Srivastava, J.; Kim, Y.A. Predicting Trusts Among Users of Online Communities: An Epinions Case Study. In Proceedings of the 9th ACM Conference on Electronic Commerce, Chicago, IL, USA, 8–12 June 2008; pp. 310–319.
36. Ghavipour, M.; Meybodi, M.R. Trust propagation algorithm based on learning automata for inferring local trust in online social networks. *Knowl. Based Syst.* **2018**, *143*, 307–316. [\[CrossRef\]](#)
37. Adali, S.; Escrivá, R.; Goldberg, M.K.; Hayvanovych, M.; Magdon-Ismael, M.; Szymanski, B.K.; Wallace, W.A.; Williams, G.T. Measuring behavioral trust in social networks. In Proceedings of the 2010 IEEE International Conference on Intelligence and Security Informatics, Vancouver, BC, Canada, 23–26 May 2010; pp. 150–152.
38. Sacco, O.; Breslin, J.G. In users we trust: Towards social user interactions based Trust Assertions for the Social Semantic Web. *Soc. Netw. Anal. Min.* **2014**, *4*, 229. [\[CrossRef\]](#)
39. Ghafari, S.M.; Yakhchi, S.; Beheshti, A.; Orgun, M.A. SETTRUST: Social Exchange Theory Based Context-Aware Trust Prediction in Online Social Networks. In Proceedings of the 5th International Workshop on Data Quality and Trust in Big Data (QUAT), Dubai, United Arab Emirates, 12–15 November 2018; Springer: Berlin/Heidelberg, Germany, 2018; Volume 11235, pp. 46–61.
40. Ghafari, S.M.; Joshi, A.; Beheshti, A.; Paris, C.; Yakhchi, S.; Orgun, M.A. DCAT: A Deep Context-Aware Trust Prediction Approach for Online Social Networks. In Proceedings of the 17th International Conference on Advances in Mobile Computing & Multimedia, Munich, Germany, 2–4 December 2019; pp. 20–27.
41. Bo, Z.; Huan, Z.; Meizi, L.; Qin, Z.; Jifeng, H. Trust traversal: A trust link detection scheme in social network. *Comput. Netw.* **2017**, *120*, 105–125. [\[CrossRef\]](#)
42. Ma, N.; Lim, E.; Nguyen, V.; Sun, A.; Liu, H. Trust relationship prediction using online product review data. In Proceedings of the 1st ACM International Workshop on Complex Networks Meet Information & Knowledge Management, Hong Kong, China, 6 November 2009; pp. 47–54.
43. Graña, M.; Nuñez-Gonzalez, J.D.; Ozaeta, L.; Kaminska-Chuchmala, A. Experiments of Trust Prediction in Social Networks by Artificial Neural Networks. *Cybern. Syst.* **2015**, *46*, 19–34. [\[CrossRef\]](#)
44. Wang, X.; Wang, Y.; Sun, H. Exploring the Combination of Dempster-Shafer Theory and Neural Network for Predicting Trust and Distrust. *Comput. Intell. Neurosci.* **2016**, *2016*, 5403105. [\[CrossRef\]](#)
45. Zhao, K.; Pan, L. A Machine Learning Based Trust Evaluation Framework for Online Social Networks. In Proceedings of the 13th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Beijing, China, 24–26 September 2014; IEEE Computer Society: Los Alamitos, CA, USA, 2014; pp. 69–74.
46. Korovaiko, N.; Thomo, A. Trust prediction from user-item ratings. *Soc. Netw. Anal. Min.* **2013**, *3*, 749–759. [\[CrossRef\]](#)
47. Borzymek, P.; Sydow, M. Trust and Distrust Prediction in Social Network with Combined Graphical and Review-Based Attributes. In *KES International Symposium on Agent and Multi-Agent Systems: Technologies and Applications*; Springer: Berlin/Heidelberg, Germany, 2010; Volume 6070, pp. 122–131.
48. López, J.; Maag, S. Towards a Generic Trust Management Framework Using a Machine-Learning-Based Trust Model. In Proceedings of the 2015 IEEE Trustcom/BigDataSE/ISPA, Helsinki, Finland, 20–22 August 2015; pp. 1343–1348.
49. Zolfaghar, K.; Aghaie, A. Evolution of trust networks in social web applications using supervised learning. *Proc. Comput. Sci.* **2011**, *3*, 833–839. [\[CrossRef\]](#)
50. Denko, M.K.; Sun, T.; Woungang, I. Trust management in ubiquitous computing: A Bayesian approach. *Comput. Commun.* **2011**, *34*, 398–406. [\[CrossRef\]](#)
51. Raj, E.D.; Babu, L.D.D. An enhanced trust prediction strategy for online social networks using probabilistic reputation features. *Neurocomputing* **2017**, *219*, 412–421. [\[CrossRef\]](#)
52. Zhao, L.; Hua, T.; Lu, C.; Chen, I. A topic-focused trust model for Twitter. *Comput. Commun.* **2016**, *76*, 1–11. [\[CrossRef\]](#)

53. Zhang, X.; Cui, L.; Wang, Y. Commtrust: Computing Multi-dimensional Trust by Mining E-commerce Feedback Comments. *IEEE Trans. Knowl. Data Eng.* **2013**, *26*, 1631–1643. [\[CrossRef\]](#)
54. Tang, J.; Gao, H.; Hu, X.; Liu, H. Exploiting Homophily Effect for Trust Prediction. In Proceedings of the 6th International Conference on Web Search and Data Mining (WSDM), Rome, Italy, 4–8 February 2013; ACM: New York, NY, USA, 2013; pp. 53–62.
55. Wang, Y.; Wang, X.; Tang, J.; Zuo, W.; Cai, G. Modeling Status Theory in Trust Prediction. In Proceedings of the 29th AAAI Conference on Artificial Intelligence, Austin, TX, USA, 25–30 January 2015; AAAI Press: Washington, DC, USA, 2015; pp. 1875–1881.
56. Zheng, X.; Wang, Y.; Orgun, M.A.; Liu, G.; Zhang, H. Social Context-Aware Trust Prediction in Social Networks. In Proceedings of the Service-Oriented Computing: 12th International Conference, ICSOC 2014, Paris, France, 3–6 November 2014; Springer: Berlin/Heidelberg, Germany, 2014; Volume 8831, pp. 527–534.
57. Moradi, P.; Ahmadian, S. A reliability-based recommendation method to improve trust-aware recommender systems. *Expert Syst. Appl.* **2015**, *42*, 7386–7398. [\[CrossRef\]](#)
58. Sanadhya, S.; Singh, S. Trust calculation with ant colony optimization in online social networks. *Procedia Comput. Sci.* **2015**, *54*, 186–195. [\[CrossRef\]](#)
59. Fazeli, S.; Loni, B.; Bellogín, A.; Drachsler, H.; Sloep, P.B. Implicit vs. explicit trust in social matrix factorization. In Proceedings of the 8th ACM Conference on Recommender Systems (RecSys 2014), Foster City, CA, USA, 6–10 October 2014; pp. 317–320.
60. Tang, J.; Gao, H.; Liu, H.; Sarma, A.D. eTrust: Understanding Trust Evolution in an Online World. In Proceedings of the 18th SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD), Beijing, China, 12–16 August 2012; ACM: New York, NY, USA, 2012; pp. 253–261.
61. Zhang, H.; Wang, Y.; Zhang, X. Transaction Similarity-Based Contextual Trust Evaluation in E-Commerce and E-Service Environments. In Proceedings of the IEEE International Conference on Web Services (ICWS), Washington, DC, USA, 4–9 July 2011; IEEE Computer Society: Los Alamitos, CA, USA, 2011; pp. 500–507.
62. Moturu, S.T.; Liu, H. Quantifying the trustworthiness of social media content. *Distrib. Parallel Databases* **2011**, *29*, 239–260. [\[CrossRef\]](#)
63. Liao, H.; Cimini, G.; Medo, M. Measuring Quality, Reputation and Trust in Online Communities. In Proceedings of the Foundations of Intelligent Systems: 20th International Symposium, ISMIS 2012, Macau, China, 4–7 December 2012; Springer: Berlin/Heidelberg, Germany, 2012; Volume 7661, pp. 405–414.
64. Su, K.; Xiao, B.; Liu, B.; Zhang, H.; Zhang, Z. TAP: A personalized trust-aware QoS prediction approach for web service recommendation. *Knowl. Based Syst.* **2017**, *115*, 55–65. [\[CrossRef\]](#)
65. Ruan, Y.; Duresi, A.; Alfantoukh, L. Using Twitter trust network for stock market analysis. *Knowl. Based Syst.* **2018**, *145*, 207–218. [\[CrossRef\]](#)
66. Tang, J.; Hu, X.; Liu, H. Is Distrust the Negation of Trust?: The Value of Distrust in Social Media. In Proceedings of the 25th Conference on Hypertext and Social Media (HT), Santiago, Chile, 1–4 September 2014; ACM: New York, NY, USA, 2014; pp. 148–157.
67. Guha, R.V.; Kumar, R.; Raghavan, P.; Tomkins, A. Propagation of trust and distrust. In Proceedings of the 13th International Conference on World Wide Web (WWW), New York, NY, USA, 17–22 May 2004; ACM: New York, NY, USA, 2004; pp. 403–412.
68. team2-ethi-mental-state. Available online: <https://github.com/asrobang1/team2-ethi-mental-state/> (accessed on 17 April 2024).
69. Burke, M.; Kraut, R.E. Growing closer on Facebook: Changes in tie strength through social network site use. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Toronto, ON, Canada 26 April–1 May 2014; pp. 4187–4196.
70. Burke, M.; Kraut, R.E. The Relationship Between Facebook Use and Well-Being Depends on Communication Type and Tie Strength. *J. Comput.-Mediat. Commun.* **2016**, *21*, 265–281. [\[CrossRef\]](#)
71. Gilbert, E.; Karahalios, K. Predicting tie strength with social media. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Boston, MA, USA, 6 April 2009; pp. 211–220.
72. Drakopoulos, G.; Kanavos, A.; Tsakalidis, K. Fuzzy Random Walkers with Second Order Bounds: An Asymmetric Analysis. *Algorithms* **2017**, *10*, 40. [\[CrossRef\]](#)
73. Savvopoulos, A.; Kanavos, A.; Mylonas, P.; Sioutas, S. LSTM Accelerator for Convolutional Object Identification. *Algorithms* **2018**, *11*, 157. [\[CrossRef\]](#)
74. Piri, J.; Mohapatra, P.; Acharya, B.; Gharehchopogh, F.S.; Gerogiannis, V.C.; Kanavos, A.; Manika, S. Feature Selection Using Artificial Gorilla Troop Optimization for Biomedical Data: A Case Analysis with COVID-19 Data. *Mathematics* **2022**, *10*, 2742. [\[CrossRef\]](#)
75. Kanavos, A.; Karamitsos, I.; Mohasseb, A.; Gerogiannis, V.C. Comparative Study of Machine Learning Algorithms and Text Vectorization Methods for Fake News Detection. In Proceedings of the 14th International Conference on Information, Intelligence, Systems & Applications (IISA), Volos, Greece, 10–12 July 2023; IEEE: New York, NY, USA, 2023; pp. 1–8.
76. Kanavos, A.; Antonopoulos, N.; Karamitsos, I.; Mylonas, P. A Comparative Analysis of Tweet Analysis Algorithms Using Natural Language Processing and Machine Learning Models. In Proceedings of the 18th International Workshop on Semantic and Social Media Adaptation and Personalization (SMAP), Limassol, Cyprus, 25–26 September 2023; IEEE: New York, NY, USA, 2023; pp. 1–6.

77. Kanavos, A.; Nodarakis, N.; Sioutas, S.; Tsakalidis, A.K.; Tsohis, D.; Tzimas, G. Large Scale Implementations for Twitter Sentiment Classification. *Algorithms* **2017**, *10*, 33. [[CrossRef](#)]
78. Vonitsanos, G.; Kanavos, A.; Mylonas, P. Decoding Gender on Social Networks: An In-depth Analysis of Language in Online Discussions Using Natural Language Processing and Machine Learning. In Proceedings of the IEEE International Conference on Big Data, Sorrento, Italy, 15–18 December 2023; pp. 4618–4625.

**Disclaimer/Publisher’s Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.