


Article

NADAL: A Neighbor-Aware Deep Learning Approach for Inferring Interpersonal Trust Using Smartphone Data

Ghassan F. Bati ¹  and Vivek K. Singh ^{2,*}

¹ Computer Engineering Department, Umm Al-Qura University, Makkah 24381, Saudi Arabia; gfbati@uqu.edu.sa

² School of Communication and Information, The State University of New Jersey, New Brunswick, NJ 08901, USA

* Correspondence: v.singh@rutgers.edu

Abstract: Interpersonal trust mediates multiple socio-technical systems and has implications for personal and societal well-being. Consequently, it is crucial to devise novel machine learning methods to infer interpersonal trust automatically using mobile sensor-based behavioral data. Considering that social relationships are often affected by neighboring relationships within the same network, this work proposes using a novel neighbor-aware deep learning architecture (NADAL) to enhance the inference of interpersonal trust scores. Based on analysis of call, SMS, and Bluetooth interaction data from a one-year field study involving 130 participants, we report that: (1) adding information about neighboring relationships improves trust score prediction in both shallow and deep learning approaches; and (2) a custom-designed neighbor-aware deep learning architecture outperforms a baseline feature concatenation based deep learning approach. The results obtained at interpersonal trust prediction are promising and have multiple implications for trust-aware applications in the emerging social internet of things.

Keywords: deep learning; neighbor-aware deep learning; phone data; trust inference



Citation: Bati, G.F.; Singh, V.K. NADAL: A Neighbor-Aware Deep Learning Approach for Inferring Interpersonal Trust Using Smartphone Data. *Computers* **2021**, *10*, 3. <http://dx.doi.org/10.3390/computers10010003>

Received: 29 November 2020

Accepted: 21 December 2020

Published: 24 December 2020

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2020 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

Interpersonal trust is defined as “a willingness to accept vulnerability or risk based on expectations regarding another person’s behavior” [1]. It facilitates multiple socio-technical systems with implications for social and physiological well-being. The emerging growth of social networks, mobile computing, and the social internet of things necessitates understanding and modeling people’s interpersonal trust as they interact with one another to undertake tasks in domains ranging from shared economy to media consumption. For instance, a person may want to rent out homes only to somebody they trust or prefer to receive news stories recommended by their trusted ties. Broadly, an ability to understand and model trust using machine learning and phone-based data would have implications for multiple social and sensor-based systems being studied under the unified vision of human-centered “Internet of Things”, sometimes also called the “Internet-of-People” [2].

Understanding human behavioral and physiological states at scale could also revolutionize the study of trust in the social sciences. Traditional studies on trust had to be undertaken in lab settings or deal with only self-reported data. Thus, these approaches contend with various issues such as scalability, cost, and self-report bias [3,4]. Hence, as highlighted in the smartphone psychology manifesto, “smartphones could transform psychology even more profoundly than PCs and brain imaging did [5].” Today, as billions of individuals use smartphones as the primary internet connection, social connection, and IoT coordination device, they leave traces of behavioral data as they interact with them. Hence, there has been a tremendous interest in mining mobile sensor-based behavioral data to automatically infer different attributes about a person (e.g., their personality traits) or their relationships (e.g., identify their colleagues) [6–10].

One useful concept utilized in this process is the idea of homophily, i.e., birds of a feather flock together, which motivates the use of data from one's neighbors to better infer specific properties about them. While this idea has already been applied in ubiquitous and social computing literature to infer some individuals' properties, it is yet to be utilized to infer some properties of their relationships [11]. We posit that social relationships are also affected by neighboring relationships within the same network. Hence, utilizing the behavioral data from neighboring relationships could provide vital clues for better inference of trusted relationships in a network.

To make this inference of trusted ties, we use the recently emerging direction of using deep learning approaches for sensor and ubiquitous data [12–15]. However, while current deep learning architectures are typically well-designed to handle low-level neighborhood notions within an entity of interest (e.g., neighboring pixels within an image or the next Bluetooth reading within a stream), they typically do not consider the inter-entity notions of a neighborhood. While this may be less of an issue when dealing with intra-entity problems, e.g., labeling objects within an image, this becomes a significant limitation in tackling problems related to human relationships as they are almost always affected by neighboring relationships within the same network. Hence, there is a need to custom-design deep learning architectures that can effectively utilize behavioral data from neighboring edges to predict some properties (e.g., interpersonal trust) for the target edge.

Taking this into cognizance, this work makes two contributions:

1. First effort to use neighboring relationships' behavioral features for inferring interpersonal trust between two people.
2. First effort to custom-design a deep learning architecture that leverages neighboring relationship properties to better model interpersonal trust.

2. Related Work

Interpersonal trust has significance in various fields (e.g., computer science, information science, sociology, psychology, political science, economy) [16–18]. In this effort, the related work directly associated with this work's scope, i.e., modeling interpersonal trust in interconnected social settings using phone sensor-based data, is discussed. We discuss the related work, which facilitates clarifying the terminology and suggests various ways to measure interpersonal trust, focusing on computational models of trust. Additionally, we review the current use of one's peers' information to model individuals and use smartphone data and machine learning to understand individuals or relationships.

2.1. Trust as a Field of Study

Trust is essential in understanding human behaviors in several fields whose presence preserves various relations and produces much good [19]. For example, trust may enable low-cost informal agreements instead of expensive complex contracts [20]. Furthermore, individuals dwelling in more trusting communities feel habitually happier and are more content with their lives, more involved with their local communities, and have more caring friends [21]. In computational settings, trust plays a role in influencing online purchases in online commerce [22]. Trust is also an essential mediator in managing individuals' security, dealing with online service agreements, and undertaking mobile commerce transactions [23–26].

Although trust is prominent in various fields, a precise scientific definition is not obvious [27]. Interpersonal trust, trust propensity, and trustworthiness are various terms that are frequently confused [19,28,29]. To alleviate such confusion, we present the following definitions for these terms:

Trust propensity: “a dispositional willingness to rely on others” [28].

Trustworthiness: “the willingness of a person B to act favorably towards a person A, when A has placed an implicit or explicit demand or expectation for action on B” [19].

Interpersonal trust: “a willingness to accept vulnerability or risk based on expectations regarding another person's behavior” [1].

A person's trust propensity measures the overall willingness to take risks and people's overall expectations to behave well generally. In contrast, interpersonal trust is something specific to a particular relationship between two people. In this work, we focus on interpersonal trust.

2.2. Measuring Interpersonal Trust

Several recent works have made efforts to elicit a person's propensity to trust other people [27,30]. Nevertheless, many of these efforts have either mainly focused on demographic traits (e.g., gender, race) or used lab-based experiments (e.g., Dictator Game) [31,32]. Unfortunately, using such approaches for understanding trust scores often constrains studies' scope to factors that can be elicited in the lab settings. Other approaches include asking users survey questions. For instance, some efforts have directly asked users if they trust a person "X" [33]. While direct, such approaches are often critiqued on the validity of the metric. Human beings are known not to be very good at answering questions directly about such metrics. A direct question involving "trust" as an operative term leaves it open for each person to interpret what they mean by "trusting person X". Hence, some of the efforts ask pointed scenario-based questions (e.g., "Would you ask person X to babysit for you?"). Lastly, there are research efforts that define behavioral metrics for interpersonal trust. For instance, Adali et al. define retweeting a message from person X as a metric for trusting person "X" [34]. While practical and useful, such a definition has little support from the traditional social science trust literature. In this work, we follow Shmueli et al. [27] and study the interconnections between a survey-based definition of interpersonal trust and phone-based behavioral features. The key contributions here lie in proposing a *neighbor-aware* deep learning approach, allowing for automatic inference of trust scores based on phone-based interaction features. We hope that the results based on trust's current operationalization will motivate further work with varied methods for quantifying trust.

2.3. Computational Modeling of Trust

Numerous recent efforts have attempted to model trust in computational settings. Notable examples include the following: Adali et al. describe a computational model for interpersonal trust in [35], which can treat trust as a social tie between a trustor and a trustee [34]. In their model, trust develops as a part of an emotional relationship between a pair of people similar to the concepts of emotional and relational trust. Likewise, Farrahi and Zia have studied the dissemination of trust as a probabilistic stochastic process [36]. Roy et al. have suggested using a pair of complementary measures to determine trust scores of actors in social networks [37]. Zolfaghar and Aghaie have studied the development of trust in social networks [38]. The authors in [39] tackle the task of trust-aware recommendation provision using deep learning. Similarly, the authors in [40] use deep learning to identify trusted ties in online social networks. A key insight in this line of work is transitivity between trusted ties which has intersections with our proposed *neighbor aware* approach. However, this line of work is quite different from ours. While "link prediction" focuses on identifying unknown trust scores based on known trust scores in the network, we focus on the task of trust score prediction based on behavioral or communication (call, SMS (short message service), face-to-face) data. Even when using neighbors' communication features, we do not assume that their corresponding trust scores are available to the predicting algorithm.

There have been a couple of recent studies focusing on studying trust using mobile or ubiquitous sensors [27,30]. Shmueli et al. [27] focus on shallow learning to model interpersonal trust but do not have neighbors' notion of modeling trust scores. Bati et al. [30] focus on modeling trust propensity, a person's trait to trust others in general, rather than trusting a particular person. Bati et al. [30] also do not use deep learning or neighbors' notion to model trust scores.

2.4. Modeling Individuals and Relationships Based on Their Neighbors

Homophily is a well-studied concept in the social sciences and social network analysis. Simply put, one often makes friends with others who are similar to them [41]. This idea has been studied in offline and online social networks to understand an individual's attributes ranging from personality traits to movie preferences [11,42–44]. Some early results in ubiquitous computing literature have recently utilized a neighbor's properties to infer an individual's personality traits and actions [45]. For instance, Lane et al. [45] have studied “the various social phenomena and environmental factors that cause people to develop correlated behavioral patterns, especially within communities connected by strong social ties”. Simply put, while current efforts (e.g., [11,45]) argue that people are affected by other people in their network, we posit that relationships are also affected by other relationships in the network.

2.5. Using Phone Logs and Machine Learning to Understand Individuals and Relationships

Smartphones have become a primary communication and internet connection device used by billions of people globally. The majority of contemporary smartphones are equipped with several sensors, and there exists significant literature utilizing smartphone sensors to automatically infer individuals' cooperation propensities and personality traits [7,46–48]. Indeed, this work builds upon a recent line of work in ubiquitous computing literature on phoneotypic modeling [47], which defines a phoneotype as the “composite of an individual's traits as observable via a mobile phone”. Hence, it argues that a combination of phone-based behavioral features could build a unique signature for an individual that can predict facets of the individual's life (e.g., propensity to cooperate).

There has been a rich array of recent work on modeling human activities using sensors and deep learning [13,14,49,50]. These efforts range in applications from health to activities of daily living and employ a wide variety of deep learning approaches, including deep neural networks (DNN), convolutional neural networks (CNN), autoencoders, restricted Boltzmann Machines, restricted neural networks (RNN), and long-short term memory (LSTM). Rather than activity recognition, where the output varies over time, interpersonal relationships are typically modeled over a cumulative period. This implies that only one score is predicted (and one learning instance) even if the dataset contains one-year worth of human activities. This changes the learning instances available and the kind of architecture suitable for many of the problems at hand.

3. Datasets

The MIT (Massachusetts Institute of Technology, Cambridge, MA, USA) Friends and Family dataset was part of a year-long study utilizing the “Funf” framework [51] and surveys to collect data about the lives of 130 individuals (about 64 families), recruited in two batches: Spring and Fall 2010, living in a families-only housing on the campus of a North American University. All community members were couples, in which at least one of the members was affiliated with this university. The community comprised over 400 residents, half of whom had children. The community had many ties of friendship among its members. Thus, most of the participants had kids or at least were couples living in close proximity with kids. The Funf platform can collect various types of data although we focus here on the call, SMS, and Bluetooth logs and the trust surveys that determine trust ties between the subjects [27].

To accommodate the various definitions of trust occurring in three important hypothetical but daily life-pertinent scenarios (health, wealth, and family), the participants were asked the following three questions [27]:

1. “Would you ask person X for help in sickness?”
2. “Would you ask person X for a hundred-dollar loan?”
3. “Would you ask person X for babysitting?”

While we have access to the answer to question (3) for all participants, we have answers to the first two questions only for the participants from the Spring batch, not the

Fall batch. We note this as a limitation of this work and report the results for both datasets (i.e., smaller N with all questions and larger N with only question #3). We refer to the dataset with all the three questions about health, wealth, and family as TrustHWF and the second dataset as TrustF throughout the paper.

To capture several aspects of human relations in the dataset, Bluetooth (BT), calls, and SMS logs were collected. Explicitly, using call logs facilitate understanding the synchronous interaction between two individuals despite their distance. Additionally, using SMS logs enable understanding the non-synchronous interaction between two individuals regardless of their distance. Bluetooth logs facilitate understanding of the participants' spatial patterns by approximating face-to-face interactions between the participant and others. For each pair of users, the number of co-location scans is counted and used as a proxy for the actual time they spend in physical proximity. The logs get updated every five minutes (to detect social interaction while preserving the phone's battery) based on scanning for adjacent Android phones [27].

We focus only on the interactions within the community (e.g., disregarding external calls). The participants collectively have recorded the following interactions during the study, as shown in Table 1.

Table 1. Summary of calls, SMS, and BT Made by the users during the study.

Feature	Total	Mean	Median
BT	474,340	4351.74	3864
Call	58,554	476.05	407
SMS	17,369	231.59	88

3.1. Mobile Phone (Smartphone) Data Features

Trust and socio-mobile behavior have been connected in previous research, both conceptually and empirically. For instance, an individual's propensity to trust others has been connected conceptually with social capital and empirically with phone data [30]. Similarly, interpersonal trust has been connected conceptually with the strength of ties and empirically with phone data [27,52]. Interpersonal trust, as reported by the i th person A_i , is often a function of the trust propensity of person A_i and the interactions between person A_i and the target entity B_i .

Here, we consider a global network $G = \langle V; E \rangle$, which consists of nodes V and edges E , where nodes V refer to all participants in the study and E refers to all edges drawn between participants (e.g., A_i, B_i) based on interactions observed between them. In the rest of this work, we consider the nearest neighbors based on Bluetooth (proxy for face-to-face) scans. However, the proposed approach is generic and will work with other types of interactions, such as calls, SMS messages, Facebook messages, and retweeting. We are interested in modeling the "interpersonal trust score" for a specific edge $(A_i \rightarrow B_i) \in E$ based on the behavioral features observed for node $A_i \in V$ as well as the edge $(A_i \rightarrow B_i) \in E$. Further, let U_{i1} and U_{i2} be the two closest neighbors of node A_i , e.g., those with the highest number of Bluetooth co-locations with A_i . We posit that knowing the behavioral features for edges $(U_{i1} \rightarrow B_i)$ and $(U_{i2} \rightarrow B_i)$ will help improve the quality of prediction for the trust beyond that possible with the behavioral data for A_i and $(A_i \rightarrow B_i)$. For simplicity of notation, we write U_{i1} and U_{i2} as U_1 and U_2 here onward.

To define behavioral features that represent the nodes and edges using social-mobile data, we have surveyed the related literature which focuses on connecting phone behavior with social outcomes (e.g., [27,46,53,54]). For instance, some researchers have suggested that social capital is connected with phone use behavior [53] and trust [55]. Social capital often contains two variations: bridging and bonding [56]. Thus, we link the notions of weak and strong ties to bridging and bonding social capital to infer interpersonal trust [25,47,57]. We use call, SMS, and Bluetooth (BT) logs to represent the features that carry "social traits" concepts for mobility and interpersonal trust and their interconnections [36,53,58]. Based

on the BT, call, and SMS metadata collected from the app, we define the following set of phone-based features ($n = 23$).

Note that while many deep learning approaches do not utilize “handcrafted” features, there remain multiple scholars who have argued that theory-driven (or handcrafted) features are useful even when using deep learning architecture [59–61]. While availing of the sophisticated non-linear interactions between features using the neural networks, such approaches still allow system designers to better understand the rationale for their models. Further, such features allow for a more interpretable comparison between shallow and deep learning approach results and work well in scenarios where the available number of instances is not exceptionally large [62]. In the current scenario, where there is only one interpersonal relationship score per edge, we have opted to use handcrafted features at the input layer even though they may interact for over a year. This also allows for a comparison across deep and shallow learning strategies for using neighbor’s sensor data for inferring interpersonal trust—neither of which has been reported in the past literature.

The features have been designed to capture two different aspects—(1) the traits (e.g., trust propensity) of the person A_i who is giving the trust rating, and (2) the relationship between A_i and B_i . While the traits of the person A_i indeed remain common across all A_i relationships, this is only one part of the equation; the second part is the specific relationship between the two nodes (e.g., A_i and B_i). This mimics real-world scenarios, where an individual’s traits when combined with their interactions with others, shape the trusted and non-trusted ties they have with others. In terms of the network representation described earlier, we try to capture the person’s traits using *node properties* and the relationship using *edge properties*.

3.1.1. Node Properties

Social Activity Level. Social activity level signifies a person’s activity determined in this work by counting the number of exchanged phone calls, SMS messages, and Bluetooth scans. An active user is expected to have a high count of social activity level [47]. Several works have linked an individual social activity level with their social capital and/or trust. Additionally, high social activity has been associated with dropping relational uncertainty and is considered a means of establishing trust in interpersonal relationships [24,27,63,64]. Thus, we consider the following features:

$$\text{Social Activity (BT, call, SMS)} = \sum \text{Activity}_i$$

where “ i ” is the individual being considered and activity is the number of BT scans, calls, and SMS that the individual is part of.

Diversity. We quantify the total number of calls, SMS messages, and Bluetooth scans in the previous set of features. Here, we also determine the diversity measured as Shannon Entropy for each one of them. Various studies have associated diversity with multiple personal well-being outcomes and personality traits [65,66]:

$$D_i = - \sum_j p_{ij} \log_b p_{ij}$$

where p_{ij} is the proportion of social events relating to person “ i ” and contact “ j ”, whereas “ b ” is the total amount of these interactions.

Tie Strength. Earlier works have correlated strength of ties and trust propensity [30]. The same literature underlines the importance of preserving relations with a person’s strong and weak ties. Each may yield various types of social capital, and probably, over time, interpersonal trust. Following Williams [57], we link the notions of “bonding” and “bridging” social capital to those of “strong” and “weak” ties proposed by Granovetter and other researchers [25,67–69]. We posit that the relative spread (or concentration) of communication with strong (respectively weak) ties might be an indicator of trusting other individuals. It is estimated that an individual dedicates at least 33% of their time with their

top-third most recurrent contacts (a proxy for strong ties) [47]. Nevertheless, a great score like 90% might indicate a person's preference to deliberately engage more with strong ties more willingly than spreading the communication effort more equally among all ties. Thus, we define the following features:

$$\text{Strong/Weak Tie Ratio (SWTR)} = \frac{\left(\frac{\sum \text{Communication with Highest 1/3 Contacts}}{\sum \text{All Communication}} \times 100 \right)}{\left(\frac{\sum \text{Communication with Lowest 1/3 Contacts}}{\sum \text{All Communication}} \times 100 \right)}$$

Reciprocity. A vital property of a person's social behavior is the ease of communicating with others. Previous research has suggested that the approachability of individuals is related to social capital levels [53]. Moreover, social capital has been associated with trust [55]. Thus, we compute the ratio of incoming to outgoing calls and SMS text messages.

$$\text{In Out Ratio (Call, SMS) : IOR} = \frac{\text{Incoming Communication Count}}{\text{Outgoing Communication Count}}$$

Loyalty. Loyalty means how frequently participants engage with their favorite people in terms of calls, SMS messages, and Bluetooth scans. Past research has connected this loyalty feature with individual well-being and propensity to trust [30,70]. Precisely, we calculate the percentage of time spent with their top three frequented communication (BT, call, SMS) out of all communication.

$$\text{Loyalty} = \frac{\sum \text{Time Spent with Top Three Contacts}}{\sum \text{Time Spent with All Contacts}} \times 100$$

Temporal Rhythms. Preceding research has associated circadian cycles, Dark Triad (i.e., narcissism, Machiavellianism, and psychopathy) and trust [71,72]. An individual's chronotype, i.e., the propensity for a person to sleep at a specific time during a day-and/or-night period (24-h), has been linked with cheating and Machiavellianism [73]. Additionally, Cai et al. have shown the importance of temporal dynamics in social trust prediction [74]. Hence, we consider temporal rhythms to be useful for predicting interpersonal trust.

The daily business hours in the USA are 8 AM–5 PM; thus, we compute daily patterns of activity and the differences between different phases of the day by defining the following features:

$$\text{Diurnal Activity Ratio (BT, Call, SMS) DAR} = \frac{\sum \text{Activity (8AM to 5PM)}}{\sum \text{Activity (5PM to 8AM)}}$$

Another layer of characterization for the abovementioned two states of the daily activity ratio is added to give more insights out of these circadian rhythms by enumerating the weekdays (Monday to Friday) to weekends (Saturday and Sunday) communication (BT, call, SMS) ratio:

$$\text{Weekday/Weekend Activity Ratio (BT, Call, SMS) WWAR} = \frac{\sum \text{Activity (Weekdays)}}{\sum \text{Activity (Weekends)}}$$

3.1.2. Edge Properties

Past research has connected the number of interactions between users conceptually with the strength of ties [4,67] and this feature has empirically been found to be predictive of interpersonal trust [27]. Hence, we consider the social activity level based on the three modalities (BT, call, SMS) as the features to characterize the edges in the network:

$$\text{Social Activity (BT, Call, SMS)} = \sum \text{Activity}_{ij}$$

where “i” and “j” are the individuals whose relationship is being considered. The features are represented visually in Figure 1 and summarized in Table 2.

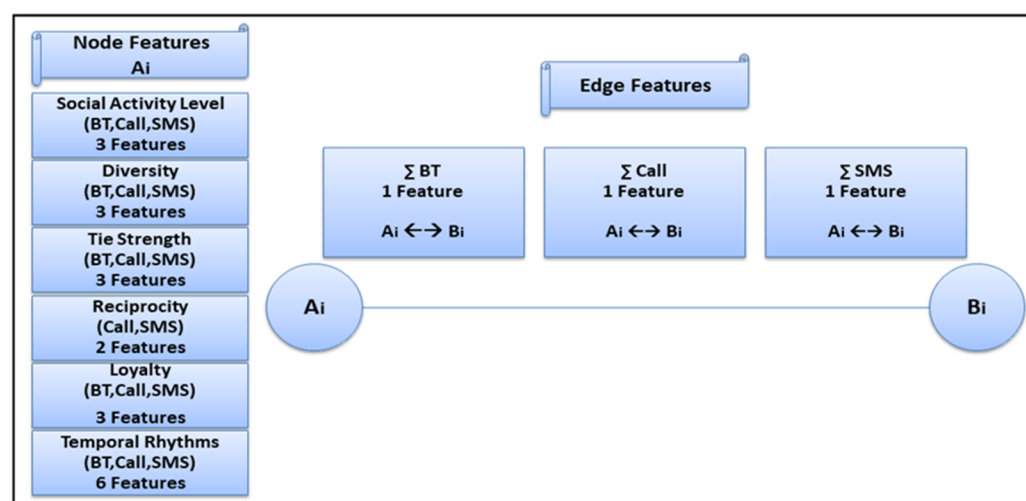


Figure 1. Summary of phone-based features in a network representation.

Table 2. Definition of phone-based features used in this paper.

Node/Edge	Feature Name	Definition
Node Features	Social Activity Level 3 Features	Social Activity (BT, Call, SMS) = $\sum Activity_i$
	Diversity 3 Features	$D_i = -\sum_j p_{ij} \log_b p_{ij}$
	Tie Strength 3 Features	Strong/Weak Tie Ratio (SWTR) = $\frac{(\frac{\sum \text{Communication with Highest 1/3 Contacts}}{\sum \text{All Communication}} \times 100)}{(\frac{\sum \text{Communication with Lowest 1/3 Contacts}}{\sum \text{All Communication}} \times 100)}$
	Reciprocity 2 Features	In Out Ratio (Call, SMS): $IOR = \frac{\text{Incoming Communication Count}}{\text{Outgoing Communication Count}}$
	Loyalty 3 Features	$Loyalty = \frac{\sum \text{Time Spent with Top Three Contacts}}{\sum \text{Time Spent with All Contacts}} \times 100$
	Temporal Rhythms 6 Features	Diurnal Activity Ratio (BT, Call, SMS) DAR = $\frac{\sum Activity (8AM to 5PM)}{\sum Activity (5PM to 8AM)}$ Weekday/Weekend Activity Ratio (BT, Call, SMS) WWAR = $\frac{\sum Activity (Weekdays)}{\sum Activity (Weekends)}$
Edge Features	Social Activity Level 3 Features	Social Activity (BT, Call, SMS) = $\sum Activity_{ij}$

4. Method

4.1. Dealing with Class Imbalance in the Datasets

To clean our datasets (TrustF and TrustHWF), we have removed all instances without any logs for BT scans, Calls, and SMS messages altogether, resulting in 13,163 instances for TrustF. 12,998 of these instances have a low interpersonal trust (zero), whereas the rest of the instances (165) have a high interpersonal trust (one). For TrustHWF, 2492 instances have a low interpersonal trust (zero), whereas the rest of the instances (447) have a high interpersonal trust (one). Here, following Shmueli et al. [27], we define trust level as high when the respondents answer any of the three questions about health, wealth, or family as true.

We notice significant skew in the dataset towards not trusting in both datasets, as shown in Figure 2. This seems reasonable as individuals are likely to trust only a small ratio of all the people they encounter.

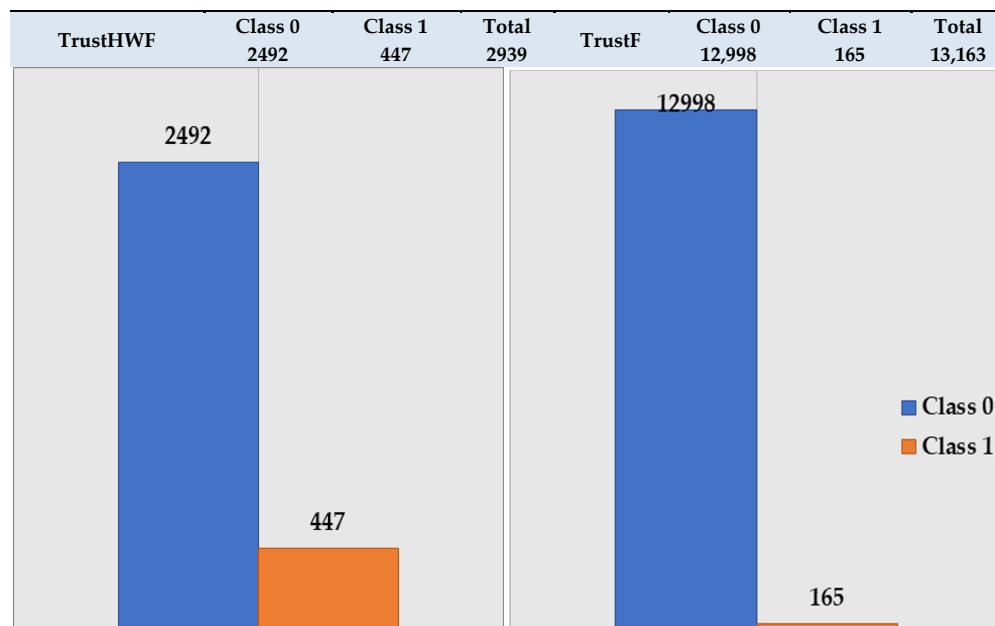


Figure 2. Class imbalance of the interpersonal trust scores (TrustHWF and TrustF).

The most common way of dealing with the class imbalance in datasets is to (artificially) balance the training set to allow for better learning opportunities before the learned model is tested out on the imbalanced test set as is expected in the real world. The most common ways for balancing a training dataset are (1) over-sampling, (2) under-sampling, and (3) a combination of over and under-sampling [75]. Here, we split the dataset into two (train/test) subsets (70/30%), respectively, and chose SMOTE+Tomek links [76] to balance the training data. In this technique, SMOTE [77] is used first which generates new minority class instances. These minority class instances are based on a hyperspace projection and are not direct copies of the existing instances. Then, Tomek's links method is used to under-sample the dataset whose primary motivation is to balance the training data and remove noisy examples lying on the wrong side of the decision border [76]. We have chosen these resampling approaches following various recent studies showing their potential in enhancing the accuracy of the classification in similar contexts [78,79]. We use the implementation as described in [75], which is inspired by [80].

4.2. Identifying Appropriate Neighbors for Better Interpersonal Trust Modeling

In this work, we would like to study the novel idea of determining neighbors' impact in enhancing shallow and deep learning algorithms' performance in inferring interpersonal trust. Following the results in [27], we consider face-to-face interactions to be the most important determinants for considered trusted relationships and, hence, identify the two nearest neighbors in terms of face-to-face frequency (Bluetooth) interactions. Note, however, that the proposed network-based inference approach is generic and can work with other types of interactions (e.g., calls, Facebook messages).

The underlying intuition of using a neighbor's information can be applied to any arbitrary number of neighbors. However, including all the neighbors would quickly become exorbitant in terms of data size and the effects of additional user data are unlikely to be useful after a threshold. Given the significance of triads as an important building block in social network literature [81,82] and "triangulation" in signal processing literature,

we focus on using data from two additional neighbors to have a total of three edges whose data is considered in this work.

To study the impact of adding the two similar neighbors based on the number of Bluetooth scans in predicting one's interpersonal trust, we have created the following additional features, as presented in Figure 3.

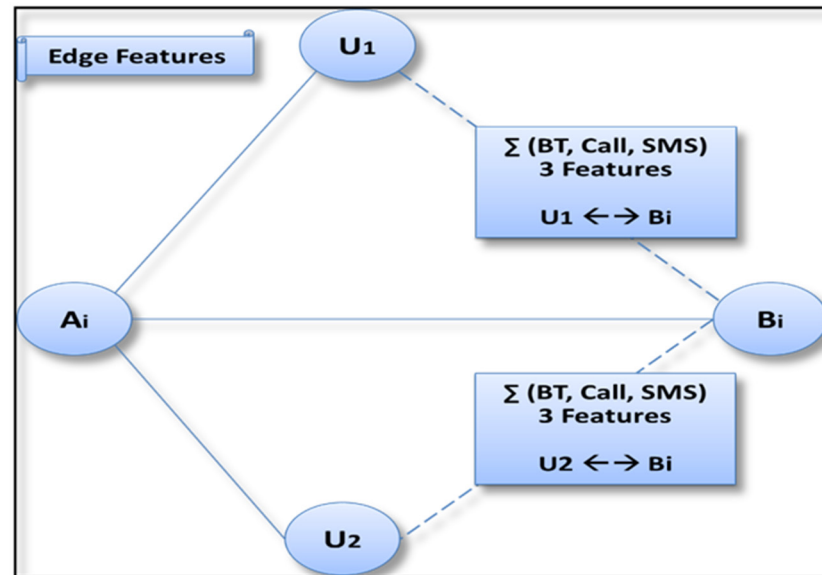


Figure 3. Additional phone-based features in a network representation after adding two neighbors (nodes U1 and U2).

4.3. NADAL: A Neighbor-Aware Deep Learning Architecture

In this work, we build upon recent work in ubiquitous computing literature by Radu et al. [83], which defines a novel deep learning approach to utilize multimodal sensor data for human activity recognition. An important insight from their work was the idea to avoid both the extremes of fusion techniques, i.e., early fusion (feature concatenation) and late fusion (decisions derived separately from single modalities are combined in the final layer). Instead, they argue a case to allow for two kinds of hidden layers. The first of which are targeting a specific sensor type, and the second of which are capturing unified concepts across sensor types. In their structure, separate architectures are constructed for each modality to learn initially sensor-specific information before the resulted concepts are unified through representations that bridge across all sensors (i.e., shared modality representations).

We consider the neighbors' data to be an additional "channel" or modality of information regarding the phenomena of interest. In that sense, our work follows that of Radu et al. [83]. However, the "channels" in our setup are quite different from those in Radu et al. [83]. While in their context, different channels were observing the same activities via different modalities, in our case the additional channels provide contextual information regarding different activities, which nevertheless could indirectly influence the prediction task at hand.

Specifically, we consider the interpersonal trust between user A_i and a target B_i (see Figure 3) to be a function of the behavioral features that characterize the edge ($A_i \rightarrow B_i$) (e.g., the number of phone Calls between them) as well as the node A_i (e.g., number of overall phone Calls made by A_i). While the node properties give a clue to the personality or the traits of A_i , the edge properties characterize the relationship between A_i and B_i .

Now, let us also consider two neighbors for A_i : U_1 and U_2 . We posit that the properties of the edges connecting these users with B_i , i.e., $\{U_1 \rightarrow B_i; U_2 \rightarrow B_i\}$ could provide additional context on the relationship ($A_i \rightarrow B_i$) and thus be useful to predict the interpersonal trust

between them. However, we do not expect the node properties (e.g., personality or trust propensity) of U_1 and U_2 to influence the relationship between A_i and B_i significantly.

Hence, taking inspiration from Radu et al. [83] and considering the different application contexts here, we define a novel architecture, as shown in Figure 4. This architecture builds upon feedforward neural networks and contains separate architectural branches for user A_i 's node and edge features as well as U_1 's and U_2 's edge features without any inter-branch connections between layers until later unifying cross-channel layers that connect the node and edge features for the A_i , and the three types of edges, respectively. It allows for the node properties of user A_i to go through several layers of neural networks to allow for different features and the interactions among them to become part of the model. The same thing happens to the other “channels” of information, i.e., the edge properties of $(A_i \rightarrow B_i)$, $(U_1 \rightarrow B_i)$, and $(U_2 \rightarrow B_i)$. Each of these properties goes through several layers of neural networks without any interaction across channels. Next, to learn the (potentially non-linear) interaction effects between the A_i 's node and edge parameters, the corresponding layers are merged and the resulting layer passes through multiple layers of networks to allow for learning of the appropriate parameters. Similarly, there could be interaction effects between the edge-based features for $(A_i \rightarrow B_i)$, $(U_1 \rightarrow B_i)$, and $(U_2 \rightarrow B_i)$, which can be learned by combining the corresponding layers and letting them pass through two layers of neural networks.

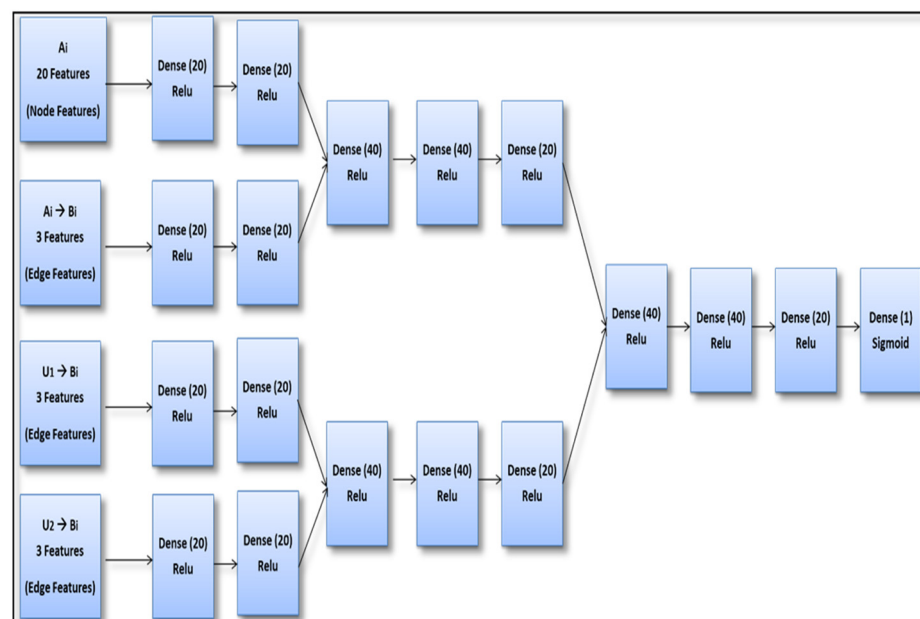


Figure 4. NADAL architecture schematic.

5. Results

5.1. Classification Results

We used Scikit-learn [84] and Keras [85] running in Google Colab Notebooks to build various models capable of automatically inferring the interpersonal trust of a user classified into two classes: “Low Interpersonal Trust (0)” or “High Interpersonal Trust (1)”. We split all datasets into a 70% training dataset and a 30% test set. We analyze the results with and without sampling, as well as with and without considering the neighboring edges. Lastly, we consider both shallow and deep learning methods, namely: decision trees, random forest, logistic regression, standard feature concatenation-based deep neural network (FC-DNN), and our proposed NADAL architecture.

5.1.1. TrustHWF Dataset

We consider multiple variants of the dataset to quantify the effect of various factors on the classification performance. Table 3 compares all (subsets of) TrustHWF dataset considered in this work and the number of features/rows in each one of them. (Note that while the training data (70%) is balanced between the two classes by creating artificial samples (SMOTE+Tomek), the testing (30%) is done on the imbalanced dataset as consistent with the real-world scenario where such an algorithm is likely to be applied.).

Table 3. Summary of subsets of the TrustHWF dataset considered in this study.

Dataset	Neighbor Awareness	Features	Instances	Class 0	Class 1
ORIGINAL	Only Main Edge (100%)	23	2939	2492	447
ORIGINAL	Main Edge + Two Neighbors (100%)	29	2939	2492	447
TRAINING SET: AS-IS	Only Main Edge (70%)	23	2057	1739	318
TRAINING SET: AS-IS	Main Edge + Two Neighbors (70%)	29	2057	1739	318
TRAINING SET: After Resampling	Only Main Edge (70%)	23	3388	1694	1694
TRAINING SET: After Resampling	Main Edge + Two Neighbors (70%)	29	3388	1694	1694
TEST SET	Only Main Edge (30%)	23	882	753	129
TEST SET	Main Edge + Two Neighbors (30%)	29	882	753	129

1. Sampling Technique: As-Is vs. SMOTE+Tomek Resampling

As mentioned in Section 4.1, we try to counter the problem of class imbalance by creating more balanced training datasets using SMOTE+Tomek resampling. To quantify the performance difference based on the resampling, we run two versions for each experiment—one with and one without the resampling.

2. Neighbor Awareness: Individual Path (Non-Neighbor-Aware) vs. Neighbor-Aware

We consider the models' performance if they only utilize the individual node and its edge connecting the target node features vs. utilizing the edge data from two of the closest neighbors. While all the individual path approaches had access to 23 features (20 node features + 3 edge features), the neighbor-aware approaches had access to 29 (20 node features + 3×3 edge features). While the difference in the number of features made little impact on the architectures for shallow learning approaches and FC-DNN, the NADAL architecture was adapted to consider only the layers that lie in the path of the abovementioned 23 features for the computation.

3. Machine Learning Approach: Shallow Learning (Random Forest) vs. Deep Learning (FC-DNN and NADAL)

The first step in the classification process is to compare multiple shallow learning algorithms for predicting interpersonal trust to select the best one to be compared to deep learning approaches, as shown in Table 4. Note that AUCROC stands for area under the receiver operating characteristic curve and Acc stands for accuracy. While a higher score is better for each of these metrics generally, multiple researchers have suggested in contradiction of using classification accuracy to interpret results in highly imbalanced datasets [86,87]. For instance, a simple baseline (Majority Zero-R) algorithm which classifies all ties as "not trusted" will achieve an accuracy of 84.79% in TrustHWF dataset and 98.75% in TrustF dataset. However, such an algorithm would be useless in practice. Hence, we

use AUCROC, which balances the majority's performance and the minority class as the primary metric to compare algorithms.

Table 4. Average results of interpersonal trust using various shallow algorithms and sampling methods (TrustHWF). Data in bold shows the best results.

Sampling Approach	Algorithmic Approach	Individual Path (Non-Neighbor-Aware)		Neighbor-Aware	
		Acc	AUCROC	Acc	AUCROC
AS-IS	Decision Tree	60.29%	67.78%	60.69%	67.99%
AS-IS	Logistic Regression	85.15%	49.87%	85.26%	50.25%
AS-IS	Random Forest	61.87%	68.90%	62.64%	69.03%
SMOTE+Tomek	Decision Tree	61.81%	66.84%	64.07%	67.33%
SMOTE+Tomek	Logistic Regression	69.05%	63.56%	66.33%	63.58%
SMOTE+Tomek	Random Forest	61.93%	69.00%	62.32%	69.13%

As can be seen, logistic regression performs the worst in all four combinations of paths and sampling approaches. Random forest is the best in terms of consistently achieving the highest AUCROC compared to decision tree and logistic regression in all four combinations of paths and sampling approaches.

Next, we consider three types of machine learning approaches. First is random forest as a representative of shallow algorithms, which will be useful for comparison. Next is the baseline deep learning approach, which builds upon feature concatenation in the first layer (FC-DNN). Lastly, the NADAL approach, which has been custom-designed to capture the interactions between neighboring nodes' edges.

After running each experiment 10 times, the average results summarized in Table 5 show the following trends:

Table 5. Average results of interpersonal trust using various classification and sampling methods (TrustHWF). Data in bold shows the best results.

Sampling Approach	Algorithmic Approach	Individual Path (Non-Neighbor-Aware)		Neighbor-Aware	
		Acc	AUCROC	Acc	AUCROC
AS-IS	Random Forest	61.87%	68.90%	62.64%	69.03%
AS-IS	FC-DNN	85.36%	53.66%	85.31%	55.41%
AS-IS	NADAL	85.34%	59.40%	84.90%	68.98%
SMOTE+Tomek	Random Forest	61.93%	69.00%	62.32%	69.13%
SMOTE+Tomek	FC-DNN	47.31%	62.58%	47.57%	64.01%
SMOTE+Tomek	NADAL	61.29%	68.08%	62.11%	70.38%

For FC-DNN, we passed all the features through a multilayer perceptron (23/40/40/20/40/40/1), all activated by ReLu (rectified linear unit) except the output layer that was activated by Sigmoid with a 16 batch size and 50 epochs as presented in Figure 5. For NADAL, the features were passed through different layers, as shown in (Figure 4). All layers in NADAL are activated by ReLu except the output layer which is activated by sigmoid with a 16 batch size and 50 epochs.

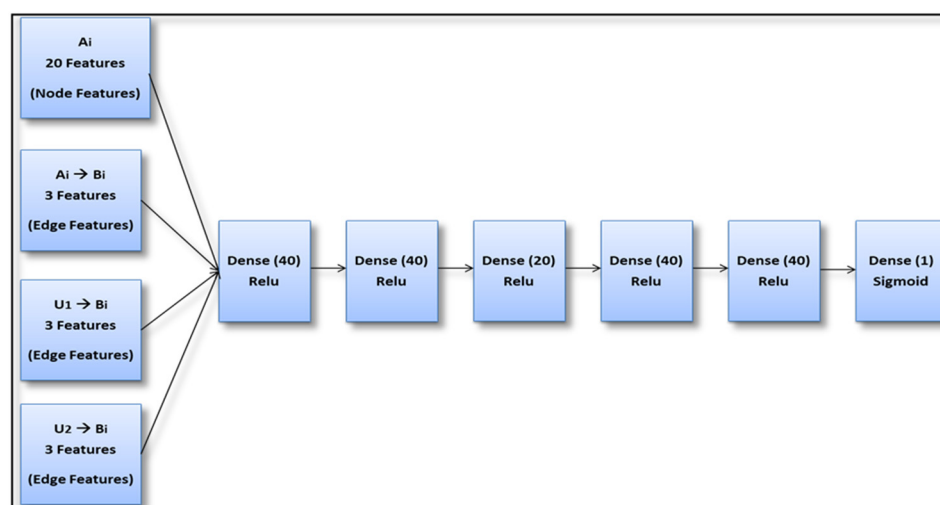


Figure 5. Standard feature concatenation based deep neural network (FC-DNN) architecture schematic.

For the same algorithmic approach and level of neighbor awareness, the models created with SMOTE+Tomek re-sampling scored higher in AUCROC. This trend is consistent with the expectation and recent research on dealing with imbalanced datasets [86]. When considering the SMOTE+Tomek results (lower half of the table), we notice that the neighbor-aware approaches consistently outperformed the non-neighbor-aware approaches. The proposed architecture (NADAL) outperformed the shallow learning approach and the baseline deep-learning approach within the neighbor-aware approaches. The best performing algorithm overall is the one with SMOTE+Tomek sampling, neighbor-aware features and NADAL deep learning architecture which is found to be statistically significantly better using two-tailed unpaired *t*-tests (at $\alpha = 0.05$ level) than all comparisons with (Random Forest and FC-DNN) algorithmic approaches together with different data consideration (i.e., Individual Path vs. Neighbor-Aware). This outcome shows the importance of using *neighboring edge properties* and *custom-designed deep learning architecture* (NADAL) for inferring interpersonal trust between two people, thus supporting the two key contributions of this work.

However, we note that this model still has a relatively modest performance (70.38% AUCROC). We posit that this may be because machine learning approaches, especially deep learning approaches, tend to need large datasets before they start performing well. Acknowledging this as a limitation, we move to the larger TrustF dataset to examine various models' performance over a larger dataset.

5.1.2. TrustF Dataset

Table 6 shows all (subsets of) TrustF dataset and the number of features/rows in each one of them, which follows the same approach described in Section 5.1.1.

Table 6. Summary of subsets of TrustF dataset considered in this study.

Dataset	Neighbor Awareness	Features	Instances	Class 0	Class 1
ORIGINAL	Only Main Edge (100%)	23	13,163	12,998	165
ORIGINAL	Main Edge + Two Neighbors (100%)	29	13,163	12,998	165
TRAINING SET: AS-IS	Only Main Edge (70%)	23	9214	9103	111
TRAINING SET: AS-IS	Main Edge + Two Neighbors (70%)	29	9214	9103	111
TRAINING SET: After Resampling	Only Main Edge (70%)	23	18,170	9085	9085
TRAINING SET: After Resampling	Main Edge + Two Neighbors (70%)	29	18,168	9084	9084
TEST SET	Only Main Edge (30%)	23	3949	3895	54
TEST SET	Main Edge + Two Neighbors (30%)	29	3949	3895	54

Table 7 shows that the decision tree performs the worst in all four paths and sampling approaches. Between random forest and logistic regression, both perform better than the other in two of the four scenarios. However, random forest is better at achieving a consistently high AUCROC in all four combinations of paths and sampling approaches.

Table 7. Average results of interpersonal trust using various shallow algorithms and sampling methods (TrustF). Data in bold shows the best results.

Sampling Approach	Algorithmic Approach	Individual Path (Non-Neighbor-Aware)		Neighbor-Aware	
		Acc	AUCROC	Acc	AUCROC
AS-IS	Decision Tree	98.55%	67.58%	98.57%	69.05%
AS-IS	Logistic Regression	98.61%	49.99%	98.63%	50.00%
AS-IS	Random Forest	92.48%	79.84%	93.12%	81.08%
SMOTE+Tomek	Decision Tree	93.04%	76.11%	93.47%	77.88%
SMOTE+Tomek	Logistic Regression	77.94%	80.60%	78.12%	81.60%
SMOTE+Tomek	Random Forest	93.78%	77.85%	94.67%	78.94%

Next, we consider three types of machine learning approaches again. First is random forest; next is the baseline deep learning approach (FC-DNN); and lastly the NADAL approach.

Table 8 shows the average results of running experiments with each of the abovementioned settings 10 times. It compares the representative shallow method (random forest) with the proposed deep learning approach (NADAL) as well as a baseline deep learning approach (FC-DNN).

Table 8. Average results of interpersonal trust using various classification and sampling methods (TrustF). Data in bold shows the best results.

Sampling Approach	Algorithmic Approach	Individual Path (Non-Neighbor-Aware)		Neighbor-Aware	
		Acc	AUCROC	Acc	AUCROC
AS-IS	Random Forest	92.48%	79.84%	93.12%	81.08%
AS-IS	FC-DNN	85.37%	50.72%	98.63%	60.48%
AS-IS	NADAL	98.64%	51.31%	98.67%	85.39%
SMOTE+Tomek	Random Forest	93.78%	77.85%	94.67%	78.94%
SMOTE+Tomek	FC-DNN	73.67%	78.28%	93.35%	82.16%
SMOTE+Tomek	NADAL	92.54%	90.63%	94.55%	93.23%

The results summarized in Table 8 show the following trends. For the same algorithmic approach and level of neighbor awareness, the models created with SMOTE+Tomek re-sampling scored higher in AUCROC. The only exception was the Random Forest. When considering the SMOTE+Tomek results (lower half of the table), we notice that the deep learning approaches (both FC-DNN and NADAL) outperform the shallow learning approach (random forest). This finding is again along expected lines as deep learning approaches tend to have more opportunity to capture linear and non-linear associations between different features and create comprehensive models.

Further, the neighbor-aware approach yields better performance in both shallow and deep machine learning approaches. All comparisons between the same algorithmic approaches but different data considerations (i.e., individual path vs. neighbor-aware) showed that the neighbor-aware approaches obtained higher scores. In the case of NADAL and random forest, these gains were found to be statistically significant using two-tailed unpaired *t*-tests (at $\alpha = 0.05$ level). This outcome validates the first major contribution of this work, i.e., proposing the use of neighboring edge properties for inferring interpersonal trust between two people, whether in shallow or deep learning.

Lastly, the proposed deep learning architecture (NADAL) was statistically significantly higher than a baseline deep learning (FC-DNN) and the Random Forest shallow learning approach when using the neighboring edge properties, which validates the second contribution. This finding suggests that early fusion of features might not allow for the same channel's interrelationships to be learned adequately without other channels' influence. The stepwise unification of different channels across the architecture seems to have provided better opportunities for the social channels to learn both intra-channel and inter-channel relationships.

The highest overall AUCROC score of 93.23% was obtained using SMOTE+Tomek sampling, neighbor-aware features, and NADAL architecture. A score of 93.23% indicates that the model could learn both the majority and minority classes reasonably well and could be useful in practice where the interpersonal trust needs to be inferred using phone-based metadata. Lastly, the noticeable improvement in the models' performance that has access to more training data (TrustF compared to TrustHWF) suggests that the proposed approach might work well in scenarios where there are a large number of rows in the dataset. A scenario that we expect to become increasingly common in the future.

6. Discussion

6.1. Methodological Considerations

The work presented here tackles the problem of inferring interpersonal trust automatically using phone log data. Such a problem requires dealing with highly imbalanced datasets and also takes place in a socially rich setting. Hence, this work proposes and empirically tests multiple techniques to improve automatic prediction quality. While a SMOTE+Tomek approach allows better learning based on a balanced training set, the neighbor-aware approach allows for the use of neighboring connections' data for better inference. Finally, the growth in such data allows for deep learning techniques to obtain

better performance. However, the architectures for deep learning need to be defined in a manner that is responsive to the task's nature. In particular, the NADAL architecture, which allows for learning appropriate features from neighboring edges while also giving due credit to the primary node in question, was found to yield the best results. As the first effort in this direction, we have chosen to use deep neural networks (DNN) using artificial neural networks (ANN), which are relatively simple and well-studied in the deep learning literature. The positive results obtained here on utilizing neighboring relationships motivate the exploration of other techniques for future work.

6.2. Privacy of User Data and Ethical Considerations

This study's data come from the MIT Friends and Family study [51], which has been adopted by multiple research groups to study questions pertaining to social and ubiquitous computing. We use a version of the dataset where all data were anonymized and hashed. Under no circumstance was the content of the calls or SMS messages available to the authors. We recognize the ethical concerns related to the automatic generation of scores to quantify human ties and interpersonal trust. Similar concerns have been raised in the past for the automatic generation of mental health scores for individuals or even survey-based quantification of interpersonal relationships [88]. In each case, the potential positives and negatives of the approach need to be weighed.

Whom one trusts is a critical mediator for almost all goods, services, and information that one procures or exchanges in technology-mediated spaces. The neighbor-aware approach yields higher confidence in inferring trusted ties in networked settings and hence can have significant implications on the flow of goods, services, and information. While access to neighbor's data is not typically feasible for an end-user, access to neighbor-based information is often available to the central organizations providing the network for transmission of goods, services, or information. This includes studies where data is collected in organizational settings (e.g., in companies and campus communities), or as available to social networking companies (e.g., Twitter, Facebook), mobile or mobile service providers (e.g., AT&T, Orange, Apple, Google) and trust-based recommendation sites (e.g., Epinions).

Nevertheless, we acknowledge potential privacy issues in the above approach. We strongly recommend an opt-in approach for the collection and use of such data. Next, we would like to raise awareness of the possibilities of using neighbor aware approaches for higher accuracy in inferring interpersonal trust. While waiting for the development of better-accepted privacy and ethics policies, we believe that it takes various studies like this to facilitate a broader understanding of the visions of using ubiquitous data and enrich the discussion in the research community around them [89,90]. Overall, this paper's findings give confidence that the use of neighboring relationship data to identify trusted ties is practical and useful, and this represents one vital way to move the literature forward.

6.3. Limitations

The current study has some limitations. Firstly, it has a relatively small sample size of 130 individuals. Hence, we are careful not to generalize the results until they are re-verified with a larger sample population. Another limitation is the sample's homogeneity. Although the sample's homogeneity stops us from generalizing the results to larger populations, it enables isolating socio-mobile behavior as a predictor. The final limitation is using a specific question-based trust metric in this work, including the one with a single question in the TrustF dataset, due to missing data in the first two questions in the version available to us. We notice that the proposed approach's performance is modest with the smaller (TrustHWF) dataset but increases quite noticeably with the availability of more data. This finding suggests that the proposed approach might work well in scenarios where there exist a large number of rows in the dataset—something which is likely to become increasingly common in the future.

Despite these limitations, this study's value lies in the new ground it breaks in multiple ways. To our knowledge, there have been no previous studies undertaken that utilize a neighbor-based approach to infer interpersonal trust. Correspondingly, the proposed NADAL architecture is the first deep learning-based attempt to utilize neighboring relationship properties to better infer aspects associated with a primary relationship. We hope that the results obtained in this work will motivate more work that applies the abovementioned techniques to settings with diverse trust measurement methods and sampled populations.

6.4. Implications

With more validation, this line of work might have several implications for individuals and communities. The users who voluntarily opt-in to such automated interpersonal trust scoring apps could receive improved and tailored recommendations for social activities, news, and mobile commerce apps; whom one trusts is a critical mediator for almost all goods and services that one exchanges in networked settings. For instance, while sharing health and exercise information with others has been shown to improve health outcomes [91], most positive outcomes are obtained when sharing such data with trusted ties [27]. Similarly, while participation in multiple shared tasks (e.g., sharing security camera footage for neighborhood safety, peer-to-peer file transfer) has significant societal benefits, a peer-to-peer notion of trust is essential to enabling such applications. Lastly, inferring trusted ties is important for internet content providers to recommend better products and services. Hence, with enhancements, the proposed automatic approach can become a vital cog in the technology-mediated lives of millions of individuals [92].

At a communal level, such apps might complement the need to run costly yearly surveys to assess the trust-based "state of the nation", as proposed by [20]. As an alternative, automated approaches might be used to create a real-time nation-wide trust census facilitating the decision-making process. Moreover, understanding the phenomenon of interpersonal trust and its "in the wild" dynamics at scale can noticeably advance the literature in various fields (e.g., economics, psychology) that study trust. For instance, this work underscores the networked structure's role (e.g., strong/weak ties, neighboring ties) and temporal variations in the development of interpersonal trust.

7. Conclusions and Future Work

In this work, we have proposed a new approach to automatically infer interpersonal trust via phone sensor-based features with a deep learning approach. This is the first effort to suggest and validate the use of behavioral features from neighboring relationships to better predict the interpersonal trust ties of the target relationship. The above problem's best results were obtained with the larger TrustF dataset based on a novel deep learning architecture (NADAL), which efficiently uses neighboring relationship data yielding an AUCROC of 93.23%. Hopefully, these results will motivate more research that leverages ubiquitous sensing data in studying the links between socio-mobile behavioral data and interpersonal trust using diverse approaches applied in various settings.

We plan to extend this work in the future by studying the impact of demographic features (e.g., gender) on our model while keeping an eye on the fairness of the machine learning processes. There are also opportunities for improving the work by creating more advanced deep learning architectures that are also neighbor-aware. With enhancements, the proposed approach can support multiple applications in domains ranging from well-being to the shared economy. More generally, the approach presented here could allow for better modeling of social relationships based on ubiquitous sensing and support a trust-enabled internet of things.

Author Contributions: Conceptualization: G.F.B. and V.K.S.; methodology: G.F.B. and V.K.S.; software: G.F.B.; validation: G.F.B. and V.K.S.; formal analysis: G.F.B. and V.K.S.; investigation: G.F.B. and V.K.S.; resources: G.F.B. and V.K.S.; data curation: G.F.B. and V.K.S.; writing—original draft preparation: G.F.B.; writing—review and editing: G.F.B. and V.K.S.; visualization: G.F.B.; supervision: V.K.S.; project administration: G.F.B. and V.K.S.; funding acquisition: G.F.B. and V.K.S. Both authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Restrictions apply to the availability of these data. Data was obtained from [MIT Media lab] and are available [from real-tycommons.media.mit.edu/friendsdataset4.html].

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

References

1. Borum, R. The Science of Interpersonal Trust. Available online: https://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1573&context=mhlp_facpub (accessed on 11 August 2018).
2. Miranda, J.; Mäkitalo, N.; Garcia-Alonso, J.; Berrocal, J.; Mikkonen, T.; Canal, C.; Murillo, J.M. From the Internet of Things to the Internet of People. *IEEE Internet Comput.* **2015**, *19*, 40–47. [CrossRef]
3. Sundsøy, P. Big Data for Social Sciences: Measuring patterns of human behavior through large-scale mobile phone data. *arXiv* **2017**, arXiv:1702.08349.
4. Giles, J. Computational social science: Making the links. *Nature* **2012**, *488*, 448–450. [CrossRef]
5. Miller, G. The smartphone psychology manifesto. *Perspect. Psychol. Sci.* **2012**, *7*, 221–237. [CrossRef]
6. Eagle, N.; Pentland, A.S. Reality mining: Sensing complex social systems. *Pers. Ubiquitous Comput.* **2006**, *10*, 255–268. [CrossRef]
7. De Montjoye, Y.A.; Quoidbach, J.; Robic, F.; Pentland, A. Predicting personality using novel mobile phone-based metrics. In Proceedings of the 6th International Conference on Social Computing, Behavioral-Cultural Modeling, and Prediction, Washington, DC, USA, 2–5 April 2013.
8. Qin, T.; Shangguan, W.; Song, G.; Tang, J. Spatio-Temporal Routine Mining on Mobile Phone Data. *ACM Trans. Knowl. Discov. Data* **2018**, *12*, 1–24. [CrossRef]
9. Yabe, T.; Sekimoto, Y.; Tsubouchi, K.; Ikemoto, S. Cross-comparative analysis of evacuation behavior after earthquakes using mobile phone data. *PLoS ONE* **2019**, *14*, e0211375. [CrossRef]
10. Bosse, S.; Engel, U. Real-Time Human-In-The-Loop Simulation with Mobile Agents, Chat Bots, and Crowd Sensing for Smart Cities. *Sensors* **2019**, *19*, 4356. [CrossRef]
11. De Salve, A.; Guidi, B.; Ricci, L.; Mori, P. Discovering Homophily in Online Social Networks. *Mob. Netw. Appl.* **2018**, *23*, 1715–1726. [CrossRef]
12. Hossain, H.M.S.; Al Haiz Khan, M.A.; Roy, N. DeActive: Scaling Activity Recognition with Active Deep Learning. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* **2018**, *2*, 1–23. [CrossRef]
13. Peng, L.; Chen, L.; Ye, Z.; Zhang, Y. AROMA: A Deep Multi-Task Learning Based Simple and Complex Human Activity Recognition Method Using Wearable Sensors. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* **2018**, *2*, 1–16. [CrossRef]
14. Wang, J.; Chen, Y.; Hao, S.; Peng, X.; Hu, L. Deep Learning for Sensor-based Activity Recognition: A Survey. *arXiv* **2017**, arXiv:1707.03502. [CrossRef]
15. El Mougy, A. Character-IoT (CIoT): Toward Human-Centered Ubiquitous Computing. In *Character Computing*; El Bolock, A., Abdelrahman, Y., Abdennadher, S., Eds.; Springer International Publishing: Cham, Switzerland, 2020; pp. 99–121. ISBN 978-3-030-15953-5.
16. Evans, A.M.; Revelle, W. Survey and behavioral measurements of interpersonal trust. *J. Res. Personal.* **2008**, *42*, 1585–1593. [CrossRef]
17. Sullivan, J.L.; Transue, J.E. The Psychological Underpinnings of Democracy: A Selective Review of Research on Political Tolerance, Interpersonal Trust, and Social Capital. *Annu. Rev. Psychol.* **1999**, *50*, 625–650. [CrossRef]
18. Tanis, M.; Postmes, T. A social identity approach to trust: Interpersonal perception, group membership and trusting behaviour. *Eur. J. Soc. Psychol.* **2005**, *35*, 413–424. [CrossRef]
19. Ben-Ner, A.; Halldorsson, F. Trusting and trustworthiness: What are they, how to measure them, and what affects them. *J. Econ. Psychol.* **2010**, *31*, 64–79. [CrossRef]
20. Ermisch, J.; Gambetta, D.; Laurie, H.; Siedler, T.; Uhrig, S.C.N. Measuring people's trust. *J. R. Stat. Soc. Ser. A* **2009**, *172*, 749–769. [CrossRef]
21. Dunbar, R.I.M. Breaking Bread: The Functions of Social Eating. *Adaptive Human Behavior and Physiology* **2017**, *3*, 198–211. [CrossRef]
22. Sahi, G.K.; Sekhon, H.S.; Quareshi, T.K. Role of Trusting Beliefs in Predicting Purchase Intentions. *Int. J. Retail. Distrib. Manag.* **2016**, *44*, 860–880. [CrossRef]
23. Kagal, L.; Finin, T.; Joshi, A. Trust-based security in pervasive computing environments. *Computer* **2001**, *34*, 154–157. [CrossRef]
24. Golbeck, J. (Ed.) *Computing with Social Trust*; Springer Science & Business Media: New York, NY, USA, 2008.
25. Granovetter, M.S. The Strength of Weak Ties. *Am. J. Sociol.* **1973**, *78*, 1360–1380. [CrossRef]

26. Han, K.; He, Y.; Xiao, X.; Tang, S.; Gui, F.; Xu, C.; Luo, J. Organizing an Influential Social Event Under a Budget Constraint. *IEEE Trans. Knowl. Data Eng.* **2019**, *31*, 2379–2392. [\[CrossRef\]](#)
27. Shmueli, E.; Singh, V.K.; Lepri, B.; Pentland, A. Sensing, understanding, and shaping social behavior. *IEEE Trans. Comput. Soc. Syst.* **2014**, *1*, 22–34. [\[CrossRef\]](#)
28. Colquitt, J.A.; Scott, B.A.; LePine, J.A. Trust, Trustworthiness, and Trust Propensity: A Meta-Analytic Test of Their Unique Relationships with Risk Taking and Job Performance. *J. Appl. Psychol.* **2007**, *92*, 909–927. [\[CrossRef\]](#) [\[PubMed\]](#)
29. McKnight, D.H.; Chervany, N.L. Trust and distrust definitions: One bite at a time. *Trust Cyber-Soc.* **2001**, *2246*, 27–54.
30. Bati, G.F.; Singh, V.K. “Trust Us”: Mobile Phone Use Patterns Can Predict Individual Trust Propensity. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, Montreal, QC, Canada, 21–26 April 2018; p. 330.
31. Barclay, P. Trustworthiness and Competitive Altruism Can Also Solve the “Tragedy of the Commons”. *Evol. Hum. Behav.* **2004**, *25*, 209–220. [\[CrossRef\]](#)
32. Exadaktylos, F.; Espín, A.M.; Brañas-Garza, P. Experimental Subjects Are Not Different. *Sci. Rep.* **2013**, *3*, 1213. [\[CrossRef\]](#)
33. Al-Oufi, S.; Kim, H.-N.; El Saddik, A. A Group Trust Metric for Identifying People of Trust in Online Social Networks. *Expert Syst. Appl.* **2012**, *39*, 13173–13181. [\[CrossRef\]](#)
34. Adali, S.; Escrivá, R.; Goldberg, M.; Hayvanovych, M.; Magdon-Ismail, M.; Szymanski, B.; Wallace, W.; Williams, G. Measuring behavioral trust in social networks. In Proceedings of the International Intelligence and Security Informatics (ISI), Vancouver, BC, Canada, 23–26 May 2010.
35. Kelton, K.; Fleischmann, K.R.; Wallace, W.A. Trust in digital information. *J. Am. Soc. Inf. Sci. Technol.* **2008**, *59*, 363–374. [\[CrossRef\]](#)
36. Farrahi, K.; Zia, K. Trust reality-mining: Evidencing the role of friendship for trust diffusion. *Hum. Cent. Comput. Inf. Sci.* **2017**, *7*, 4. [\[CrossRef\]](#)
37. Roy, A.; Sarkar, C.; Srivastava, J.; Huh, J. Trustingness & trustworthiness: A pair of complementary trust measures in a social network. In Proceedings of the IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), San Francisco, CA, USA, 18–21 August 2016.
38. Zolfaghar, K.; Aghaie, A. Evolution of trust networks in social web applications using supervised learning. *Procedia Comput. Sci.* **2011**, *3*, 833–839. [\[CrossRef\]](#)
39. Deng, S.; Huang, L.; Xu, G.; Wu, X.; Wu, Z. On Deep Learning for Trust-Aware Recommendations in Social Networks. *IEEE Trans. Neural Netw. Learn. Syst.* **2016**, *28*, 1164–1177. [\[CrossRef\]](#) [\[PubMed\]](#)
40. Liu, F.; Liu, B.; Sun, C.; Liu, M.; Wang, X. Deep belief network-based approaches for link prediction in signed social networks. *Entropy* **2015**, *17*, 2140–2169. [\[CrossRef\]](#)
41. Bonchi, F. Influence Propagation in Social Networks: A Data Mining Perspective. In Proceedings of the 2011 IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology, Lyon, France, 22–27 August 2011; p. 2.
42. Bisgin, H.; Agarwal, N.; Xu, X. Investigating homophily in online social networks. In Proceedings of the Web Intelligence and Intelligent Agent Technology (WI-IAT), 2010 IEEE/WIC/ACM International Conference, Toronto, ON, Canada, 31 August–3 September 2010; Volume 1, pp. 533–536.
43. Olson, D.V.A. The Influence of Your Neighbors’ Religions on You, Your Attitudes and Behaviors, and Your Community. *Sociol. Relig.* **2019**, *80*, 147–167. [\[CrossRef\]](#)
44. Fudolig, M.I.D.; Bhattacharya, K.; Monsivais, D.; Jo, H.-H.; Kaski, K. Link-centric analysis of variation by demographics in mobile phone communication patterns. *PLoS ONE* **2020**, *15*, e0227037. [\[CrossRef\]](#) [\[PubMed\]](#)
45. Lane, N.D.; Li, P.; Zhou, L.; Zhao, F. Connecting personal-scale sensing and networked community behavior to infer human activities. In Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing, Seattle, WA, USA, 13–17 September 2014; pp. 595–606.
46. Khan, W.Z.; Xiang, Y.; Aalsalem, M.Y.; Arshad, K. Mobile Phone Sensing Systems: A Survey. *IEEE Commun. Surv. Tutor.* **2013**, *15*, 402–427. [\[CrossRef\]](#)
47. Singh, V.K.; Agarwal, R.R. Cooperative phoneotypes: Exploring phone-based behavioral markers of cooperation. In Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing, Heidelberg, Germany, 12–16 September 2016; pp. 646–657.
48. Ponciano, V.; Pires, I.M.; Ribeiro, F.R.; Villasana, M.V.; Teixeira, M.C.; Zdravevski, E. Experimental Study for Determining the Parameters Required for Detecting ECG and EEG Related Diseases during the Timed-Up and Go Test. *Computers* **2020**, *9*, 67. [\[CrossRef\]](#)
49. Guan, Y.; Plötz, T. Ensembles of Deep LSTM Learners for Activity Recognition using Wearables. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* **2017**, *1*, 1–28. [\[CrossRef\]](#)
50. Krishna, K.; Jain, D.; Mehta, S.V.; Choudhary, S. An LSTM Based System for Prediction of Human Activities with Durations. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* **2018**, *1*, 1–31. [\[CrossRef\]](#)
51. Aharon, N.; Pan, W.; Ip, C.; Khayal, I.; Pentland, A. Social fMRI: Investigating and shaping social mechanisms in the real world. *Pervasive Mob. Comput.* **2011**, *7*, 643–659. [\[CrossRef\]](#)
52. Adali, S. *Modeling Trust Context in Networks*; Springer: New York, NY, USA, 2013.
53. Singh, V.K.; Ghosh, I. Inferring Individual Social Capital Automatically via Phone Logs. *Proc. ACM Hum. Comput. Interact.* **2017**, *1*, 1–12. [\[CrossRef\]](#)

54. Rauber, J.; Fox, E.B.; Gatys, L.A. Modeling patterns of smartphone usage and their relationship to cognitive health. *arXiv* **2019**, arXiv:1911.05683.
55. Putnam, R. Social capital: Measurement and consequences. *Can. J. Policy Res.* **2001**, *2*, 41–51.
56. Putnam, R.D. Bowling alone: America's declining social capital. *J. Democr.* **1995**, *6*, 65–78. [CrossRef]
57. Williams, D. On and Off the Net: Scales for Social Capital in an Online Era. *J. Comput. Mediat. Commun.* **2006**, *11*, 593–628. [CrossRef]
58. Yakoub, F.; Zein, M.; Yasser, K.; Adl, A.; Hassanien, A.E. Predicting personality traits and social context based on mining the smartphones SMS data. In *Intelligent Data Analysis and Applications*; Springer: Berlin/Heidelberg, Germany, 2015; pp. 511–521.
59. Jin, L.; Gao, S.; Li, Z.; Tang, J. Hand-Crafted Features or Machine Learnt Features? Together They Improve RGB-D Object Recognition. In Proceedings of the 2014 IEEE International Symposium on Multimedia, Taichung, Taiwan, 10–12 December 2014; pp. 311–319.
60. Li, W.; Manivannan, S.; Akbar, S.; Zhang, J.; Trucco, E.; McKenna, S.J. Gland segmentation in colon histology images using handcrafted features and convolutional neural networks. In Proceedings of the 2016 IEEE 13th International Symposium on Biomedical Imaging (ISBI), Prague, Czech Republic, 13–16 April 2016; pp. 1405–1408.
61. Majtner, T.; Yildirim-Yayilgan, S.; Hardeberg, J.Y. Combining Deep Learning and Hand-Crafted Features for Skin Lesion Classification. In Proceedings of the 2016 Sixth International Conference on Image Processing Theory, Tools and Applications (IPTA), Oulu, Finland, 12–15 December 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 1–6.
62. Antipov, G.; Berrani, S.-A.; Ruchaud, N.; Dugelay, J.-L. Learned vs. Hand-Crafted Features for Pedestrian Gender Recognition. In Proceedings of the 23rd ACM international conference on Multimedia—MM '15, Brisbane, Australia, 26–30 October 2015; ACM Press: New York, NY, USA, 2015; pp. 1263–1266.
63. Golbeck, J.; Hendler, J. Inferring binary trust relationships in web-based social networks. *ACM Trans. Internet Technol.* **2006**, *6*, 497–529. [CrossRef]
64. Greenspan, S.; Goldberg, D.; Weimer, D.; Basso, A. Interpersonal Trust and Common Ground in Electronically Mediated Communication. In Proceedings of the 2000 ACM Conference on Computer Supported Cooperative Work, Philadelphia, PA, USA, 2–6 December 2000; ACM: New York, NY, USA; pp. 251–260.
65. De Montjoye, Y.A.; Wang, S.S.; Pentland, A.; Anh, D.T.; Datta, A. On the Trusted Use of Large-Scale Personal Data. *IEEE Data Eng. Bull.* **2012**, *35*, 5–8.
66. Singh, V.K.; Freeman, L.; Lepri, B.; Pentland, A.P. Classifying spending behavior using socio-mobile data. *Hum. J.* **2013**, *2*, 99–111.
67. Gilbert, E.; Karahalios, K. Predicting tie Strength with Social Media. In Proceedings of the 27th International Conference on Human Factors in Computing Systems, Boston, MA, USA, 4–9 April 2009.
68. Nelson, R.E. The strength of strong ties: Social networks and intergroup conflict in organizations. *Acad. Manag. J.* **1989**, *32*, 377–401.
69. Gao, J.; Schoenebeck, G.; Yu, F.-Y. The Volatility of Weak Ties: Co-evolution of Selection and Influence in Social Networks. In Proceedings of the 18th International Conference on Autonomous Agents and MultiAgent Systems, Montreal, QC, Canada, 13–17 May 2019; pp. 619–627.
70. Singh, V.K.; Bozkaya, B.; Pentland, A. Money walks: Implicit mobility behavior and financial well-being. *PLoS ONE* **2015**, *10*, e0136628. [CrossRef]
71. Jonason, P.K.; Jones, A.; Lyons, M. Creatures of the night: Chronotypes and the Dark Triad traits. *Personal. Individ. Differ.* **2013**, *55*, 538–541. [CrossRef]
72. Lyons, M.; Hughes, S. Feeling me, feeling you? Links between the Dark Triad and internal body awareness. *Personal. Individ. Differ.* **2015**, *86*, 308–311. [CrossRef]
73. Adan, A.; Almirall, H. Horne & Östberg morningness-eveningness questionnaire: A reduced scale. *Personal. Individ. Differ.* **1991**, *12*, 241–253.
74. Cai, G.; Lv, R.; Tang, J.; Liu, H. Temporal dynamics in social trust prediction. *Wuhan Univ. J. Nat. Sci.* **2014**, *19*, 369–378. [CrossRef]
75. Lemaitre, G.; Nogueira, F. Imbalanced-learn: A Python Toolbox to Tackle the Curse of Imbalanced Datasets in Machine Learning. *J. Mach. Learn. Res.* **2017**, *18*, 559–563.
76. Batista, G.E.; Bazzan, A.L.; Monard, M.C. Balancing Training Data for Automated Annotation of Keywords: A Case Study. In Proceedings of the Brazilian Workshop on Bioinformatics, Macaé, RJ, Brazil, 3–5 December 2003; pp. 10–18.
77. Chawla, N. SMOTE: Synthetic Minority Over-sampling Technique. *J. Artif. Intell. Res.* **2002**, *16*, 321–357. [CrossRef]
78. Ijaz, M.F.; Attique, M.; Son, Y. Data-Driven Cervical Cancer Prediction Model with Outlier Detection and Over-Sampling Methods. *Sensors* **2020**, *20*, 2809. [CrossRef] [PubMed]
79. Wang, Z.; Wu, C.; Zheng, K.; Niu, X.; Wang, X. SMOTETomek-Based Resampling for Personality Recognition. *IEEE Access* **2019**, *7*, 129678–129689. [CrossRef]
80. Techniques to Deal with Imbalanced Data Kaggle. Available online: <https://www.kaggle.com/npramod/techniques-to-deal-with-imbalanced-data> (accessed on 11 August 2018).
81. Buskens, V.; Raub, W.; Van Der Veer, J. Trust in triads: An experimental study. *Soc. Netw.* **2010**, *32*, 301–312. [CrossRef]
82. Dang-Pham, D.; Pittayachawan, S.; Bruno, V. Applying network analysis to investigate interpersonal influence of information security behaviours in the workplace. *Inf. Manag.* **2017**, *54*, 625–637. [CrossRef]

-
83. Radu, V.; Tong, C.; Bhattacharya, S.; Lane, N.D.; Mascolo, C.; Marina, M.K.; Kawsar, F. Multimodal deep learning for activity and context recognition. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* **2018**, *1*, 157. [\[CrossRef\]](#)
 84. Pedregosa, F. Scikit-learn: Machine learning in python. *J. Mach. Learn. Res.* **2011**, *12*, 2825–2830.
 85. Chollet, F. Others Keras. Available online: <https://keras.io> (accessed on 10 August 2018).
 86. Chawla, N.V. Data mining for imbalanced datasets: An overview. In *Data Mining and Knowledge Discovery Handbook*; Springer: Boston, MA, USA, 2009; pp. 875–886.
 87. Zheng, A. *Evaluating Machine Learning Models a Beginner's Guide to Key Concepts and Pitfalls*; O'Reilly Media, Inc.: Sebastopol, CA, USA, 2015.
 88. Tufekci, Z. Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency. *Colo. Technol. Law J.* **2015**, *13*, 203–218.
 89. Shifali, A.; Yttri, J.; Nilsen, W. Privacy and security in mobile health (mHealth) research. *Alcohol Res. Curr. Rev.* **2014**, *36*, 143–151.
 90. Jin, H.; Su, L.; Ding, B.; Nahrstedt, K.; Borisov, N. Enabling Privacy-Preserving Incentives for Mobile Crowd Sensing Systems. In *Proceedings of the 2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS)*, Nara, Japan, 27–30 June 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 344–353.
 91. Ivanov, A.; Sharman, R.; Rao, H.R. Exploring factors impacting sharing health-tracking records. *Health Policy Technol.* **2015**, *4*, 263–276. [\[CrossRef\]](#)
 92. Möhlmann, M.; Geissinger, A. Trust in the Sharing Economy: Platform-Mediated Peer Trust. In *Cambridge Handbook on the Law of the Sharing*; Cambridge University Press: Cambridge, UK, 2018.