Trust Forge: Harnessing Machine Learning to Build Trust on Social Networks

Kavitha Chitrala[1], Shanthi Makka[2(✉)], and S. Sowjanya[1]

[1] Vardhaman College of Engineering, Kacharam, Shamshabad, Hyderabad 501218, Telangana, India

[2] Computer Science and Engineering, Vardhaman College of Engineering, Kacharam, Shamshabad, Hyderabad 501218, Telangana, India

dr.shanthimakka@gmail.com

Abstract. A social media platform is a form of service offered by an online platform that facilitates easy communication between individuals, as well as the establishment of interpersonal connections and social exchanges. Additionally, it supplies users with a webpage where they may create an open persona and engage adding additional users. Trust is a significant concern in social networking sites, and to address this issue, we have employed the Naive Bayes algorithm to establish trust in online networks. This algorithm is implemented through direct and indirect communication, and trust values are calculated using Dempster-Shafer theory and Bayesian conditional. The effectiveness of our proposed approach is demonstrated through the reenactment results obtained with various parameter arrangements. "In summary, our comparison demonstrates that Multi-faceted trust modeling is statistically and significantly superior to Naive Bayes Model in addressing based on accuracy."

Keywords: Naive Bayes · online social network · trust · Direct trust · Indirect trust

1 Introduction

The term "virtual social Media" fundamentally refers to whatever type of human communication or data sharing that takes place online via a PC, mobile device, or other portable device. There are numerous websites and programs that enable it. Social networks play a significant part in day-to-day living because online interactions are now among the most common forms of communication. Because we live in a time and era where data is readily available [5] at the touch of a button and is all around us, social media platforms have experienced fast growth. However, online networks are not the only crucial component that we should not disregard. Online social networks are a contentious topic right now since the majority of people believe that they just ruin people's lives, while some believe that they are a godsend because they bring individuals from throughout the globe.

X. Cheng (Ed): BROADNETS 2024, LNICST 602, pp. 135–143, 2025.
https://doi.org/10.1007/978-3-031-81171-5_14

1.1 Trust

Trust is a fundamental concept that has a significant impact on numerous aspects of society, relationships, & human life. It refers to the reliance or confidence one places in the integrity, ability, or character of a person, group, organization, or system. Trust is built on the belief that the trusted entity will act in a certain way or fulfill certain expectations, and it forms the basis for cooperation, collaboration, and healthy social interactions.

Here are some key aspects and implications of trust:

Foundation of Relationships: Trust is essential for building and maintaining healthy relationships, whether they are personal, professional, or societal. It is the emotional and psychological glue that binds people together.

Trust-Building: Trust can be built through transparency, honesty, competence, consistency, and a track record of keeping promises. In simple way we can say that, trust is a foundational element of human relationships [6] and societal structures. It influences our interactions with others, shapes our choices, and is essential for the functioning of various institutions and systems. Building and maintaining trust is an ongoing process that relies on honesty, integrity, and consistent behavior.

1.2 Different Forms of Online Social Network Trust

Even while OSNS links a single person to the entire world, it has the potential [7] to falsify information and data. In that specific circumstance, trust significantly helps to simplify the matter. Micro and macro level trust can be broadly classified into two sorts in OSNS.

2 Literature Survey

According to the author [1], social interactions have a significant impact on each person's ability to interact with others and even exchange thoughts with them. Trust is a key factor in this activity. This essay examines a different trust paradigm for a social media platform online. Accordingly to the model incorporates the importance of reputation and social network relationships for each individual person. In addition, the author makes use Utilizing the Matrix Factorization model (MF) to assess the relationship between two customers. The Gaussian Kernel Density Estimation (GKDE) design is used to predict that a person's reputation will depend on their other relationships with clients. The reputation is evaluated based on the followers, and positive reputation is added, and both A new trust model that is used to evaluate the trust connection is created from the reputation and interaction model when paired with valid weights (Table 1).

Table 1. Literature Survey

Reference No.	Title	Author	Findings
[2]	The effect of social media marketing on brand trust, brand equity and brand loyalty	*Haudi Haudi, Wiwik Handayani*	The goal of this research is to determine the effects of social media marketing initiatives on brand equity, brand trust, and brand loyalty. Using a simple random selection technique, 450 respondents who had been using social media for at least six months were chosen for the study's sample. The Structural Equation Modeling (SEM) method was applied using SPSS 3.3.3 software
[3]	Cynicism as strength: Privacy cynicism, satisfaction and trust among social media users	*Md Irfanuzzaman Khan*	Theory (ECM), we polled 475 social media users to see if privacy cynicism has a negative impact on social media satisfaction and trust
[4]	Trust in social media brands and perceived media values: A survey study in China	*Mingmin Zhang*	Social status value has a direct impact on social media brand trust, whereas information value and organizational communication value have an indirect impact through their respective contributions to social networking, entertainment, and/or social status values. We provide a critical explanation for social media trust in our work and create a scale of perceived media values (PMV) that other studies can utilize

3 Methodology

This section starts with a system overview before moving on to the Gaussian NB model, Naïve-Bayes Model, and cross-validations, which are all provided in turn (Fig. 1).

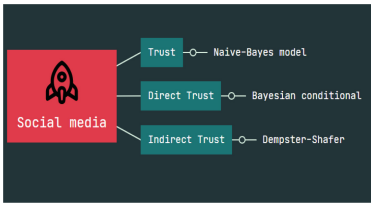

Fig. 1. Model Design

3.1 System Explanation

In recent years, online social networking is expanding quickly, [9] and many activities are being employed to spread information. With OSNS's assistance, the user can also arrange, locate, and share their ideas and experiences online. Additionally, [10] because of their candor anddecentralization, OSNS may be accessible to malicious users. Thus, there are many trust-related problems that potential customers must deal with. The user benefits from effective and efficient trust assessment (evaluation) in this way.

3.2 Naive-Bayes model

This model is a classifier that uses a machine learning (ML) model to categorize [11] different items (objects) based on particular characteristics. The Naive-Bayes model is simple to construct and frequently utilized with big datasets. In addition, the algorithm is both straightforward and powerful. This algorithm primarily relies on two components.

1. Naive
2. Bayes

The assumption made by naive Bayes classifiers is that each element in a class is unrelated to each other. Even though a property of one class is dependent on another, Nave Bayes primarily uses probability theory and independently contributes to all of the attributes. Now let's look at the Bayes theorem. A theory in probability and statistics known as the Bayes theorem measures the chance of an event happening given the chance of an event that has already happened.

Cross-validation: It is a technique used to gauge how well the results of statistical study extrapolate to other data sets. It is used to calculate the precise accuracy of a predictive model's performance estimate. The fundamental benefit of cross-validation is the ability to distinguish between training and test data. The other name for Cross-approval is an evaluation of revolution.

3.3 Gaussian NB Model

This particular NB approach is utilized most often when the data set comprises continuous values. Gaussian NB model. Additionally, [12] it is anticipated that each individual feature will follow the Gaussian distribution, which is the normal distribution. After preprocessing is completed, the Gaussian model is applied. The NB model is then constructed using sk-learns. Using the training set of data, the Gaussian NB model classifier is trained. Fit() can be used even for training. Once the classifier is built, the test set may be found using the predict() method, and the model is capable of making predictions.

3.4 OSN (Direct Trust) Bayesian Conditional Trust Calculation

By altering or rejecting the actual data or information, the affiliated perceptive mobile user can evaluate the discovered mobile user's devious behaviors in addition [13] to listening to the data or information that the discovered mobile user forwards during direct observation. The Bayesian inference is one of the statistical methods of the Bayes theorem that is utilized to update the probability hypothesis. Using the Bayesian inference approach, we built a model using continuous random variables that characterize as φ(phi) and take values between 0 and 1. In this case, the beta distribution is followed by the φ, meaning that φ ∼ Beta(h,d) with respect to h and d.

$$Beta(h, d) = \frac{\varphi^{h-1}((1-\varphi)^{1-d}}{\int_0^1 \varphi^{h-1}((1-\varphi)^{1-d} b\Omega} \tag{1}$$

The values of trust are assumed in this section with two caveats. Namely, h & d, & $0 \leq \varphi \leq 1$, Φ is beta distribution.

As more perceptions become available, we reduce our confidence in the trust by disseminating its likelihood iteratively using a probability distribution. Expect that by the (t1)th perception, the prior probability PDF (density function) will have been established. The PDF can then be used to determine the back circulation at the t th perception in accordance with the Bayes hypothesis.

$$f_x(\varphi) = \frac{f_x(a_x|\varphi, b_x) f_{x-1}(\varphi)}{\int_0^1 f_x(a_x|\varphi, b_x) f_{x-1}(\varphi)} d(\varphi) \tag{2}$$

The data packets that must be successfully sent are represented by a_x and b_x in this situation, and the observed mobile user at the time of observation accepts these packets at x th observation. Also $f_x(a_x|\varphi, b_x)$ determine as binomial distribution

$$f_x(a_x|\varphi, b_x) = \left(\frac{b_x}{a_x}\right) \varphi^{at} (1-\varphi)^{bt-at} \tag{3}$$

In addition the conjugate prior likelihood distribution (prior probability distribution), or beta distribution, for the binomial distribution in Bayesian deduction (inference). The prior appropriation $f_x(a_x|\varphi, b_x)$ is unquestionably recognized to seek a beta distribution, reflecting what is currently believed about the delivery of at the $f_x - 1(\varphi)$ perception, because the probability function $f_x(a_x|\varphi, b_x)$ chases a binomial dispersion. The beta

circulation is pursued by the back dispersion $f_x - 1(\varphi)$ same manner as the previous appropriation $f_x - 1(\varphi)$ does. In particular, if $f_x - 1(\varphi) \sim \text{Beta}\, f_x(a_x - 1|b_x - 1)$ and a_x, b_x from the xth perception are also provided, then that is the case.

$$f_x(\varphi) \sim Beta(c_{x-1} + a_x, d_{x-1} + b_x - a_x), x \geq 1 \tag{4}$$

Due to ignorance, the distribution of φ was first presented as having a consistent distribution, thus that f0(φ) ∼ Beta(1,1). Similar to how f_x (φ) follows Beta(a_x, b_x) with (specification) parameters.

$$c_x = c_{x-1} + a_x, d_x = d_{x-1} + b_x \tag{5}$$

$$c_{0=1} \qquad d_{0=1}$$

As a consequence, trust values can be stated statistically as a beta distribution anticipation

$$\text{That is } Q_x[\varphi] = \frac{c_x}{c_x + d_x} \tag{6}$$

The trustworthiness of mobile users is currently 0.5; however, as more data becomes available, the figure will change. As a result of its ability to provide more accurate weights on mischievous actions in Bayesian models, As a punishment element used for fading reputation, a new factor has been stated. Here, trust is measured using the following formula:

$$Q_x[\varphi] = \frac{c_x}{c_x + d_x} \tag{7}$$

The assessment of trust is made more accurate and realistic with the help of the penalty element. It determines behavior in two ways. The first is by checking records to see if the user of mobile content has engaged [14] in any malicious behavior. If they haven't, the trust value will decline. Second, because of the aspect of punishment, there is not a restriction that the conduct does not immediately restore the trust value. As a result of the explanation above, we may determine that TrD is the direct observation, and TrD = $Q_x[\varphi]$.

3.5 DST Function

The mass function, probability function, and belief function [15] serve as the foundation for the DST function. Upcoming use Then

The likelihood function Let Y = {y1,y2,y3} represent the configuration of completely unconnected conclusions and evidence under certain considerations. The configuration of every subset of E (power set (E)), that is, {{∅,{y1},{y2},{y3},{y2,y3},{y1,y2},{y1,y3},{y1,y2,y3}}, is the discernment frame of X. Every element in the range [0,1] is mapped by the mass/probability function (m) from the discernment frame. P(X) → [0 1] is m. It satisfies the requirements that m(∅) = 0 and that the sum of the individual items in the discernment frame equals 1.

$$\sum b \in_p (\text{Y})\text{m(b)} = 1 \tag{8}$$

Belief Function: The total of the mass elements of all the sets in the power set that are subsets of S, for any set S in the power set, is the belief function.

$$\mathrm{Bel}(A) = \Sigma\{m(B)|B \subseteq A\} \tag{9}$$

possibility function: The possibility function (pl(S)) for every set S in the power set is defined as the total of the mass elements of all the sets in the power set that intersect with X.

$$\begin{aligned} \mathrm{pl}(S) &= \sum m(d \cap X \neq \emptyset m(D)) \quad \text{where} \\ \mathrm{pl}(S) &= 1 - \mathrm{bel}(S) \end{aligned} \tag{10}$$

The Dempster's rule must be adhered to when combining:

If we take 1,2 as two observer clients, their confirmations on a comparable edge of decrement are m1(B), m2(C). We then use condition to find the mix of these two confirmations (m1, m2).

$$m12(A) = \Sigma\{B \cap C = A\}[m1(B) * m2(C)]/[1 - K] \tag{11}$$

where K represents constant, which is described as

$$K = \Sigma\{B \cap C = \emptyset\}[m1(B) * m2(C)] \tag{12}$$

3.5.1 Results and Analysis

In this experiment, we apply machine learning methods to compare trust. After developing the model, we examine social network samples of direct and indirect trust and assess how accurate the model is in comparison to alternative methods. The information in the Instagram data set is mainly about posts, and the training data is made up of 678775 user history logs. Each log type is {Impressions; Comments; Likes; Hashtags; Caption; Follows;}. Splitting the data set in half, so that the training set is 80% and the testing set is 20%. Testing set will conclude the experiment.

The precision after scrutiny is 0.96% (Figs. 2 and 3).

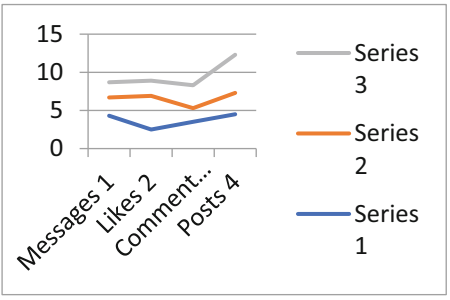

Fig. 2. Direct communication through social media Platform

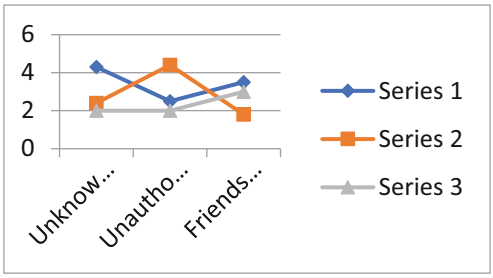

Fig. 3. Indirect Communication

4 Conclusion

In every person's life, an important paradigm is the online social network. Since data interchange is essential to real, practical life, it must also be dependable and safe. Because we used a machine learning platform and the Navie Bayes algorithm, which enables us to quantify trust using both direct and indirect approaches as well as Bayesian inference and Dempster-Shafer theory, the results are more dependable and accurate.

References

1. Yuji, W.: He rust Value Calculating for Social Network Based on Machine Learning: Conference on Intelligent Human-Machine Systems and Cybernetics USA (2017)
2. Haudi, H., Handayani, W.: The effect of social media marketing on brand trust, brand equity and brand loyalty. International Journal of Data and Network Science
3. Khan, M.I.: Cynicism as strength: Privacy cynicism, satisfaction and trust among social media users (2022)
4. Zhang, M.: Trust in social media brands and perceived media values: A survey study in China. Department of Journalism and Communication, South China Normal University, China (2022)
5. Zhao, K., Pan, L.: A machine learning based rust evaluation framework for online social networks. IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications (2014)
6. Meo, P.. Ferrara, E.: Rust and Compactness in Social Network Groups. IEEE ANSAC IONS ON CYBE NE ICS (2015)
7. Makka, S., et al.: Application of blockchain and internet of things (IoT) for ensuring privacy and security of health records and medical services. 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), pp. 84–88. Uttar Pradesh, India (2022). https://doi.org/10.1109/IC3I56241.2022.10072427
8. Uany, Y.: A survey of rust management systems for online social communities –trust modelling, rust Inference and Attacks. Department of computer & information science, In USA (2016)
9. Makka, S., Arora, G., Mopuru, B.: IoT based health monitoring and record management using distributed ledger. In: Journal of Physics: Conference Series. Vol. 2089, No. 1, p. 012030. IOP Publishing (2021)
10. Islam Habis Mohammad Hatamleh: Trust in Social Media: Enhancing Social Relationships (2023)

11. Karlsena, R.: Social Media and Trust in News: An Experimental Study of the Effect of Facebook on News Story Credibility. Digital Journalism (2021)
12. Kim, D.Y., Kim, H.Y.: Trust me, trust me not: A nuanced view of influencer marketing on social media. Journal of Business Research, Elsevier (2021)
13. Parmentier, A.: Personalized multifaceted trust modeling to determine trust MANETs. International Conference on Advanced Computing and Communications ADCOM, (IITM PhD forum), pp. 55–60.1 (2015)
14. Shen, J.: Hierarchical Trust Level Evaluation for Pervasive Social Networking, in 2017
15. Uany, Y.: A Survey of rust Management Systems for Online Social Communities –Trust Modelling, rust Inference and Attacks. In USA (2016)