Journal of
Theoretical and Applied Electronic Commerce Research

Article

SenseTrust: A Sentiment Based Trust Model in Social Network

Alireza Mohammadi and Seyyed Alireza Hashemi Golpayegani *

Computer Engineering and Information Technology Department, Amirkabir University of Technology, Tehran 1591634311, Iran; mohammadi.a@aut.ac.ir
* Correspondence: sa.hashemi@aut.ac.ir

Abstract: Online social networks, as popular media and communications tools with their own extensive uses, play key roles in public opinion polls, politics, economy, and even governance. An important issue regarding these networks is the use of multiple sources of publishing or re-publishing news and propositions that can influence audiences depending on the level of trust in these sources between users. Therefore, estimating the level of trust in social networks between users can predict the extent of social networks' impact on news and different publication and re-publication sources, and correspondingly provide effective strategies in news dissemination, advertisements, and other diverse contents for trustees. Therefore, trust is introduced and interpreted in the present study. A large portion of interactions in social networks is based on sending and receiving texts employing natural language processing techniques. A Hidden Markov Model (HMM) was designed via an efficient model, namely SenseTrust, to estimate the level of trust between users in social networks.

Keywords: social network; trust; sentiment analysis; recursive neural tensor network; hidden markov model

Citation: Mohammadi, A.; Hashemi Golpayegani, S.A. SenseTrust: A Sentiment Based Trust Model in Social Network. *J. Theor. Appl. Electron. Commer. Res.* **2021**, *16*, 2031–2050. https://doi.org/10.3390/jtaer16060114

Academic Editor: Eduardo Álvarez-Miranda

Received: 2 June 2021
Accepted: 22 July 2021
Published: 27 July 2021

1. Introduction

It is generally accepted that trust is a key factor for the formation and development of interpersonal relations. The success of many businesses, as well as almost all news organizations and media depend on their ability to gain the trust of their audience and customers. The estimation of the level of trust between people can be a positive first step for the assessment of trust-centered relationships. In Section 1.1, the concept of trust, particularly trust in social networks, was examined. Then, previous research studies in this domain were reviewed.

1.1. Trust

Trust is difficult to define but invokes similar feelings in most people. In general, trust can be described as one's certainty that an entity functions as expected, despite one's inability to monitor and control the environment in which the entity operates [1]. Due to the differences in the origins of trust in different fields, there are different types of trust with different aspects and properties, and each needs to be modeled in its own way [2]. In psychology, trust is the psychological state of a person who accepts or ignores the possibility of being vulnerable to the trustee based on the positive expectations of the trustee's intent or behavior [3]. It is believed that trust has three dimensions: Cognitive, affective, and behavioral [4]. In sociology, trust has been defined as "a bet about the future contingent actions of the trustee" [5]. However, this bet or expectation is said to be trust only if it has some impact on the actions of the person who places the trust in another. Trust can be understood and discussed from two perspectives: Personal and social. At the personal level, which is a psychological viewpoint, trust revolves around the notion of vulnerability [6]. This trust can be differentiated from cooperation based on the presence of guarantees (assurances) that interactions will be controlled and bad behavior will be met with sanctions (penalties). However, cooperation can be considered a type of trust if it relies more on the future consequences of actions (fear of future behavior of others) [7]. In this respect, social trust only has two dimensions: Cognitive and behavioral, as the affective dimension builds over time as the trust between involved people increases [8]. At the social level, trust can be viewed as a property of a social group, which is reflected in the group's collective psychological state. This causes the group members to act under the assumption that other members are trustworthy and expect other members to trust them as well [9].

In the context of computer science, trust can be separated into two categories: User trust and system trust. The concept of user trust originates from psychology and sociology [10]. The standard definition of user trust is the subjective expectation of an entity regarding future behavior of others [11]. According to this definition, trust is inherently personal. In online systems, such as eBay and Amazon, trust is built on feedback arising from the past interactions of users [12]. From this perspective, trust is relational. Frequent interactions between two people strengthen the relationships that build trust based on past experiences. Trust increases with positive experiences and decreases with negative ones.

There are two types of trust in online systems: Direct trust, which results from the person's experience of direct interaction with others, and recommendation trust, which is based on experiences of other people in a social network and in a sense grow based on the propagative property of trust. In P2P-based trust models, peers collect information about other peers from their own social networks, which are also known as referral networks [13]. In these models, each peer is assessed from two perspectives: Trustworthiness as an interaction partner, that is, the capability to provide a certain service, or in other words expertise [14], and trustworthiness as a recommender, which refers to the ability to provide good recommendations, which is also known as sociability. After each interaction, the expertise and sociability of peers in the referral chain will be updated to reflect the experience of the member. The immediate neighbors of the member must be updated periodically to reflect the changes in trust in those peers based on their expertise and sociability.

The standard definition of system trust originates from the field of security [15]. According to this definition, trust is the "expectation that a device or system will faithfully behave in a particular manner to fulfill its intended purpose". For example, we call a computer trustworthy if its software and hardware perform their duties as we expect, that is, if its services are available, functioning, and behaving as they must and always do [16]. The concept of system trust must be supported by software and hardware solutions. For example, researchers in [17] presented a software-based mechanism, and in [18] a hardware-based mechanism for this purpose. In all disciplines, trust relationships revolve around two concepts: Risk and interdependence [19]. Risk originates from uncertainty in the intention of others. Interdependence means that people in trust relationship have somewhat aligned interests that they cannot achieve without the other. A relationship that does not meet these two conditions is not a trust relationship. Hence, it can be stated that risk and interdependence are necessary conditions for trust, and thus, changes in these conditions can alter the form and level of trust.

Trust has many different aspects. In the calculative aspect of trust, it is said to be the result of a calculation by the trustor that is designed to maximize the trustor's stakes in the interaction. This aspect of trust is popular in economics for modeling trust and cooperation with Prisoner's dilemma games. This aspect also has common use in organizational science. In an article published in 1990, Coleman James describes this phenomenon as follows: A rational actor trusts if the ratio of the chance of success to the chance of failure is greater than the ratio of the value of loss in the event of failure to the value of gain in the event of success [20]. In the relational aspect, trust is defined as the confidence built over time as a result of repeated interactions between the trustor and the trustee. The basis of relational trust is the trustor's knowledge about the relation itself, as trustworthiness and dependability in previous interactions improve the positive expectations of the trustee's intentions [21]. In computer science, this form of trust is called direct trust, that is, the trust is based on the direct interactions of two individuals. The emotional aspect of trust is defined in terms of security and comfort by which the trustor relies on the trustee [22]. In psychology, emotional trust is said to be the outcome of direct relations between individuals [23]. Influenced by cognitive trust, emotional trust helps the trustor develop a positive perception of the continuity of the relationship. Empirical studies, such as [24], have shown that the previous direct experiences of the trustor can influence the trustor's emotions toward and emotional trust on the trustee. Holmes believes that emotional trust is analogous to an emotional security, which helps a person to feel comfortable about relying on another person beyond the existing evidence of the person [23]. In its cognitive aspect, trust is the sense of confidence derived from reason and rational behavior [9]. According to the social capital theory [25], cognitive trust is influenced by three forms of social capital: Information channels, norms and sanctions, and the trustee's obligations to the trustor. The trustee's cognitive trust on the trustee can also be influenced by the social relation networks and strong relations between members [26]. Specifically, positive referrals by social network relations increase the cognitive trust of the trustor toward the trustee [27]. Mullring's research [28] suggests that cognitive trust precedes emotional trust and that emotional trust leads to the formation of desirable or undesirable expectations on part of the trustee. Institutional trust is the trust resulting from an environment created by an organization, where cooperation between members is encouraged and misconducts are properly disciplined [9]. This can be done at the organizational level [29] or at the social level (e.g., legal systems formed to protect individual and property rights). For example, Publius [30] is an application that utilizes institutional trust to help users publish content anonymously without concern about censorship and manipulation of contents.

Trust also has multiple properties that are critical to understanding this concept. First, trust is context-specific, meaning that it is always bounded to a particular context. For example, if person A trusts person B in regard to medical knowledge, this trust does not necessarily extend to the context of mechanical knowledge. This means that, for example, person B is trustworthy as a doctor, but not as a repairman. This property of trust is not the same as trust context, which represents the environment where trust relationship is present (e.g., law enforcement, insurance, social control, etc.) [31]. The second property of trust is its dynamic nature, in the sense that it can increase or decrease with new experiences (interaction or observation) [32]. Trust may also decrease over time. Newer experiences are more important than old ones, and also old experiences gradually become obsolete and outdated. This particular characteristic of trust is extensively modeled in computer science and has been used in various approaches, for example, by setting the old experiences to age, giving more weight to new experiences, and using only the most recent experiences. In some models, trust computations are performed periodically to ensure that the results are up-to-date. The next property of trust is its propagative nature. For example, when person A trusts person B, and person B trusts person C, then person A somewhat trusts person C even though he does not know him. However, this does not mean that trust is transitive [33]. It is the propagative nature of trust that allows trust information to disseminate from one member to another member of a social network and a trust chain to be created. This property of trust has been the subject of many studies, such as [34,35] where researchers have used this property in their trust models. Another property of trust is that it is self-reinforcing. People are likely to exhibit positive behaviors toward persons whom they trust. On the contrary, they are less likely to interact with persons whom they do not trust enough, and this may lead to even less trust between people [36]. The last property of trust that is of interest to this study is that trust in event sensitive, meaning that, while it takes a long time to build trust, it can be destroyed by a single event [37].

1.2. Related Works

Generally, trust evaluation models in social networks can be divided into three categories; trust models based on network topology, trust models based on interaction, and hybrid trust model. As follows, examples and more explanations for each one were provided [2].

1.2.1. Trust Models Based on Network Topology

Network topology is influenced by level of trust in social networks. High density in a network (such as more relations between members) can show more trust between them. Increasing both levels of output and input can, in turn, increase trust between members. Studies on network topology [38] have shown that:

1. Members whose levels of output are greater have higher levels of trust.
2. If a person's relation is more oriented to individuals with higher output levels, they are endowed with higher levels of trust.
3. While centralization of individuals (those who are in a network center) has a positive impact on their levels of trust, the average levels of trust in all members decease as the entire network centralizes.

Measures presented in this study have been accepted by numerous researchers, but this is not common. For example, interactions can be found in social networks formed on the basis of controversies and objections and members with high levels of output can demonstrate their objections towards a specific topic and do not trust in them. More examinations have revealed that social network topology is usually formed based on the concept of trust or friend-of-a-friend FOAF protocol. Generally, a network of trust is created for each person. This network indicates other members available in an individual's social network as nodes and the amount of trust in each member via edges. Then, various approaches are used for scrolling networks and gaining trust between both nodes. This approach represents the essence of trust dissemination for its estimation. As follows, some of the more important studies in this domain were reviewed.

In the method presented with the development of the concept of FOAF for the creation of a trust network in semantic web in [39], individuals were allowed to specify their level of trust in people they knew. In this model, nine certain levels from "very trusted" to "very untrusted" were used to express trust. Trust can be also expressed at a generalized level or in a specific field (domain). Several different levels of trust can be further determined for an entity in various fields. This model utilizes ontology for defining different levels in various fields. The FOAF graph developed through annotation of trust is also used for obtaining trust between two nodes or individuals in a network that are not connected directly to each other. Moreover, trust is calculated by means of network topology using weighted edges.

In the TidalTrust method, FOAF relation list is used to extract trust relationships between two users in a social network [40]. This method is based on the assumption that neighbors with higher levels of trust in each other accept each other better as a third party in terms of trust. Accordingly, in this method, the paths between two users with no direct relations and level of trust between users of these paths are used to calculate trust. According to this method, shorter paths and higher levels of trust have less difference between average points for stable grading of trust. Given the development of her research studies in the domain of trust, Golbeck developed another investigation [41] with a focus on similarities of users' profiles to build trust in social networks. However, other investigations such as [42] discussed trust based on similarities between two members. The main component of similarity between two users in the virtual world in this study was mentioned as similarities of published contents between them and cosine similarity was also used to determine the similarity of the published contents. The main point is that if two texts are written to confirm and refute a theory with the same keywords based on tf-idf criteria (this issue occurred in the example provided in this study), these two texts are assessed using a similar manner, but they are in fact opposed. Therefore, for the above-mentioned method in this study, many counterexamples can be presented. In another model, in [43], where an extended version is provided by Golbeck, mutual grading of trust and components ensuring each entity in a network were considered and trust was then calculated via a graph of weighted edges. Initially, the similarities between the two raters were estimated by means of comparison of ratings given by them to similar entities. Then, it was used to select a suitable neighbor to benefit from their recommendations.

Such recommendations were subsequently compared and the one belonging to the rater similar to the trustee was selected.

Another approach established to create a local-group trust matrix in the domain of semantic web is named Appleseed [44]. This method has been established with the idea of developing a trust matrix in semantic web. The reasons behind the creation of this method are using graph exploration of partial trust and reducing calculation complexities. In most cases, this approach meets the need to explore a comprehensive trust graph and then mitigate the complexity of calculations by lowering the domain of calculations to a reduced trust graph. In [45], researchers also used a graph-based solution and a trust network to generate a node recommender in social networks. This model used similarities between graphs for more recommendations. In another study [46], a method was also developed for calculating trust based on trust chain and trust graph. The proposed model by these researchers benefited from proof-of-trust graph calculating trust within a trust chain. In social trust model presented by Caverli, social relations and feedback were simultaneously employed to calculate trust [47]. Therefore, users could rate each other following interactions. Then, trust manager could combine these ratings to gain social trust between members. The rank for each member was also weighted using the quality of relations (high-quality communications refer to greater relations with members with high level of trust).

In another model called Sunny [48], there was a focus on data obtained from social chains and channels. In this regard, they presented Bayesian trust extraction model to estimate the reliability of information about trust obtained from a specific source. In another study [49]; the researcher, unlike many similar investigations extracting trust network from user feedback, developed this concept without explicit grading of users. The level of trust and trust links in the proposed method by this researcher were calculated through considering reputation for each user (i.e., a person's skill in a specific domain) and level of dependence on that issue or specific field. The given method included two main steps:

1. Calculating a user's skill in a specific subject: calculating the quality of reviews of users' contents relying on reputation of those who had rated them or authors' reputation.
2. Determining level of dependence between users on thematic categories through calculating average ratings and users' reviews in thematic categories, and also calculating level of trust via level of dependence in users to a subject and other skills concerning that subject.

In [50], researchers provided a method based on gravity to estimate trust. There were two main steps within this method. Firstly, the power of friendship was re-estimated based on extensiveness of trusted neighbors for each user and this depended on interpreting their relations with others with level of trust and limitations. Then, neighborhoods in social networks were utilized to calculate effective trust processes in non-neighborhoods in social networks. This model was formed based on the assumption that social relations could change over time and such relations might impose restrictions on trust relationships.

Methods in which network topology is considered the basis for calculating trust only sheds light on the aspect of the number of users associated with each other and the flow of trust in their network. From this perspective, these methods have been criticized since they do not take actual interactions between users into account. Therefore, the volume, number, and shared contents between users are among the main features of trust in social networks.

1.2.2. Trust Models Based on Interaction

Unlike the models explained in the previous section, some models only used interactions with networks to estimate trust. Some major research studies in this domain were delineated as follows. In the method proposed by a group of researchers using behavioral pattern of user interactions, trust in an online community was predicted [51]. They also identified two categories to display users' interactions and actions in a community:

1. Categorizing users' activities in terms of information shared such as reviews, comments posted, ratings, etc. through measures such as number/sequence of reviews, number/sequence of rates, and average of number/length of comments posted, and so on.
2. Categorizing binary interactions for different possible interactions/relations that may occur between two individuals; for example, between author and rater, author and author, and rater and rater.

This model also includes time difference between user reactions creating a relationship which is called "temporary cause". In this method, a supervised training approach is provided which predicts trust between users based on evidence obtained from users themselves (user factors) like information obtained from interactions between two users (interaction factors). Then, such factors are employed to train the categorizer predicting trust between users.

STrust Model is a social trust model that is exclusively based on interactions in social networks [52]. This model consists of two types of trust:

1. Popularity trust which refers to acceptance of a member in a community and shows a member's trust from other members' perspective.
2. Participation trust that points to members' participation in a community and reflects their trust in a community.

Popularity trust is extracted from criteria such as number of followers, readers, and positive feedback to individuals' posts. Moreover, participation trust is comprised of criteria, such as the sequence of visits to networks/organizations by members, the number of people followed, as well as the number of posts read and commented. A combination of popularity trust and participation trust can, thus, determine a foundation to gain social trust in a community.

In the same study, trust was estimated on the basis of behavioral interactions between members in a social network [53]. Behavioral trust is thus estimated based on two types of trust:

1. Conversational trust that specifies length and/or sequence of relations between two members. Longer relations or those with longer sequences indicate more trust between two individuals.
2. Publication trust which refers to publication of information received from a person in a network by another one. Publication of more information received from one person in a network by another individual shows their trust in that person's information and implicitly reflects their trust in producers of that information.

Social trust models based on interaction consider interactions to estimate trust but disregard social trust topology which provides important information about members interacting with each other in a community as a significant source for estimating social trust. Therefore, trust models need to consider graph topology and interactions to calculate social trust in social networks.

1.2.3. Hybrid Trust Models

Trust models make use of a combination of interactions and social network topology for social trust calculation. In this respect, a group of researchers [54] proposed a model for opportunity networks. Such networks allow users participate in various social interactions via programs, such as content distribution and micro-blogs. This model involves network topology and its dynamicity and also provides two complete approaches for building social trust:

1. Explicit social trust, which can be established based on conscious social relations. Whenever two users interact with each other, they exchange their lists of friends with each other and store them as graphs of friends. Trust is also created based on a friendship graph in which individuals assign highest level of trust with a value of one to each other through direct relationships.

2. Implicit trust, which is created based on sequence and length of relationships between two users. For this purpose, two criteria can be used: Familiarity and similarity of nodes. Familiarity refers to duration of interactions/relations between two nodes and similarity is degree of compliance of two nodes in a familiarity circle.

In this model, explicit social trust is estimated based on network topology, but implicit trust can be estimated on the basis of users' interactions in a network. In this model, only duration and sequence of interactions are taken into account; while the essence of interactions for estimating trust between two individuals is of utmost importance. For example, in cases wherein two individuals are debating, it does not mean trust.

2. Methodology

A correlation between human sentiment and the level of trust is the main idea behind Sensetrust approach. In this respect, once a person feels good about another person, place, or service, they can trust it, and no trust will build up within them if they do not feel happy about it. Further, if a person's trust in something or someone is destroyed, no traces of good feelings about that person or thing can be observed.

Relying on this fact, various studies have been thus far carried out in this field. As an example, in a study [55] analyzing sentiments of articles published in Lithuania, researchers estimated the level of trust in the government amongst its citizens. Another investigation [56], focusing on exploring users' sentiments in opinions published in e-commerce systems, assessed the level of users' trust in e-commerce services, and researchers in another study [57] exploited the correlation between trust and human sentiment for recommender systems.

In the proposed approach in this study, users' sentiments about each other on a social network were taken into account as the basis of their trust in one another. To analyze users' sentiments towards each other, the contents exchanged on social networks that are generally textual were examined.

2.1. Sentiment and Trust Correlation: A Simple Test

A test was conducted to shed light on the correlation between type of users' sentiments towards each other and their level of trust. Firstly, a total of 300 short emails retrieved from Enron Company [58] that are publicly available [59] and generally less than ten sentences, exchanged between 50 pairs of senders and recipients, were selected.

This collection of emails is essentially comprised of conversations, exchanged via email, by employees working in Enron Corporation. For example, the emails exchanged between two employees in a conversation extracted from the dataset are presented in the Table 1.

A group of users (50 persons) were then asked to identify the sender's sentiments towards each email and place them in one of the following five categories:

$$\{Very\ Negative,\ Neative,\ Nature,\ Positive,\ Very\ Positive\}$$

Then, another group of users (50 persons) was requested to specify, for each email, the level of trust that the email recipient had gained from the sender and put it in one of the following three categories:

$$\{Untrusted,\ Nature,\ Trusted\}$$

It should be noted that crowdsourcing mechanism ensures that users practice these categories honestly and carefully. Table 2 shows the number of emails per category. Accordingly, the columns represent sentiment and the rows are associated with trust categories. So, most emails in the category of Untrusted are Very Negative and Negative. Moreover, emails categorized as recipient's trust in Nature senders have been mainly placed in the same category and majority of e-mails marked as Trusted are Positive or Very Positive in terms of categorization of sentiments.

Table 1. Emails Sample.

Sender	Receiver	Email ID	Subject	Body
joseph.alamo@enron.com	susan.mara@enron.com	20011102165120	Re: A.98-07-003—Comments of AReM and WPTF on the Assigned Commissioner's Ruling Regarding Direct Access	A.98-07-003—Response to SDG&E to the Assigned Commissioner's Ruling Regarding Comments on Certain Direct Access Issues Attached for your information are the comments filed today by the Alliance for Retail Energy Markets and the Western Power Trading Forum with regard to the ACR concerning retroactive direct access suspension.
joseph.alamo@enron.com	susan.mara@enron.com	20010919125209	Staff Meeting & Conference call on 20 September 2001	Please consider this an invitation to a Staff meeting and conference call.
susan.mara@enron.com	joseph.alamo@enron.com	20010509023200	AGENDA for Workshop on Assuring Adequate Capacity	Please see the attached memo and agenda for the Workshop on Assuring Adequate Capacity in Competitive Markets.

Table 2. Test Results.

		Sentiment Levels				
		Very Negative	Negative	Nature	Positive	Very Positive
Trust Levels	Untrusted	9	43	13	0	0
	Nature	0	3	93	4	0
	Trusted	0	0	11	86	38

In the same process, the users were asked to declare the level of trust in each recipient to the sender after analyzing all exchanged emails in one of the three categories mentioned above.

After completion of both crowdsourcing processes, all users (n = 100 participants) were asked to answer the question below:

"Do you trust an online social network user who gives you a good feeling of their writings in a particular field?"

The answers were then reduced into the following three options;

- Yes: 97 users
- I do not know: 3 users
- No: 0 users

The content of the Table above along with the question-answer can substantiate this self-evident and natural assumption that a person is trustworthy if others feel good about them in that field.

2.2. Reliability and Validity

Once a method is proposed to estimate trust between social network users, its efficiency needs to be unquestionably measurable and comparable to other ones suggested to estimate or calculate trust among users. In this study, a dataset labeled by experts and containing textual exchanges between social network users as well as their trust is used to determine the efficiency of the given method. The experiment is discussed in the Section 3 in detail, but in this section, efficiency is defined as an index to measure the proposed method performance.

It should be noted that, textual exchanges expressing trust are placed in three levels:

$$\{UnTrust\ ,\ Nature,\ Trust\}$$

They can be also in five levels as:

$$\{Very\ UnTrust,\ UnTrust,\ Nature,\ Trust,\ Very\ Trust\}$$

In some studies reviewed in the Section 1.2, trust had been correspondingly defined up to nine levels with the same logic. Definitely, these levels of trust can be also expressed by their numerical equivalents. For example, trust can be interpreted within five levels in which the lowest level of trust is represented by 0 and the highest value is shown by 4. Indeed, the closer the level of trust calculated by the proposed method to expert opinions utilized to label the data, the higher the efficiency of the method. By the same logic, the error rate of the method presented in this study for each experiment is defined as follows:

$$Error = |\ Trust\ value\ computed\ by\ SenseTrust - Trust\ value\ labaled\ by\ Experts\ |$$

In accordance with the error rate outlined above, the score assigned to trust estimation or calculation method in each experiment is defined as:

$$Score = Number\ of\ Max\ level\ Of\ Trust\ Levels - Error$$

For example, this score is calculated for interpreting trust in five levels from 0 to 4 as follows:

$$Score = 4 - Error$$

Ultimately, efficiency of trust estimation or calculation method is directly related to sum of scores for all experiments:

$$\text{Efficiency } = \frac{\sum_{k=1}^{\text{number of tests}}\ score\ of\ k-th\ test}{Number\ of\ Max\ level\ Of\ Trust\ Levels * number\ of\ tests}$$

Obviously:

$$0 \leq \text{ Efficiency} \leq 1$$

The more the efficiency is closer to 1, the more the proposed method can predict a higher level of trust among users and the more it can be in agreement with expert opinions, denoting a better performance.

Other indices employed to explain the performance of methods or models for trust estimation among social network users such as precision, recall, F-measure, accuracy, and specificity can be also utilized. Possibly, each index might have been named in the related literature with other labels, so the Table 3 should be taken into account for their detailed definitions.

Table 3. Basic Indices Definition.

		Real Trust Level (by Experts)	
	Total Tests	**Condition Negative**	**Condition Positive**
Proposed Models' Predicted Trust Level	Predicted Positive	False Positive (FP)	True Positive (TP)
	Predicted Negative	True Negative (TN)	False Negative (FN)

These indices are described in Table 4 according to the Table 3:

Table 4. Indices Definition.

Name	Formula
Precision	$\frac{TP}{TP+FP}$
Recall	$\frac{TP}{TP+FN}$
F-Measure	$\frac{2*Precision*Recall}{Precision+Recall}$
Accuracy	$\frac{TP+TN}{TP+TN+FP+FN}$
Specificity	$\frac{TN}{TN+FP}$

Apparently, all these indices range between zero and one; thus, the closer the indices to one, the better the performance of the proposed method or model.

2.3. Sentiment Analysis

So far, extensive research has been done on the text analysis for sentiment extraction. In [60], a complete review of works carried out in the field of sentiment analysis up to 2008 is provided. This study explains the applications of sentiment analysis and the challenges that hinder progress in this area and also provides a complete description of definitions from preliminary concepts such as features, unsupervised learning, and linguistic models, all the way to more complex concepts such as text summarization. One of the seminal works in this field involves [61], a method known as soft clustering, which was introduced and its theoretical foundations discussed. Although the nature of the examples presented in this article did not exactly agree with the concepts of sentiment analysis, they implicitly constituted the theoretical foundations of sentiment analysis. Later, the same authors also directly contributed to the progress of sentiment analysis. Following these developments, researchers studied the possibility of sentiment analysis with machine learning methods such as Naïve Base, Maxent and SVM, eventually concluding that machine learning methods can outperform human methods in this application [62]. In [63], a text sentiment analysis was implemented with subjectivity summarization based on minimum cuts and a method called Cut-Based Classification and the necessary architecture and evaluation framework were introduced. In another research [64], the same authors presented a sentiment analysis system based on text analysis and use of class relationships for sentiment categorization. Several major breakthroughs in the area of sentiment analysis are the results of research carried out at Stanford University's natural language processing laboratory, for example in [58,65]. In [65], researchers introduced a machine learning framework that focused on the position of words in the sentence, or as the authors put it, the sentence level sentiment; a notion that was neglected in previous works. Another innovation of this work was the neural representation of the words, which this team later used for deep learning methods. Overall, the authors of that article claimed that the introduced algorithm can accurately predict sentence-level sentiment distributions. In [58], the same researchers expanded the previous work with an emphasis on a deeper understanding of language by examining longer phrases with the use of recursive neural networks in the construction of vectors of expressions and sentences with different lengths and with different types of syntactic rules. As demonstrated, this laboratory has made continuous and consistent effort to introduce new sentiment analysis solutions and improve the quality of existing methods.

In another research [59] published by these researchers, they completed their previous works on sentiment analysis by introducing a group of deep recursive models. The important innovation of this research was the attention to the level of sentimental impact of the components of a sentence depending on their position (syntactic position) in the sentence. For this purpose, the parse tree of the sentence was developed and the effect of each component of the sentence on the sentimental impact of the entire sentence was computed according to the component position. Since other machine learning methods were unable to process this form of data to generate acceptable solutions, a recursive neural tensor network was introduced to resolve this problem. This method was trained and evaluated using the comments about movies that were posted on the IMDB website. The general procedure of the approach introduced by these researchers was as follows:

The comments posted by visitors were transformed into a sentence parse tree.

Parse trees were processed by crowdsourcing. In this step, crowdsourcing participants were asked to assign one of five tags ranging from "completely negative" to "completely positive" to each component of each sentence of each comment. Then, each sentence component was given an overall tag based on the majority of tags assigned to that component. The crowdsourcing results were used to create a dataset called Sentiment Treebank to serve as the basis for model training.

The dataset created in the previous step was used to train the proposed model.

To evaluate the recursive neural tensor network model, it was used to estimate the sentiment of sentences not included in the training dataset.

An interesting point in this research is the use of descriptive measures at five levels for expressing the underlying sentiment of textual comments, which can be likened to nine levels discussed earlier for trust in social networks [39]. Another interesting point is the survey method adopted to discover the underlying sentiments of the texts, which seems like an excellent approach for determining the sentiments of commenters implicitly and without an explicit definition of good or bad feeling experienced as a result of watching the movie, and only by relying on sentiment-containing text samples.

In relation to the efficiency and accuracy of Recurrent Neural Tensor Network (RNTN), researchers believe that:

"It pushes the state of the art in single sentence positive/negative classification from 80% up to 85.4%. The accuracy of predicting fine-grained sentiment labels for all phrases reaches 80.7%,"

An example of the output of this study can be observed in the Figure 1. The statement of "Yet, the act is still charming here." is evaluated as a positive appraisal which can be correct.

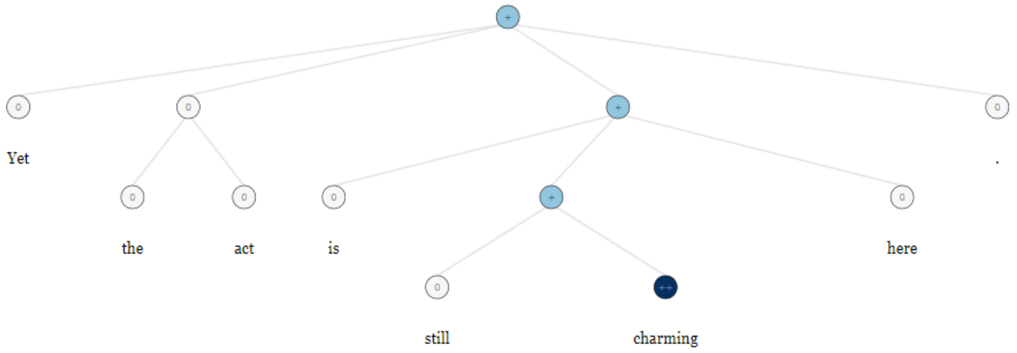


Figure 1. This is a figure. Schemes follow the same formatting.

The tree diagram above is drawn based on the software output for RNTN by Stanford University, which is in the form of the following text:

(3 (2 *Yet*) (3 (2 (2 *the*) (2 *act*)) (3 (4 (3 (2 *is*) (3 (2 *still*) (4 *charming*))) (2 *here*)) (2.))))

2.4. Train RNTN for Trust Sentiment

In order to create a model for recognizing a sense of trust between two individuals, it is required to initially select a dataset comprised of sentences exchanged between individuals. To this end, wide ranges of data sources are available. In this respect, providing a functional programing interface, Twitter provides access to a wide range of tweets and information about their authors. Various crawlers have been also developed for Facebook and other social networks that allow retrieval of published texts by members of that social network for free or in return for charges to researchers or businesses. A variety of text collections are similarly at hand in various academic or corporate databases that can be utilized for this purpose. Given the limitation that most of libraries developed for natural language processing have based language as the standard and formal one, and do not have proper functioning in terms of a colloquial language, a collection of emails from Enron Company was selected for the proposed method in this study. The feature of these data was that they had been published in the official and institutional context of Enron Company and had an appropriate structure to process texts and thus required less pre-processing. Steps to create a training dataset for training RNTN were as follows:

First, a set of emails was selected and a parse tree was created for each one.

In crowdsourcing platform, participants were requested to rate sense of trust hidden in each part of speech of the parse tree of each single sentence. The scoring range was from very Negative to very Positive in 5 levels.

After scoring the components of the parse trees, the participants were asked to rate receiver's level of trust in email senders and receivers within a score range from untrusted to trusted in 3 levels.

Finally the dataset of trust sentiment tree bank was created and used for training RNTN. After generating the training datasets, we trained this RNTN using the k-fold cross validation method with K = 10. In each fold, 85% of the data was used for training and 15% was used to test the outcome.

As an example, the textual email below was given to a trained RNTN to detect a sense of trust and the result was negative.

$$Please\ consider\ this:\ an\ invitation\ to\ a\ Staff\ meeting\ \&\ conference.$$

The following tree diagram in Figure 2 is a schematic output of RNTN:

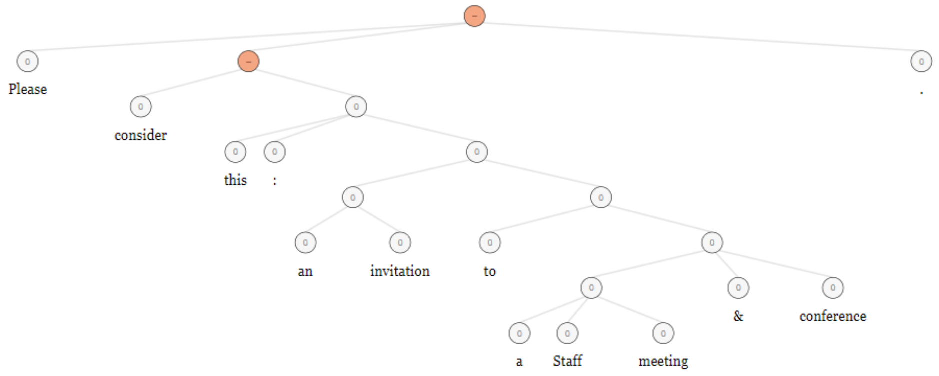


Figure 2. Example of RNTN's Output After Training for Trust.

The imperative sense in emails to remind employees of a meeting and a conference implies a negative sense of trust.

The trained model with these datasets was named as $MC(c_{i,j,k})$, and it was noted that $c_{i,j,k}$ was the kth content sent from ith user to jth one. So, the sense of trust in kth sentence sent from ith user to jth one was defined through interpreting S_{t_k} as follows:

$$S_{t_k} = MC(c_{i,j,k})$$

2.5. Hidden Markov Model

By the end of the previous section, sense of trust could be estimated in the form of a number in one sentence. However, the relationship between humans is the result of a set of exchanged sentences. Therefore, estimating sense of trust in the sentences exchanged between two individuals, a sequence of numbers expressing sense of trust in sentences was obtained. Interpreting sense of trust as S_{t_k}, the sequence of values of sense of trust derived from the sentences exchanged by ith and jth users was defined via interpretation of $SS_{t_{i,j}}$ as follows:

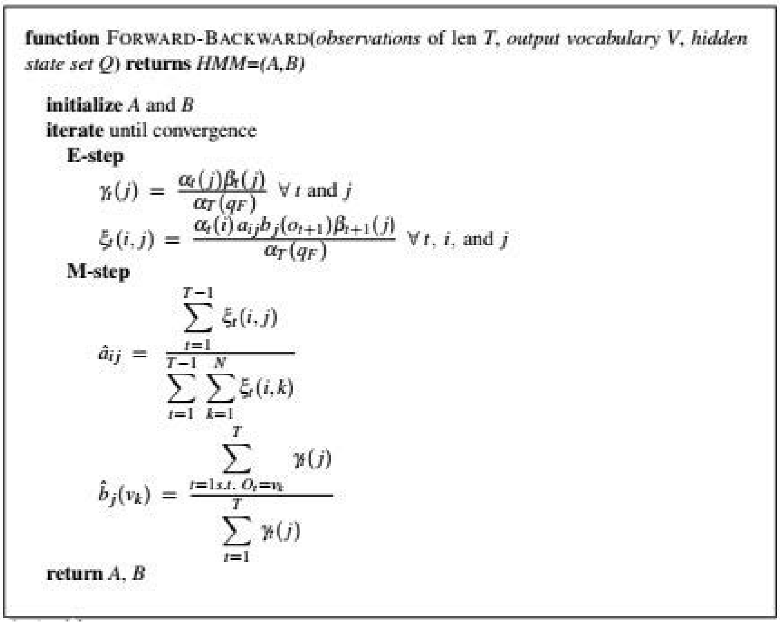
$$SS_{t_{i,j}} = \left\langle S_{t_k} \middle| S_{t_k} = MC(c_{i,j,k})\ for\ all\ k \right\rangle$$

At this point, level of trust between two individuals could be estimated by knowing this sequence of numbers. One of the best models used to classify the sequence is HMM. This model is also considered as one of the most advanced technologies in the field of machine learning which can be used to classify sequences [66].

In relation to the form of the present problem to classify sequences of numbers with a specified label, the main purpose was actually to learn HMM parameters through a sequence of observations. The basic parameters of HMM are as follows:

1. A set of states.
2. Sequence of observations.
3. State transition probabilities
4. A sequence of observation likelihoods, also called emission probabilities.
5. Initial state probabilities

Learning an HMM model is typically possible through defining intermediate variables and using Forward-Backward or Baum-Welch algorithm [67] a special case of Expectation-Maximization or EM algorithm [68]. Figure 3 illustrates this algorithm [69].



```
function FORWARD-BACKWARD(observations of len T, output vocabulary V, hidden
state set Q) returns HMM=(A,B)

  initialize A and B
  iterate until convergence
    E-step
      $\gamma_t(j) = \frac{\alpha_t(j)\beta_t(j)}{\alpha_T(q_F)}$ $\forall$ t and j
      $\xi_t(i,j) = \frac{\alpha_t(i)a_{ij}b_j(o_{t+1})\beta_{t+1}(j)}{\alpha_T(q_F)}$ $\forall$ t, i, and j
    M-step
      $\hat{a}_{ij} = \frac{\sum_{t=1}^{T-1}\xi_t(i,j)}{\sum_{t=1}^{T-1}\sum_{k=1}^{N}\xi_t(i,k)}$
      $\hat{b}_j(v_k) = \frac{\sum_{t=1 s.t. O_t=v_k}^{T}\gamma_t(j)}{\sum_{t=1}^{T}\gamma_t(j)}$
  return A, B
```

Figure 3. Example of RNTN's Output After Training for Trust.

For training HMM with the forward-backward algorithm, the following two components are required:

A collection of HMM states: In the proposed model, states refer to the same levels of trust:

$$Trust\ Levels = \{Untrusted,\ Nature,\ Trusted\}$$

Which convert into HMM states:

$$States = \{Ut,\ Nt,\ Tr\}$$

Each state is also specified by numbers:

$$States = \{1,\ 2,\ 3\}$$

A series of observations in the proposed model are as follows:

$$Observations = \left\{ SS_{t_{i,j}}\ for\ all\ i\ and\ j \right\}$$

These observations are then expressed using vocabulary of the levels of sentiment:

$$Sentiment\ Levels = \{Very\ Negative,\ Negative,\ Nature,\ Positive,\ Very\ Positive\}$$

Which is equal to:

$$Vocabulary = \{Vn,\ Ne,\ Na,\ Po,\ Vp\}$$

The following stochastic automaton represents the learning model in Figure 4.

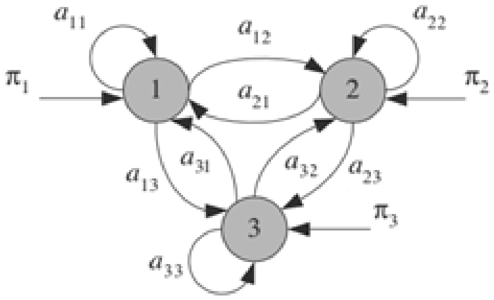
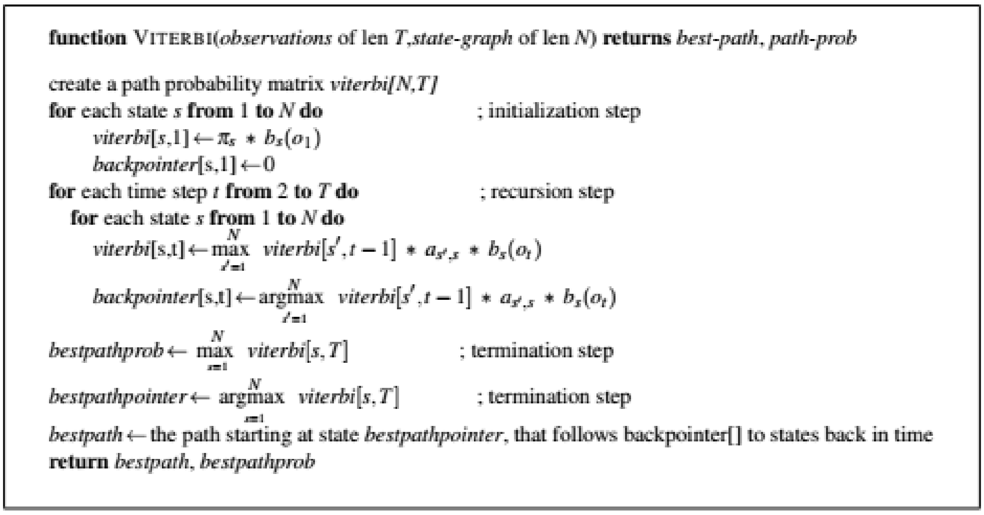


Figure 4. Stochastic automaton Representation of HMM.

To implement the model, C# programming language and Accord library were employed.

The sequence of levels of sentiments were then considered as observations and the trained HMM model was applied for the highest probability sequence of trust states with the Viterbi algorithm presented in Figure 5 [69].



```
function VITERBI(observations of len T,state-graph of len N) returns best-path, path-prob

create a path probability matrix viterbi[N,T]
for each state s from 1 to N do                        ; initialization step
    $viterbi[s,1] \leftarrow \pi_s * b_s(o_1)$
    $backpointer[s,1] \leftarrow 0$
for each time step t from 2 to T do                    ; recursion step
  for each state s from 1 to N do
    $viterbi[s,t] \leftarrow \max_{s'=1}^{N}\ viterbi[s',t-1] * a_{s',s} * b_s(o_t)$
    $backpointer[s,t] \leftarrow \operatorname{argmax}_{s'=1}^{N}\ viterbi[s',t-1] * a_{s',s} * b_s(o_t)$
$bestpathprob \leftarrow \max_{s=1}^{N}\ viterbi[s,T]$                ; termination step
$bestpathpointer \leftarrow \operatorname{argmax}_{s=1}^{N}\ viterbi[s,T]$       ; termination step
bestpath ← the path starting at state bestpathpointer, that follows backpointer[] to states back in time
return bestpath, bestpathprob
```

Figure 5. Viterby Algorithm.

2.6. SenseTrust Schema

To summarize the SenseTrust model and as clarified in the previous sections, it should be noted that this model relies on the logic that if a user feels good about exchanged content with another social network user. They are trustworthy in terms of exchanges. Tapping into the same logic, in the SenseTrust model:

- Textual content exchanged has a high volume of exchanges between social network users in the form of texts.
- To perform sentiment analysis on each statement, the outputs of researchers at Stanford University entitled as RNTN is used to discover the hidden sentiments.
- To analyze trust among social network users, based on sentiments discovered in the statements exchanged, Hidden Markov Model (HMM) is utilized.
- Both RNTN and HMM are trained with emails extracted from Enron Corporation undergoing crowdsourcing and labeling.
- To estimate trust among social network users:
  - ○ Statements exchanged among users are imported into the SenseTrust model.
  - ○ They are trained by RNTN and levels of sentiments in statements are discovered through sentiment analysis.
  - ○ Sequences of the values of hidden sentiments in statements are conveyed to the trained HMM to determine the level of trust among users.
  - ○ The SenseTrust output is trust among social network users with three levels of interpretation (Untrusted, Nature, Trusted).
- The SenseTrust model can estimate trust among users of most conventional social networking sites including Twitter, Facebook, etc. based on textual exchanges.

The schema of the SenseTrust model is as follows (Figure 6):

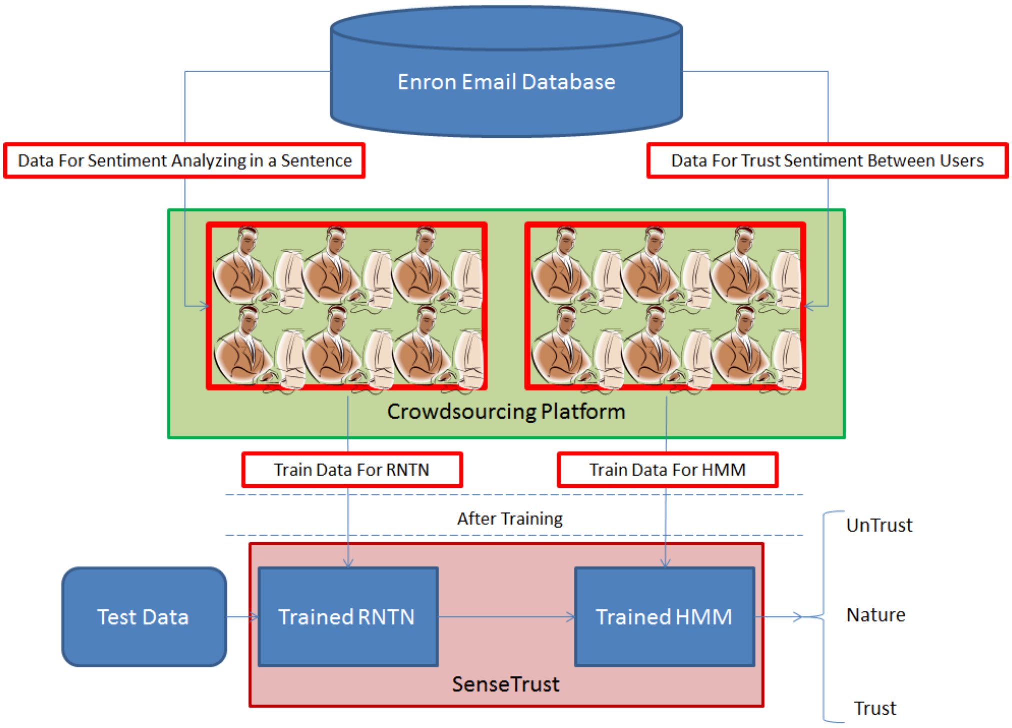


Figure 6. SenseTrust Schema.

3. Experimental Results

Similar to the training phase of the SenseTrust model, a collection of emails retrieved from Enron Corporation was used to test the system. Crowdsourcing was also performed to label the emails to reflect on senders' trust in recipients. Moreover, the emails had been labeled based on three levels of trust as considered in the training phase.

For each of the three levels, 30 email-based conversations (90 conversions in total) were included, each one encompassing at least six and ten emails as a maximum exchanged between senders and recipients.

The SenseTrust outputs compared with the labels allotted by experts at crowdsourcing for this collection of conversations are outlined in the Table 5:

Table 5. Experimental Results.

		Chats Labeled by Experts		
		Trusted	**Nature**	**Untrusted**
Chats Labeled by SenseTrust	**Untrusted**	25	4	0
	Nature	5	23	4
	Trusted	0	3	26

Given the three levels of trust and error rate introduced in the Section 2.2, it is scored as:

$$Score = 2 - Error$$

And, for the index of efficiency:

$$\text{Efficiency} \; = \frac{\sum_{k=1}^{\text{number of tests}} score\ of\ k - th\ test}{2 \times 90}$$

It can be observed that efficiency of the SenseTrust model is by 91%.

The proposed method can be also evaluated via the indices of precision, recall, F-measure, accuracy, and specificity. Such indices for the performance of the SenseTrust in terms of levels of trust and the mean score of each value are illustrated in the Table 6:

Table 6. Experimental Results in Other Indeces.

Trust Level	Precision	Recall	F-Measure	Accuracy	Specificity
UnTrusted	0.86	0.83	0.84	0.89	0.92
Nature	0.71	0.76	0.73	0.82	0.85
Trusted	0.89	0.86	0.87	0.91	0.94
Average	**0.82**	**0.81**	**0.81**	**0.87**	**0.90**

4. Discussion

The main purpose of the present study was to propose a method for estimating trust among social network users. As reviewed in Section 1.2, numerous investigations had been fulfilled in this respect. Mostly, understanding how trust is estimated among social network users and how a user shows trust towards another one is expressed in a descriptive category with terms like Trusted or Nature.

A major category of research in the field of trust in social networks is concerned with network topology, i.e., analyzing network structure of users' communications in social networks and calculating different network indices as the basis of estimating levels of trust among users. As a simple example, it is implied that, if a group of users are interpreted as nodes in a social network or they are very close or connected, that user is more trusted. Claims of these studies to estimate levels of trust merely by their structures have not been so far validated. For example, many users of online social networks who are closely related may share opposing positions or texts regarding a particular topic or context, indicating lack of trust to each other in that topic or context. Therefore, the proposed model in this study, i.e., SenseTrust, fails to rely on network topology.

Another major category of research establishes interactions among social network users as an index for estimating trust. As perceived, since trust is built on relationships and actions between two individuals, this interaction index is useful in estimating the levels of trust. Other categories of research also introduce hybrid models, but leading studies have been accomplished in this field mainly based on the interaction index and hybrid models are founded on essentials of interaction.

In the SenseTrust model, the index of interaction among social network users is the basic one for trust estimation. The assumption is in reference to this evident and humane fact that "if one person feels good about another one in terms of a topic or context, they trust these individuals in that topic or context". In one experiment, this issue was tested and it was observed that collective judgment and understanding of those participating in the experiment had confirmed this assumption. Reviewing similar works, it becomes clear that considering good sentiments between two social network users as a proxy index of trust between them is the conceptual innovation of this research.

Relying on this assumption to develop the SenseTrust model, online social networking platform was selected. Since textual exchanges are the main means of interaction in online social networks and sentiment analysis in the related literature on natural language processing and artificial intelligence is fully-fledged, the foundation of the SenseTrust model is on sentiment analysis of texts exchanged between users. Drawing on sentiment analysis of textual exchanges as the theoretical contribution of SenseTrust in the domain of trust in social network is an innovative contribution as similar research was examined.

There are two basic mainstays of trust estimation in the SenseTrust model; firstly, analysis of hidden sentiments behind texts exchanged between two social network users, secondly, trust estimation via analysis of this sequence of sentiments, which are completed by RNTN, and HMM; respectively. To train both models, the labeled data at crowdsourcing were used. The SenseTrust model was also implemented as software and then trained and tested with real data. Therefore, it was found to be superior to some similar works with merely theoretical contribution, in terms of trust in social network because of its practical implementation and contribution. Furthermore, the results of practical experiments demonstrate that the SenseTrust model has an acceptable performance in terms of different indices and it is therefore comparable to the findings of other studies in this field.

5. Conclusions and Future Works

In this study, the SenseTrust model has been introduced as a model for estimating trust among social network users. The basis for the proposed model is the selection of the index regarding how one user felt about another user as a proxy index of their trust in that user. The proposed model is also founded on interaction among social network users and deals with sentiment analysis of texts exchanged between users. Using cutting-edge technologies in the field of sentiment analysis in mature texts and technologies, sequence analysis along with implementation of the model in the form of software. The utilization of labeled real data at crowdsourcing for training models can lead to acceptable performance of the SenseTrust model in practical experiments.

In the conceptual dimension, the main contribution of this study is selecting users' sentiments towards each other as an index for estimating their trust towards each other in a social network. In the theoretical dimension, a combination of sentiment analysis of texts and analysis of numerical sequences derived from the previous phase is the most significant contribution of this research among similar works. Implementation, training, and experimental testing of the proposed model as well as calculation of various indices that can serve as the basis for judging performance and comparing the SenseTrust model with other achievements in this field is also the practical contribution of this research on estimation of trust among social network users.

The main implication of this study is changes in researchers' views towards trust in social networks, which can make future research focuses on trust in sentiment analysis or more efficient definition of proxy index for sentiments among users. Moreover, concentration on different essentials of the SenseTrust model can improve efficiency, accuracy, and other indices.

Apart from the two foundations of the SenseTrust i.e., textual sentiment analysis (in this research, RNTN was trained and used) and sentiment sequence analysis (as HMM was trained and used in this study), each one can be examined in new research for the purposes of introduction and use of other effective methods. The proposed model in this study is currently limited to analyzing texts exchanged among social network users, so use of other interactions by users such as voice and video sharing or specific actions in some online social networking sites, such as Like and Dislike and so forth can be of topics for future research. For example, providing efficient methods and models for sentiment analysis of images or audios exchanged between users in social networks can broaden the scope of the SenseTrust model. Analyzing all interactions by users including conventional text, image, and audio files and actions in social networks can thus provide a context for future research into in-depth analysis of trust in social networks.

Author Contributions: A.M., conceptualization, methodology, software, formal analysis, data curation, writing—original draft preparation, writing—review and editing; S.A.H.G., validation, writing—review and editing, supervision. Both authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: To get access to the data created during study, please contact corresponding author.

Conflicts of Interest: The authors declare no conflict of interest.

Websites List

Site 1: Accord Framework
https://www.accord-framework.net (accessed on 2 June 2021)
Site 2: Carnegie Mellon University—Enron Email Dataset
https://www.cs.cmu.edu/~enron/ (accessed on 2 June 2021)
Site 3: Wikipedia—Enron Company
https://en.wikipedia.org/wiki/Enron (accessed on 2 June 2021)

References

1. Bawa, S.; Singh, S. A privacy, trust and policy based authorization framework for services in distributed environ-ments. *Int. J. Comput. Sci.* **2007**, *1*, 85–92.
2. Nepal, S.; Paris, C.; Sherchan, W. A Survay of Trust in Social Networks. *ACM Comput. Surv.* **2013**, *45*, 1–33.
3. Rotter, J.B. A new scale for the measurement of interpersonal trust. *J. Personal.* **1967**, 651–665. [CrossRef]
4. Reay, I.; Dick, S.; Miller, J.; Beatty, P. Consumer trust in e-commerce web sites: A meta-study. *ACM Comput. Sur-Veys (CSUR)* **2011**, *43*, 1–46.
5. Dumouchel, P. Trust as an action. *Eur. J. Sociol.* **2005**, *46*, 417–428. [CrossRef]
6. Sitkin, S.B.; Burt, R.S.; Camerer, C.; Roussea, D.M. Not so different after all: A cross-discipline view of trus. *Acad. Manag. Rev.* **1998**, *23*, 393–404.
7. Takahashi, N.; Peterson, G.; Molm, L.D. Risk and trust in social exchange: An experimental test of a classical propo-sition. *Am. J. Sociol.* **2000**, *105*, 1396–1427.
8. Kollock, P. The emergence of exchange structures: An experimental study of uncertainty, commitment, and trust. *Am. J. Sociol.* **1994**, *100*, 313–345. [CrossRef]
9. Weigert, A.; Lewis, J.D. Trust as a social reality. *Soc. Forces* **1985**, *63*, 967–985.
10. Marsh, S.P. Formalising Trust as A Computational Concept. Ph.D. Thesis, University of Stirling, Scotlan, UK, 1994.
11. Mui, L. Computational Models of Trust and Reputation: Agents, Evolutionary Games, and Social Networks. Ph.D. Thesis, Massachusetts Institute of Technology, Cambridge, MA, USA, 2002.
12. Kutvonen, L.; Koutrouli, E.; Ruohomaa, S. Reputation management survey. In Proceedings of the Second International Conference on Availability, Reliability and Security (ARES'07), Vienna, Austria, 10–13 April 2007.
13. Hailes, S.; Abdul-Rahman, A. Supporting trust in virtual communities. In Proceedings of the 33rd Annual Hawaii International Con-ference on System Sciences, Maui, HI, USA, 7 January 2000.
14. Yu, B.; Venkatraman, M.; Singh, M.P. Community-based service location. *Commun. ACM* **2001**, *44*, 49–54.
15. Chen, S.; Nepal, S.; Levy, D.; Zic, J.; Yao, J. Truststore: Making amazon s3 trustworthy with services composition. In Proceedings of the 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing, Melbourne, VIC, Australia, 17–20 May 2010.
16. Nepal, S.; Hwang, H.; Zic, J.; Moreland, D. A snapshot of trusted personal devices applicable to transaction processing. *Pers. Ubiquitous Comput.* **2010**, *14*, 347–361.

17. Perrig, A.; van Doorn, L.; Khosla, P.; Seshadri, A. SWATT: Software-based attestation for embedded devices. In Proceedings of the IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 12 May 2004.
18. Li, J.; Chen, L. Revocation of direct anonymous attestation. In *Trusted Systems*; Springer: Berlin/Heidelberg, Germany, 2001; pp. 128–147.
19. Williamson, O.E. Calculativeness, trust, and economic organization. *J. Law Econ.* **1993**, *36*, 453–486. [CrossRef]
20. James, S.C. *Foundations of Social Theory*; Belknap Press of Harvard University Press: Cambridge, MA, USA, 1990.
21. Stassen, W. Your news in 140 characters: Exploring the role of social media in journalism. *Glob. Media J. Afr. Ed.* **2010**, *4*, 116–131. [CrossRef]
22. Bock, G.W.; Kuan, H.H. The collective reality of trust: An investigation of social relations and networks on trust in multi-channel retailers. In Proceedings of the ECIS 2005, Regensburg, Germany, 26–28 May 2005.
23. Holmes, J.G. Trust and the appraisal process in close relationships. *Adv. Pers. Relatsh.* **1991**, *2*, 57–104.
24. Taylor, R.K. Marketing strategies: Gaining a competitive advantage through the use of emotion. *Compet. Re-View Int. Bus. J. Inc. J. Glob. Compet.* **2000**, *10*, 146–152. [CrossRef]
25. Coleman, J.S. Social capital in the creation of human capital. *Am. J. Sociol.* **1988**, *94*, S95–S120. [CrossRef]
26. Granovetter, M.S. The strength of weak ties. *Am. J. Sociol.* **1973**, *78*, 1360–1380. [CrossRef]
27. Komiak, S.X.; Benbasat, I. Understanding customer trust in agent-mediated electronic commerce, web-mediated electronic commerce, and traditional commerce. *Inf. Technol. Manag.* **2004**, *5*, 181–207. [CrossRef]
28. Möllering, G. The nature of trust: From Georg Simmel to a theory of expectation, interpretation and suspension. *Sociology* **2001**, *35*, 403–420. [CrossRef]
29. Miles, R.E.; Creed, W.D. Organizational forms and managerial philosophies-a descriptive and analytical review. *Res. Organ. Behav. Annu. Ser. Anal. Essays Crit. Rev.* **1995**, *17*, 333–372.
30. Rubin, A.D.; Cranor, F.; Waldman, M. Publius: A robust, tamper-evident, censorship-resistant, web publishing sys-tem. In Proceedings of the 9th USENIX Security Symposium, Denver, CO, USA, 14–17 August 2000.
31. Lenzini, G.; Uusitalo, I.; Toivonen, S. Context-aware trust evaluation functions for dynamic reconfigurablein. In Proceedings of the Workshop on Models of Trust for the Web (MTW'06), Scotland, UK, 22 May 2006.
32. Bhargava, B.; Lilien, L.; Rosenthal, A.; Winslett, M.; Sloman, M.; Dillon, T.S.; Chang, E.; Hussain, F.K.; Nejdl, W.; Staab, S. The pudding of trust: Managing the dynamic nature. *IEEE Intell. Syst.* **2004**, *19*, 74–88.
33. Christianson, B.; Harbison, W.S. Why isn't trust transitive? In *Security Protocols*; Springer: Berlin/Heidelberg, Germany, 1997; pp. 171–176.
34. Singh, M.P.; Sycara, K.; Yu, B. Developing trust in large-scale peer-to-peer systems. In Proceedings of the 1st IEEE Symposium on Mul-ti-Agent Security and Survivability, Drexel, PA, USA, 31–31 August 2004; pp. 1–10.
35. Sabater, J. Trust and Reputation for Agent Societies. Ph.D. Thesis, Autonomous University of Barcelona, Barcelona, Spain, 2005.
36. Yu, B.; Singh, M.P. A social mechanism of reputation management in electronic communities. In *Cooperative Information Agents IV-The Future of Information Agents in Cyberspace*; Springer: Berlin/Heidelberg, Germany, 2000; pp. 154–165.
37. Sherchan, W.; Bouguettaya, A.; Nepal, S. A behaviour-based trust model for service web. In Proceedings of the IEEE International Conference on Service-Oriented Computing and Applications (SOCA'10), Perth, WA, Australia, 13–15 December 2010.
38. Buskens, V. The social structure of trust. *Soc. Netw.* **1998**, *20*, 265–289. [CrossRef]
39. Parsia, B.; Hendler, J.; Golbeck, J. Trust networks on the semantic web. In *Cooperative Information Agents VII*; Springer: Berlin/Heidelberg, Germany, 2003; pp. 238–249.
40. Golbeck, J.A. Computing and Applying Trust in Web-Based Social Networks. Ph.D. Thesis, University of Maryland, College Park, MD, USA, 2005.
41. Golbeck, J.A. Trust and Nuanced Profile Similarity in Online Social Networks. *ACM Trans. Web (TWEB)* **2009**, *3*, 1–33. [CrossRef]
42. Shahriari, H.R.; Mohammadhassanzadeh, H. Using User Similarity to Infer Trust Values in Social Networks Re-gardless of Direct Ratings. In Proceedings of the 9th International ISC Conference on Information Security and Cryptology, Tabriz, Iran, 13–14 September 2012; pp. 171–187.
43. Chen, H.; Wu, Z.; Zhang, Y. A social network-based trust model for the semantic web. In *Autonomic and Trusted Computing*; Springer: Berlin/Heidelberg, Germany, 2006; pp. 183–192.
44. Ziegler, C.N.; 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.
45. Hang, W.C.; Singh, M.P. Trust Based Recommendation Based on Graph Similarities. 2010. Available online: http://www.csc.ncsu.edu/faculty/mpsingh/papers/mas/aamas-trust-10-graph.pdf (accessed on 13 September 2012).
46. Hu, Y.; O'keefe, W.C.; Zuo, T. Trust computing for social networking. In Proceedings of the 6th International Conference on Infor-mation Technology: New Generations, Las Vegas, NV, USA, 27–29 April 2009.
47. Liu, L.; Webb, L.; Caverlee, S. Socialtrust: Tamper-resilient trust establishment in online communities. In Proceedings of the 8th ACM/IEEE-CS Joint Conference on Digital Libraries (JCDL'08), Pittsburgh PA, USA, 16–20 June 2008; ACM Press: New York, NY, USA, 2008.
48. Kuter, U.; Golbeck, J.A. Sunny: A new algorithm for trust inference in social networks using probabilistic confidence models. *Adv. Artif.* **2007**, *7*, 1377–1382.

49. Kim, Y.A.; Le, M.-T.; Lauw, H.W.; Lin, E.-P.; Liu, H.; Sricastava, J. Building a web of trust without explicit trust ratings. In Proceedings of the 24th IEEE International Conference on Data Engi-neering Workshop, Cancun, Mexico, 7–12 April 2008.
50. Tang, M.; Ghunaim, H.C.; Maheswaran, A. Towards a gravity-based trust model for social networking sys-tems. In Proceedings of the International Conference on Distributed Computing Systems Workshops, Toronto, ON, Canada, 22–29 June 2007.
51. Lim, E.P.; Lauw, H.W.; Le, M.T.; Sun, A.; Srivastava, J.; Kim, Y.; Liu, H. 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 July 2008.
52. Sherchan, W.; Paris, C.; Nepal, S. STrust: A trust model for social networks. In Proceedings of the 10th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom'11), Changsha, China, 16–18 November 2011.
53. Escriva, S.; Goldberg, R.; Hayvanovych, M.K.; Magdon-Ismail, M.; Szymanski, M.; Wallace, B.K.; Williams, W.A.; Adali, G. Measuring behavioral trust in social networks. In Proceedings of the IEEE International Conference on Intel-ligence and Security Informatics (ISI'10), Vancouver, BC, Canada, 23–26 May 2010.
54. Legendre, F.; Anastasiades, C.; Trifunovic, S. Social trust in opportunistic networks. In Proceedings of the INFOCOM IEEE Conference on Computer Communications Workshops, San Diego, CA, USA, 15–19 March 2010.
55. Petkevič, V. Media Sentiment Analysis for Measuring Perceived Trust in Government. *Soc. Commun. Trust Interact.* **2018**, *50*, 23–45.
56. Shaozhong, Z.; Zhong, H. Mining Users Trust from E-Commerce Reviews Based on Sentiment Similarity Analysis. *IEEE Access* **2019**, *7*, 13523–13535.
57. Alahmadi, D.; Zeng, X.-J. Improving Recommendation Using Trust and Sentiment Inference from OSNs. *Int. J. Knowl. Eng.* **2015**, *1*, 9–17. [CrossRef]
58. Socher, R.; Huval, B.; Manning, C.D.; Ng, A.Y. Semantic Compositionality through Recursive Matrix-Vector Spaces. In Proceedings of the Conference on Empirical Methods in Natural Language Processing, Edinburgh, UK, 27–31 July 2011.
59. Socher, R.; Perelygin, A.; Wu, J.Y.; Chuang, J.; Manning, C.D.; Ng, A.Y.; Potts, C. Recursive Deep Models for Semantic Compositionality Over a Sentiment Treebank. In Proceedings of the Conference on Em-pirical Methods in Natural Language Processing, Seattle, WA, USA, 18–21 October 2013.
60. Lee, L.; Pang, B. Opinion Mining and Sentiment Analysis. *Found. Trends Inf. Retr.* **2008**, *2*, 1–135.
61. Tishby, N.; Lee, L.; Pereira, F. Distributional Clustering of English Words. 1994. Available online: https://arxiv.org/abs/cmp-lg/9408011 (accessed on 24 July 2021).
62. Lee, L.; Vaithyanathan, S.; Pang, B. Sentiment Classification using Machine Learning Techniques. *Int. J. Sci. Res. (IJSR)* **2016**, *5*, 819–821.
63. Lee, L.; Pang, B. Sentiment Analysis Using Subjectivity Summarization Based on Minimum Cuts. 2004. Available online: https://arxiv.org/abs/cs/0409058 (accessed on 1 July 2021).
64. Lee, L.; Pang, B. Seeing Stars: Exploiting Class Relationships for Sentiment Categorization with Respect to Rating Scales. 2005. Available online: https://arxiv.org/abs/cs/0506075 (accessed on 1 July 2021).
65. Socher, R.; Pennington, J.; Huang, E.H.; Ng, A.Y.; Manning, C.D. Semi-Supervised Recursive Autoencoders for Predicting Sentiment Distributions. In Proceedings of the Conference on Empir-ical Methods in Natural Language Processing, Edinburgh, UK, 27–31 July 2011.
66. Alpaydin, E. *Introductio to Machine Learning*; The MIT Press: Cambridge, MA, USA; London, UK, 2010; Chapter 15.
67. Baum, L.E. An inequality and associated maximization technique in statistical estimation for probabilistic functions of Markov processes. In Proceedings of the Inequalities III: Proceedings of the 3rd Symposium on Inequalities, Los Angeles, CA USA, 1–9 September 1969.
68. Dempster, A.P.; Laird, N.M.; Rubin, D.B. Maximum likelihood from incomplete data via the EM algorithm. *J. R. Stat. Soc.* **1977**, *39*, 1–21.
69. Jurafsky, D.; Martin, J.H. *Speech and Language Processing*, 2nd ed.; Prentice Hall: Hoboken, NJ, USA, 2009.