Incorporating Machine Learning Algorithm with Fuzzy Logic for the Trust Model in Online Social Networking

P. Maragathavalli[1], V. Dhivakaran[2], S. Ravindran[3], Sharun Ratheesh[4] and E. Madeleine[5]

[1-5]Department of Information Technology, Pondicherry Engineering College, Puducherry, India.

Abstract - *Social networks have become the major infrastructure of today's daily activities of people. Users can able to interact with each other in these networks and share their interest on resources and give their opinions about these resources or spread their information. Since each user has a limited knowledge of other users and most of them are anonymous. Trustworthiness plays a main role on identifying a suitable product or specific user. The inference mechanism of trustworthiness in social networks refers to utilizing available information of a specific user who intends to contact an unknown user. This mostly happens when purchasing a product, deciding to have friendship or other applications which require predicting the reliability of the second party.*

In this paper, first the raw data of the real world dataset, Epinions is examined and the feature vector is calculated for each pair of social network users. Next, fuzzy logic is incorporated to rank the membership of trust to a specific class. Finally, to classify the trust values, machine learning technique, Convolutional Neural Networks (CNNs) is used instead of traditional weighted sum methods, to express the trust between any two users in the presence of a special pattern. The results show that the accuracy of the proposed method is better than the existing work, and unlike other methods, does not decrease by increasing the number of samples.

Keywords: *Trust Inference, Social Networks, Reliability Prediction, Fuzzy Logic, Special Pattern.*

1. INTRODUCTION

In recent days, millions of users around the world are connected by means of Online social networks(OSNs), such as Facebook, Twitter, and Weibo. In fact, the number of users in these networks is increasingly growing despite some of them may have decrease in the number of active users, as shown in Fig. 1.1. On the other hand, users exchange huge amounts of information in social networks every day; based on the level of trust factor is one of the most important issues. For example, when choosing a book to read, we may choose a book that we know its writer, or a book that is suggested by someone who we trust in. Similar cases happen in social networks especially when the interaction with unknown users, who are not endorsed by other users, increases the risks. Hence, users in social networks share information with other users according to their trust in them. Due to the dimensions of social networks, the number of users that are unknown to a specific user is very high and studying and evaluating trust between users in social networks is an important challenge.

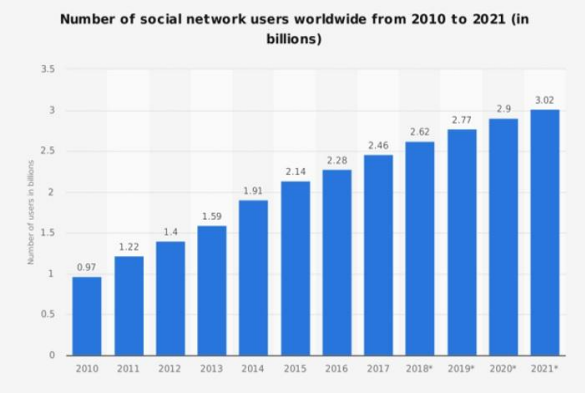

Fig. 1.1 Number of social network users worldwide from 2010 to 2021 (in billions)

1.1 CHARACTERISTICS OF TRUST

From the psychological and sociological perspectives, trust refers to the subjective expectation about the behavior of another person in future. Without trust, life would rapidly become chaotic. Trust measures the confidence in entities behaving in an expected manner.

Numerous activities related to e-commerce are carried out in social networks, in which trust plays an important role in decision making of customers. Suggestion by a friend is a common service that has been provided by almost all of the social networks, and evaluation of trust between users improves the quality of suggestions. Another important point is that the huge amount of sensitive contents on Web makes the security of personal information of users a necessity. Using the trust based on access control, the privacy of users could be protected. All of these points imply the importance of trust evaluation.

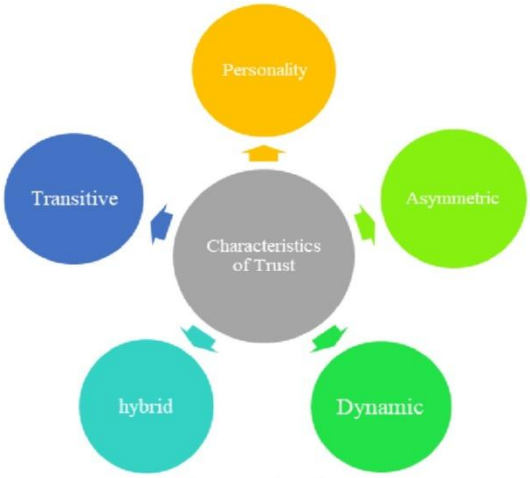

Fig. 1.2 Characteristics of Trust

Based on the environment, trust could have different attributes. However, in most cases, especially in distributed environments, and in social networks, it follows certain properties that are illustrated in Fig. 1.2.

1.2 CATEGORIZATION OF TRUST

Generally, previous works in trust could be categorized on three criteria (Fig. 1.3):

(i) Trust information collection;

(ii) Trust value evaluation;

(iii) Trust value dissemination.

Each of them could have their subcategories. Trust information collection has three subcategories: attitudes, behaviors, and experiences. Trust value assessment could be classified based on their data models into graph, user interaction and hybrid methods. Trust value dissemination could be divided into trust-based recommendation and visualization models.

Since in Fig. 1.3, the second category, trust value assessment, is the most important category in the trust inference methods, it will be described in more detail. To model the trust, numerous techniques have been employed, namely statistical and machine learning techniques, techniques based on heuristics, and techniques based on behavior.

The statistical and machine learning methods focus on presenting a mathematical model for trust. Heuristic methods try to build a practical model to implement trust systems. The behavior-based models focus on behaviors of users in the society.

The machine learning solutions, such as artificial neural networks, and hidden Markov model have also been used to calculate and predict trust. By analyzing the patterns of the input data, and building a model, machine learning methods are very flexible in evaluating the test data. Furthermore, different classifiers are proper solutions to classify the trust in social networks.

However, in some of the previous work to calculate trust for each feature present in the feature vector, a weight is chosen and then using a formula, the approximate value for trust is obtained. The weight of each factor reflects its importance, and getting proper values for the weights of factors to have the best result is a very daunting task.

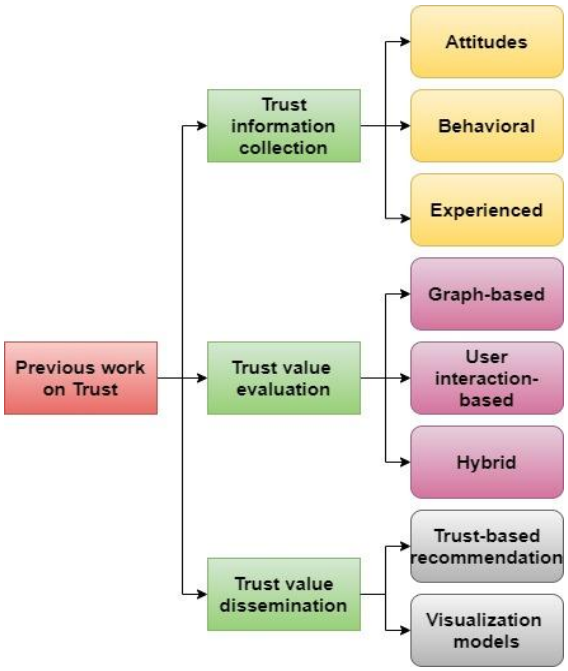

Fig. 1.3 Categorization of previous works in the trust field

On the other hand, different datasets have been used for trust evaluation of users in social networks, and each has its own advantages and disadvantages. A table comparing the most used datasets in trust evaluation studies is provided later in this paper. However, choosing the proper dataset such that its generality enables us a comparison with other methods, is a challenging problem. In addition, features provided by each dataset are different from other ones, which cause different approaches for evaluation of the final trust. Therefore, datasets without complexities and having basic primitive features are better choices for the trust evaluation problem. A final note about the dataset remains with its reality, where datasets from real social network sites are more interesting. In this paper, a real social network is used which contains all the mentioned characteristics.

2. LITERATURE SURVEY

RELATED WORKS

In [4], machine learning methods have been used. The authors realized the trust evaluation as a classification problem, and present an approach based on machine learning. One of the disadvantages of this paper is that by increasing the number of instances, the accuracy decreases, and this is a challenge for complex and big networks. Hence in this paper, we attempt to solve the problem of decreasing accuracy when the number of instances increases.

In [5], evaluated trust according to the behavioral connection of users of social networks. They defined behavioral trust based on conversation trust and propagation trust. Conversation trust refers to the period of time that two users have connections with each other; the longer and the more a connection, the more the trust between these users. To compute propagation trust between two users, the volume of information exchanged between them is a main measure and implicitly for the user who propagates the information.

In [6], presented the STrust model for social trust calculation according to interactions inside the social network. Their model consists of two types of trust: popularity of trust, which refers to the level of acceptability and admissibility of a user in the network (how much this user is reliable from the view of other users) and interaction of trust, which refers to the level of contribution of a user in the network. In general, a framework for constructing trust communities based on model which relies on social assets is presented.

In [7], proposed a social model for trust in opportunistic networks, which excite users to contribute in social interactions via applications such as content distribution and microblogs. The authors used two definitions for evaluation of trust: implicit and explicit social trust. The explicit trust is based on conscious relations. When two users are in interaction with each other, their friends' lists are exchanged with one another and saved in friendship graphs. The trust is calculated according to the friendship graph and assigned to the direct link of the friend which has the most value of trust. Implicit trust between two users is defined according to the value and duration of the relation between them, which is calculated based on two parameters: familiarity and similarity of nodes. In this model, the explicit trust is computed according to the structural features of the network, while implicit trust is computed based on interactions of the network graph. The disadvantage of this method is that it only considers the value and duration of the relations while the spirit and nature of the relation is also important. Since, if two users have a considerable amount of relation with each other but their relation is negative, it does not mean necessarily that they trust each other.

In [8], Calculated trust based on three aspects: similarity of profiles, reliability of information and social comments. The advantage of their method which stays inside the hybrid categories is that various aspects of trust is considered. On the other hand, the final value of trust is computed according to a weighted linear sum of all factors, such that the weight of each factor reflects its importance. Reaching good values for weights which results in better final values is a hard task. Despite the accomplished values can be a reference for the trust values, they may not match with users' expectations and hard for them to believe, since trust is a heuristic and mental concept.

In [9], defined trust and celebrity in social networks according to web-based environments. The authors defined direct, indirect and world-wide trust, and applied some important factors such as distance of trust path and acceptability of service, which have not been considered in previous work.

In [10], Calculated the trust value with a weighted sum of features present in the feature vector. Then using a formula, the approximate value for trust is obtained. The weight of each factor reflects its importance, and getting proper values for the weights of factors to have the best result is a very daunting task.

In [11], a novel and complex method is proposed to obtain the trust chain based on the 1-hop trust (the trust between users that are directly in contact). The authors have used Facebook and INFOCOM datasets, and have also presented a mathematical analysis to prove their method.

2.1 SUPPORT VECTOR MACHINE

The support vector machine (SVM) method is one of the supervised learning methods with is used for classification and regression. This method has been shown to have a better performance than older methods, such as perceptron neural networks. The goal of these methods is to find and distinguish complicated patterns in data (using clustering, classification, ranking, data cleaning, etc.)

2.2 DECISION TREE

Decision tree (DT) is a method for approximating the objective functions with discrete values. This method can handle noises well, and can learn disjunctive combination of conjunctive statements. The decision tree is a tree in which the instances are classified in such a manner that

the tree is grown from downwards the root, and finally ends in leaves.

Also, the instances are ordered based on their feature values. Each node in the decision tree represents a feature in instances that are to be classified, and each branch represents the value that the node can have. Instances are classified starting from the root, and their ordering is based on their feature values. The feature that can classify the training data better than the others is considered as the root. Then, a similar process is repeated on each section of training data. Hence, the decision tree analyzes the input data to find the best features for a split in nodes. In each node, features are analyzed and the feature that minimizes the entropy is selected.

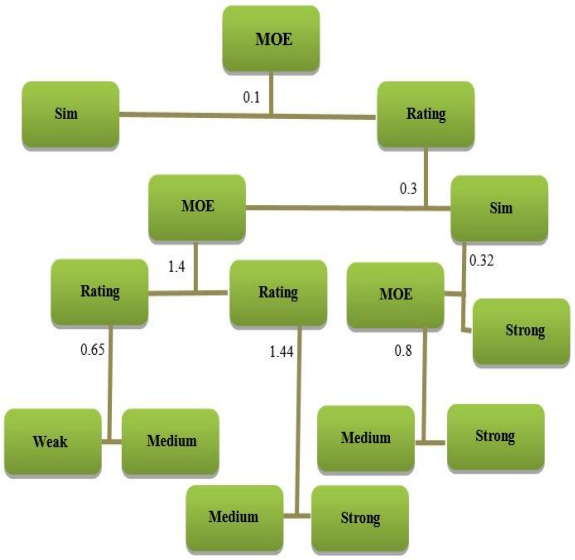

Fig. 2.1 Decision Tree (DT)

2.3 k-NEAREST NEIGHBORS

The k-Nearest Neighbors method (k-NN) is a supervised classifier, like Naive Bayes. The accuracy of this algorithm is highly dependent to the value of k. If k is set too high, irrelevant data will be taken into account and thus, the accuracy will decrease. If k is set too low, such as k=1, the one neighbor that will be considered may be noise, and hence, the test data may be labeled incorrectly. In other words, if k is low, the information will be local, and if k is high, the information will be global.

In k-NN, to predict the label of a new instance, its Euclidean distance to all of the instances should be calculated. Then, we take the k nearest neighbors and predict its label based on them. Algorithms like k-NN are called instance-based or lazy learners, because: 1) There are no models in these methods to apply to our data. The data should be always available to classify new instances. Hence, it is called instance based. 2) There is no training and testing in this algorithm and the classification is accomplished in one phase. Thus, it is called lazy.

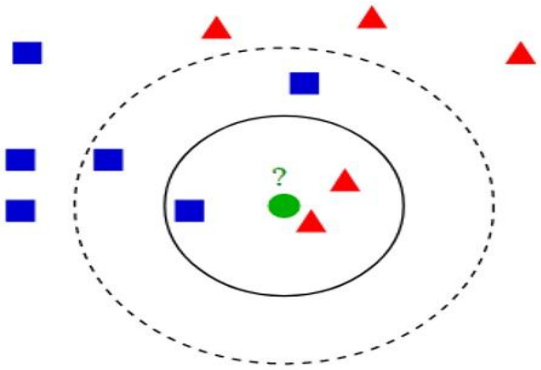

Fig. 2.2 k-Nearest Neighbor (k-NN)

2.4 DATASET PREPROCESSING

A number of well-known datasets related to the trust factor in social networks are available for researchers, some of which are presented in Section 4 and investigated in this research. Epinions dataset that we have used in our paper has the highest number of opinions (reviews) and therefore is one of the richest dataset in this sense. This dataset is easy to download and available, and its simple and partial structure has made it more understandable compared to other ones.

The reason for choosing Epinions dataset is that the features taken from this dataset are general and hybrid ones which could also be calculated for other datasets as well. In fact, choosing the dataset with hybrid properties, such that the feature vector could be calculated for it is of great importance. The final factors in choosing a dataset is having the “trust” label that we need in training and testing phases using machine learning methods.

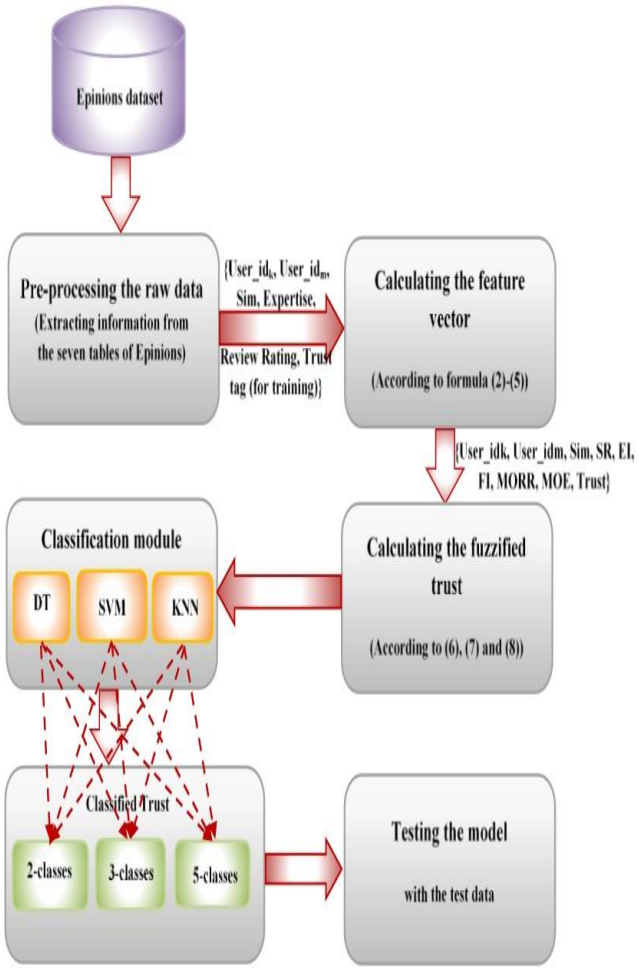

Fig. 2.3 State diagram of existing work

2.5 FEATURE VECTOR

To calculate each feature, the data are not incorporated directly from the dataset, but are useful for trust evaluation is combined with other data, leading to the feature vector. Furthermore, only those information that are useful for trust evaluation are incorporated. This results in using less and more efficient data, as the dataset may have various data.

Expertise Intersection: Each user can have expertise in some fields. For calculating this feature, the number of fields that both users have expertise in, is divided to the number of all of the available fields.

Mean of Review Ratings (MORR): The mean of review ratings values that are stored for U2.

Mean of Expertises (MOE): This feature is the mean value of the expertises of U2. Numbers are assigned based on expertises, in such a way that when the user has a higher expertise in a field, he/she gets a higher number. If the user has higher number of expertises, the value of this feature becomes larger.

Trust: This shows the real value of trust of U1 to U2, which is a normal value, and the real trust of U1 to U2. For the test instances, this feature shows the value evaluation, and is the label. In the test instances, this value is set to 0. In the next phase, the label value in the feature vector, i.e. the trust evaluation is mapped into a fuzzy value.

Sl. No	Title of the Paper	Name of the Journal, Year	Technique / method / algorithm	Data set used	Parameters used	Strengths	Limitations
1	Trust classification in Social Networks Using Combined Machine Learning Algorithms and Fuzzy Logic	Iranian Journal of Electrical and Electronic Engineering, 2019	Machine learning algorithm and fuzzy logic	Epinions	Accuracy	Multilevel classification	Feature vector Dependency

2	A Multidimensional Trust Evaluation Framework for Online Social Networks Based on Machine Learning	IEEE Translations and content mining, IEEE Access, 2019	Trust evaluation using machine learning techniques	Twitter	Accuracy	Better precision	Less scalable
3	Social network analysis and mining using machine learning techniques	Computer Networks, Elseiver, 2019	Data mining and machine learning Algorithms	Twitter messages with emotions	Trust value	Sentiment analysis with minimal support	Data loss
4	Predict Pairwise Trust Based on Machine Learning in Online Social Networks	IEEE Translations and content mining, IEEE Access, 2018	Machine learning	Ciao	Privacy, Efficiency	Trust prediction is effective	Vulnerable to attacks
5	A Trust-Based Privacy-Preserving Friend Recommendation Scheme for Online Social Networks	IEEE Transactions on Dependable and Secure Computing, 2018	Defining the trust chain based on 1-hop trust	Facebook	Security level	Two datasets, having a security level	More Computational Complexity

Table 2.1 Comparative Study on various Existing Methods of Online Social Networking

3. PROPOSED SYSTEM

3.1 EXISTING WORK

In existing system, extracts the feature vector from a dataset of raw information after pre- processing. This feature vector is fed into a classifier, and the extra information has been removed from it. For a better granularity, the trust value in feature vectors are converted into fuzzy values using membership functions. The trust value is converted in three phases into fuzzy values.

- Using a dataset with basic and limited information, because evaluating trust with datasets with comprehensive information is much simpler and yields better results, but datasets such as the one used in this paper are more challenging; however, the processing speed of these methods are very high.
- Extraction of new feature based on the dataset by processing the basic features; in fact, the proposed features in this paper are not present in the previous works to the best of our knowledge.
- Using machine learning methods for evaluating trust instead of using weighted sums, to obtain a model that can decide whether there is trust or not, based on the feature vector; in this research, three methods are used for obtaining reliability, namely support vector machine, decision tree, and k-nearest neighbors.

3.2 LIMITATIONS OF EXISTING WORK

- Less Accuracy
- Dependence of the feature vector to the dataset
- Low Trust value
- Difficulty in obtaining the best value for each factor

3.3 PROPOSED WORK

In this proposal, new technique which is integrating machine learning algorithm and fuzzy logic is used to calculate and predict trust based upon domain of the ratings and reviews which is not present in the existing method. Convolutional Neural Networks used to classify the trust. Using hybrid methods (graph structure of the network and interactions of the users) for a better performance. Fuzzy logic is used for a better assignment of trust into fuzzy values; since trust is not necessarily binary, and in real world, there are various degrees of trust between users.

Furthermore, different classifiers are proper solutions to classify the trust in social networks.

Processing steps involved,

- Preprocessing the raw data of the dataset
- Calculating the features for the feature vector and for each pair of users
- Calculating the fuzzy trust values
- Training and classification using CNNs
- Evaluation of the proposed system by the test samples

3.4 TRUST VALUE

To calculate each feature, the data are not incorporated directly from the dataset, but are useful for trust evaluations are combined with other data, leading to the feature vector. Furthermore, only those information that are useful for trust evaluation are incorporated. This results in using less and more efficient data, as the dataset may have various data.

It is desirable that by preprocessing these features, the feature vector could be obtained and then, using the feature vector, the trust value of U1 to U2 could be calculated.

$$Tr\ (U_1,U_2) = \alpha.V^T\ (U_1,U_2)$$

Where,

- U_1,U_2 – Users
- α - weight for the feature vector

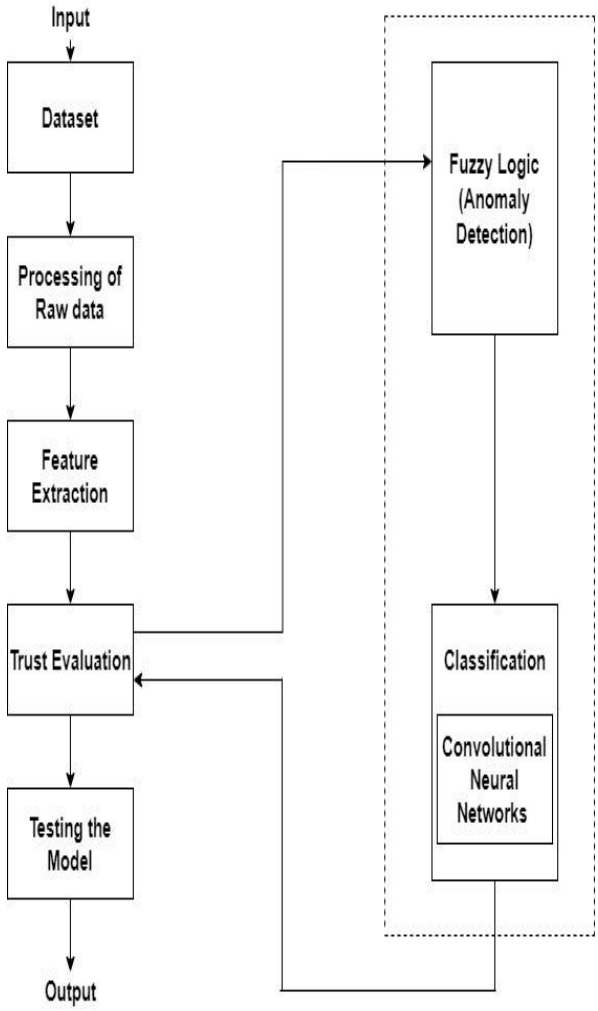

Fig. 3.1 Design of Proposed System

4. MODULE DESCRIPTION

Our project consists of three modules.

They are:

1. Data Collection and Processing Module
2. Trust Evaluation Module
3. Classification Module

4.1 DATA COLLECTION AND PROCESSING MODULE

➢ Preprocessing is a necessary procedure to improve the quality of raw data, which includes the normalization of the main signal detection, the extraction of the informative area, and the correction of imperfections such as filling holes, noise removal etc. With the appropriate signal preprocessing procedure, the

undesired information is eliminated from the raw information and has few effects on the quality of the feature extraction, leading to an improvement in the identification accuracy rate.

➢ In this module, from the dataset we are extracting total positive and negative reviews and ratings by doing preprocessing the raw data which are useful for the trust value evaluation.

➢ The feature extraction minimizes the size of data by extracting the features of the preprocessed information that are useful for classification. For the better results reviews and ratings are comparing with the price of the product.

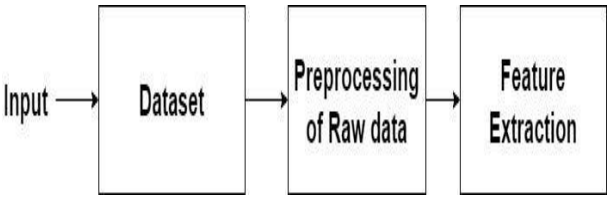

Fig. 4.1 Data Collection and Processing Module Diagram

4.2 TRUST EVALUATION MODULE

➢ The data are not incorporated directly from the dataset, but are useful for trust evaluations are combined with other data, leading to the feature vector. Furthermore, only those information that are useful for trust evaluation are incorporated. This results in using less and more efficient data, as the dataset may have various data.

➢ In this module, trust evaluation takes place using fuzzy logic.

➢ Using this method it shows that unique positive and negative reviews and rating which are useful for the classification process and also shows that the reviews by description.

Fig. 4.2 Trust Evaluation Module Diagram

4.3 CLASSIFICATION MODULE

➢ Classification is unsupervised learning, where no label or target value is given for the data.

➢ This method of gathering items or (documents) based on some similar characteristics among them.

➢ It performs categorization of data items exclusively based on similarity among them.

➢ In this module, it shows the trust value (Polarity consistency value) classification using Convolutional Neural Networks (CNNs).

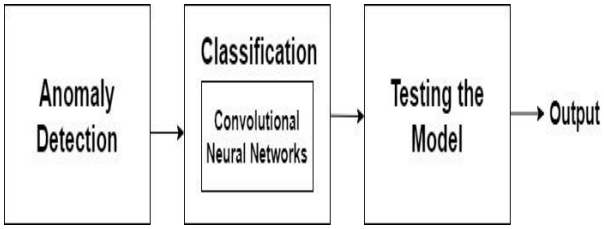

Fig. 4.3 Classification Module Diagram

4.4 PERFORMANCE PARAMETERS

1. ACCURACY

Accuracy is what we usually mean, when we use the term accuracy. It is the ratio of number of correct predictions to the total number of input samples.

The formula for calculating Accuracy A is,

$$A = \frac{TP + TN}{TP + TN + FP + FN}$$

Where,

- TP = True Positive
- TN = True Negative
- FP = False Positive
- FN = False Negative

2. TRUST VALUE

Trust is viewed as a structurally embedded asset or property of relationships, Networks that helps to shape interaction patters with Online Social Networking.

$$Tr\ (U_1,U_2) = \alpha.V^T\ (U_1,U_2)$$

Where,

- U_1,U_2 - Users
- α - weight for the feature vector

5. RESULTS

These datasets have different features, for example the number of users, the number of opinions or reviews. Accordingly, the Epinions dataset that we have used in our paper has the highest number of opinions (reviews) and therefore is one of the richest dataset in this sense. This dataset is easy to download and available, and its simple and partial structure has made it more understandable compared to other ones.

The Epinions dataset contains seven tables (Table 5.1) and each table includes a number of properties. The raw data in the dataset need to be preprocessed in order to get usable.

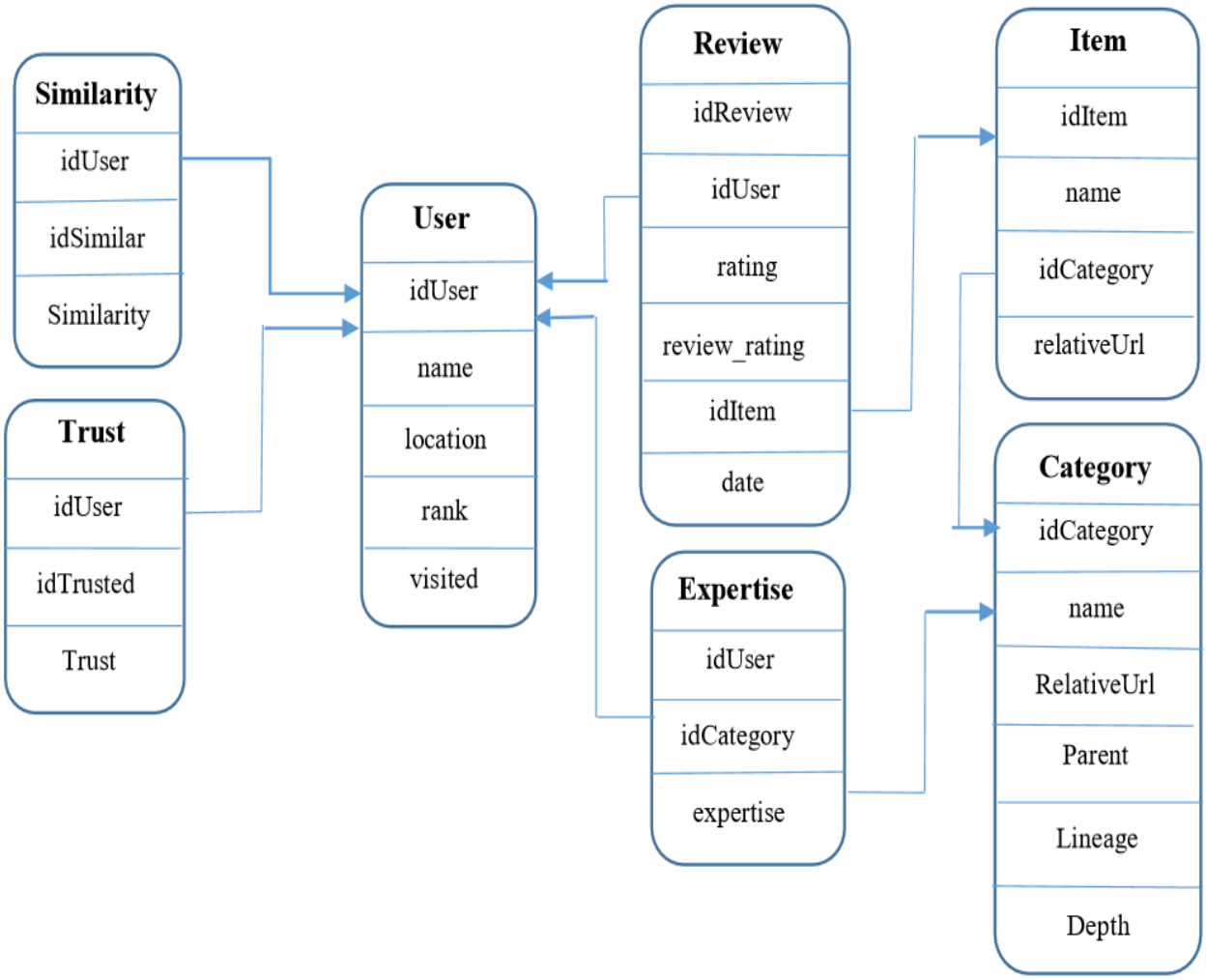

Table 5.1 Epinions dataset and their relationships

The Expertise table shows that each user has expertise in which fields. The Item and Category tables contain information about the products.

The last table, the Trust table, is the definitive one because it contains the labels of the training data. In this table it is shown that in reality, each user in this social network trust which users, and does not trust which users. In fact, the trust means the subjective expectation of a person from the future behavior of a person and the trust of user U1 to user U2 is shown as Tr(U1, U2).

In the Epinions website, users could review various products, could sign up for free and write subjective reviews about products such as software, music albums, TV shows, hardware, and office supplies.

Another reason for choosing Epinions dataset is that the features taken from this dataset are general and hybrid ones which could also be calculated for other datasets as well. In fact, choosing the dataset with hybrid properties, such that the feature vector could be calculated for it is of great importance. The final factors in choosing a dataset is having the "trust" label that we need in training and testing phases using machine learning methods.

5.1 Data Collection and Processing Module

In the below figure, from the dataset we are extracting total positive and negative reviews and ratings by doing preprocessing the raw data which are useful for the trust value evaluation. The feature extraction minimizes the size of data by extracting the features of the preprocessed information that are useful for classification. For the better results reviews and ratings are comparing with the price of the product.

Fig. 5.1 Snapshot of Data Collection and Processing

5.2 Trust Evaluation Module

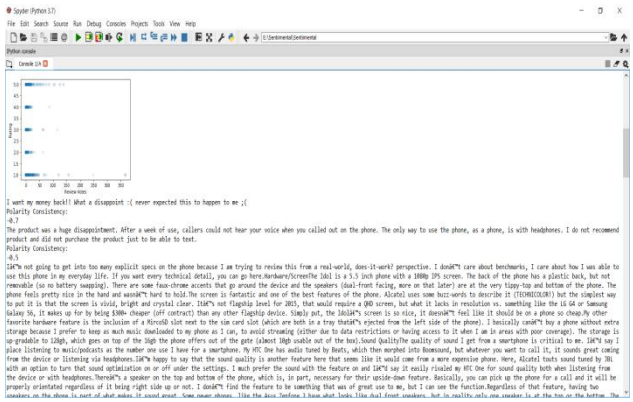

Fig. 5.2 Snapshot of Trust Evaluation process

In the above figure, trust evaluation takes place using fuzzy logic. Using this method it shows that unique positive and negative reviews and rating which are useful for the classification process and also shows that the reviews by description.

5.3 Classification Module

In this stage, it shows the trust value (Polarity consistency value) classification using CNNs. Fig 5.3 Clearly classifies the negative, neutral and positive reviews. Fig 5.4 show that Trustworthiness among the products (in Amazon datasets Mobile reviews are much better than other products) using reviews and ratings.

Fig. 5.3 Snapshot of Classification Process

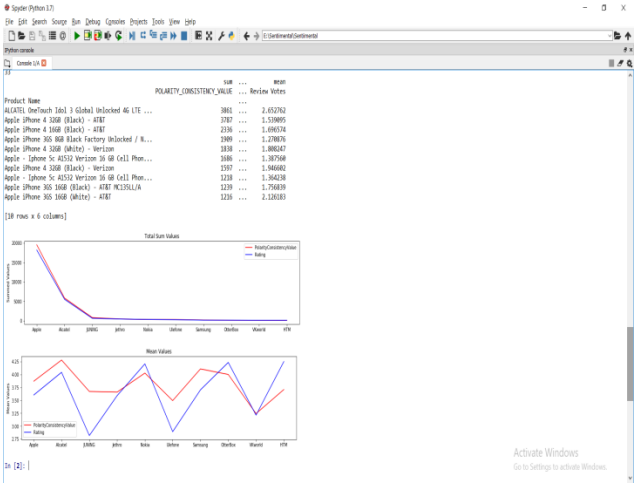

Fig. 5.4 Snapshot of Classification Process

6. CONCLUSIONS

In this paper, integrating machine learning algorithm and fuzzy logic is used to calculate and predict trust based upon ratings and reviews which is not present in the existing system. Fuzzy logic is used for a better assignment of trust and Convolutional Neural Networks used to classify the trust.

Our proposed system improves the trustworthiness and privacy among the users. In the existing system it shows the accuracy of 86%. Compare to the existing system, our proposed system increases the accuracy by 91%.

In the future works, more focus could be on user interface to obtain the information directly from the social network for a better performance. However, in this method, people should be accessed directly to give their opinions about other users in the social network to have the label.

Some of the features that are significant in Semantic Web could be effective in trust evaluation, but those are not present in the information obtained from the social networks. Concentrate on these types of information and their calculation. Furthermore, since trust evaluation is an important factor in improving systems, we suggest applying the proposed method in this paper on these systems to show its performance.

7. REFERENCES

[1] **M. Naderan, E. Namjoo** and **S. Mohammadi**, "Trust Classification in Social Networks Using Combined Machine Learning Algorithms and Fuzzy Logic", Iranian Journal of Electrical and Electronic Engineering, ISSN: 0973-4562, Vol. 15, No. 3, Sep 2019, pp.294-309.

[2] **Xu Chen, Yuyu Yuan, Lilei Lu,** and **Jincui Yang**, "A Multidimensional Trust Evaluation Framework for Online Social Networks Based on Machine Learning", IEEE Translation and Content Mining, IEEE Access, ISSN: 2169-3536 , Vol. 7, Jul 2019, pp.175499-175513.

[3] **I.Hemalatha, Dr.G.P.Saradhi Varma** and **Dr. A.Govardhan**, "Social network analysis and mining using machine learning techniques", Elsevier, Vol. 5, Jun 2019, pp. 603-607.

[4] **Z. Kang and P. Li**, "A machine learning based trust evaluation framework for online social networks," in IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications, Beijing, 24-26 Sep. 2018.

[5] **S. Adali, R. Escriva, M. K. Goldberg, M. Hayvanovych, M. Magdon-Ismail, B. K. Szymanski, W. A. Wallace,** and **G. Williams**, "Measuring behavioral trust in social networks," in IEEE International Conference on Intelligence and Security Informatics (ISI'10), Vancouver, BC, Canada, pp. 150–152, 23-26 May 2017.

[6] **S. Nepal, W. Sherchan,** and **C. Paris**, "STrust: A trust model for social networks," in 10th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom'11), Changsha, China, pp. 841–846, 16-18 Nov. 2017.

[7] **S. Trifunovic, F. Legendre,** and **C. Anastasiades**, "Social trust in opportunistic networks," in INFOCOM IEEE Conference on Computer Communications Workshops, San Diego, CA, USA, 15-19 Mar. 2017.

[8] **J. Zhan** and **X. Fang**, "A novel trust computing system for social," in IEEE International Conference on Privacy, Boston, MA, USA, 9-11 Oct. 2017.

[9] **F. Alam** and **A. Paul**, "A computational model for trust and reputation relationship in social network," in International Conference on Recent Trends in Information Technology (ICRTIT), Chennai, India, 8-9 Apr. 2016.

[10] **G. Yin, F. Jiang, S. Cheng, X. Li,** and **X. He**, "AUTrust: a practical trust measurement for adjacent users in social network," in IEEE Second International Conference on Cloud and Green Computing, Xiangtan, China, pp. 360–367, 1-3 Nov. 2016.

[11] **L. Guo, C. Zhang** and **Y. Fang**, "A Trust-Based Privacy-Preserving Friend Recommendation Scheme for Online Social Networks", IEEE Transactions on Dependable and Secure Computing, Vol. 12, No. 4, pp. 413-427, 2016.

[12] **Y. Zhang, H. Chen,** and **Z. Wu**, "A social networkbased trust model for the semantic web," in The International Conference on Autonomic and Trusted Computing, Wuhan, China, pp. 183–192, 3-6 Sep. 2015.

[13] http://www.trustlet.org/downloaded_epinions.html

[14] **B. Lang**, "Trust degree based access control for social networks," in International Conference on Security and Cryptography (SECRYPT), Athens, Greece, pp. 1–6, 26-28 Jul. 2015.

[15] **S. Meyffret, E. Guillot, L. M´edini,** and **F. Laforest**, "RED: A rich Epinions dataset for recommender systems," Technical Report at LIRIS UMR CNRS, Nov. 2018.

[16] Epinion, http://www.epinions.com.

[17] http://www.trustlet.org/extended_epinions.html

[18] Statista, "Number of social media users worldwide from 2010 to 2021," http://www.statista.com/statistics/278414/number-of-worldwide-social-network-users.

[19] Weka,https://www.cs.waikato.ac.nz/ml/weka, 2017.

AUTHOR BIOGRAPHIES

Dr. P. MARAGATHAVALLI

She received her B.E degree in CSE from Bharathidasan University, M.Tech. degree in CSE from Pondicherry University and PhD degree in CSE from Pondicherry University. She is working as Assistant Professor in the Department of Information Technology; Pondicherry Engineering College. She is a Life member of ISTE.

V. DHIVAKARAN

He is pursuing his B.Tech degree in the Department of Information Technology, Pondicherry Engineering College from Pondicherry University

S. RAVINDRAN

He is pursuing his B.Tech degree in the Department of Information Technology, Pondicherry Engineering College from Pondicherry University.

SHARUN RATHEESH

He is pursuing his B.Tech degree in the Department of Information Technology, Pondicherry Engineering College from Pondicherry University.

E. MADELEINE

She is pursuing her B.Tech degree in the Department of Information Technology, Pondicherry Engineering College from Pondicherry University.