Article

A Comparative Analysis of Different Trust Metrics in User-User Trust-Based Recommender System

Falguni Roy [1,*]

[1] Institute of Information Technology, Noakhali Science & Technology University, Sonapur, Noakhali, Bangladesh.; falguniroy.iit@nstu.edu.bd

[*] Correspondence: falguniroy.iit@nstu.edu.bd;

Abstract: Information overload is the biggest challenges nowadays for any website, especially the e-commerce website. However, this challenge arises for the fast growth of information on the web (WWW) with easy access to the internet. Collaborative filtering based recommender system is the most useful application to solve the information overload problem by filtering relevant information for the users according to their interests. But, the existing system faces some significant limitations like as data sparsity, low accuracy, cold-start and malicious attacks. To alleviate the mentioned issues, the relationship of trust incorporates in the system where it can be between the users or items, and such system is known as the trust-based recommender system (TBRS). From the user perspective, the motive of the TBRS is to utilize the reliability between the users to generate more accurate and trusted recommendations. However, the aim of the paper is to present a comparative analysis of different trust metrics in the context of the type of trust definition of TBRS. Also, the study accomplishes on twenty-four trust metrics in terms of the methodology, trust properties & measurement, validation approaches, and the experimented dataset.

Keywords: trust-based recommender system; pearson correlation coefficient; confidence; mean absolute error; precision; recall; coverage;

1. Introduction

For the extensive evaluation of internet accessibility, information sharing in the World Wide Web (WWW) is becoming an easy job for every user. Currently, most web applications allow millions of users to create, edit and share information in the WWW in an unbound manner. As a result, the system users face information flooding issues where a user could not get the required information in a timely and structured manner for taking the right decision. The issue is also known as the information overload problem [1]. To get rid of the issue, the recommender system (RS) is one of the smartest solutions. The primary objective of the RS is to provide useful personalized information for the user by recommending information from the information pool of the WWW [2]. Generally, a recommender system serves its objective in two steps. In the first step, the recommender system analyses its users' historical data and user-entered data and then, predicts the user's personalized data for recommending information subsequently in the last step based on the output of the first step. The recommender system first inaugurated in the year 1992 by a project named Tapestry [3]. Initially, the recommender system applied for e-commerce [4] and amusement based websites like Amazon [5], Netflix [6] etc. but its application domain is not limited nowadays. Different applications of e-tourism [7], e-learning [4,8], e-government [9] and e-resource service [10] had implemented recommender system to assist its users by receiving faster required information.

Usually, a recommender system (RS) recommends those items to the user that are not yet experienced by the specific user, and the process of recommendation started by deducing a relationship between users or entities [11]. However, a recommender system broadly categorized into three types based on the information filtering and recommendation strategy, which is the collaborative filtering (CF), content-based filtering (CBF), and hybrid filtering (HF) [12]. The content-based filtering (CBF) approach needs two attributes and an algorithm for recommending items to the user. However, the attributes are the user preferences profile and abundant descriptions of items, and the algorithm predicts user succeeding preferences to recommend a new set of items by deducing a matching between attributes [13]. Though the CBF could provide accurate recommendations in the case of new user and item, known as cold-start, as it recommends items by matching user preferences and item descriptions but, it is not lucrative for some limitations [14,15]. CBF could not provide accurate recommendations if there exists inappropriate information in item descriptions and also faces difficulties in retrieving multimedia information like colour, texture, etc. [13,14]. However, CBF also suffers the overspecialization problem by recommending same types of items continuously [4,14]. Further, CBF faces difficulties in measuring the correctness of the recommendation, as it does not contain users' feedback, such as item rating [4].

The collaborative filtering (CF) based RS needs continuous users participation in the system and an algorithm that examines the user-item rating matrix to identify similar tasted users or similar types of items for predicting target user's choices and then provides recommendations [13,16]. The whole process of CF executes in three steps, including data prepossessing, identifying neighbours of the target, and recommending items [17]. Whereas, the target could be any user or item. Generally, CF categorized as the memory and/or model based CF according to the way of neighbourhood selection [12,13,18,19]. Model-based CF utilizes different machine learning algorithm for example Matrix Factorization [20,21], Bayesian method [22], clustering techniques [23], and genetic algorithms [24,25] to inspect user-item rating matrix for offering new recommendations. On the contrary, memory-based CF statistically analyzes the user-item rating matrix to deduce uniformity between items or users and offers recommendations based on the similarities [13,17].

On the other side, hybrid filtering (HF) is the amalgamation of both CBF and CF approaches to enhance both approaches' benefits by alleviating each approach's limitations [26,27]. According to the operations, it categorized into seven category such as switching, weighted, cascade, mixed, feature-combination, meta-level, and feature-augmented hybrid [27]. Usually, the HF needs a vast amount of information for offering recommendations as it is the integration of different approaches; its computational complexity is high and expensive in comparison with others. In spite of the fact that CF suffers some significant flaws such as data sparsity, and cold-start [10] but it is the foremost proficient and widely utilized approach within the RS so far [17,18,28,29].

Usually, a CF-based recommender system faces few problems that affect the system performance. Usually, the RS performance determines by the accuracy of users' tastes prediction with the coverage of the maximum item of the system. The performance could be degrade due to the presence of data sparsity [10,13,18,30,31] and cold-start [10,13,18,32] problems. Data sparsity states the scenario when the amount of the ratings in the user-item rating matrix is not enough for identifying a remarkable overlapping between the items that are rated by a pair of user and causes the difficulties to create accurate predictions [18]. However, the cold-start issue further categorized as either a cold-start user or cold-start item. The cold-start user issue emerges when there exists a large number of new users or the users who have rated a low amount of items in the system [18,27]. Also, the cold-start item defines the same problem in item prospective [13,18]. However, there has a proportional relationship between the cold-start and data sparsity problem in the data. The RS also suffers reliability issues because users are generally unconscious about the recommendation process and they have no monitoring power over it. It creates a reliability issue and decreases users' trust in the recommendations of the system.

The trust-based recommender system (TBRS) is one of the modern forms of the RS. It includes a trust relationship in the system to ameliorate the system's accuracy and reliability to conquer existing issues such as data sparsity and cold-start [19,28]. Usually, in the context of RS, trust determines one's faith in others' aptness of providing valuable ratings concerning the preference of the target [33].

However, TBRS also divides as either explicit trust or implicit trust in terms of the methodology of trust information collection in the system [18,34,35]. Explicit trust in the system is determined by the users directly. Usually, explicit TBRS allows its users to take extra responsibility to assign other users as trusted users [36]. However, explicit trust defines in binary format for the privacy concern, which also limits a user to express the degree of trust to the trusted users. Conversely, implicit trust is defined in the system by using weighted similarity measures [13,29,37] or applying probabilistic technique [35] in the user-item rating matrix. It also allows manifesting the degree of trust between users. However, TBRS further classifies as memory-based and model-based approaches based on the methodology of the trust integration in the RS [38].

In the last few years, several surveys have done on the trust-based recommender system (TBRS), and the surveys focus on either the properties of trust or the process of the recommendation of TBRS. Also, most of the surveys have performed on the implicit trust [34,39,40]. For example, Guo et al. [34] reviewed six implicit trust metrics according to the trust properties. On the other side, Yadav et al. [40] also surveyed implicit trust metrics. However, Gupta et al. [39] presented a survey of eight implicit trust metrics based on the trust properties besides trust establishment type, inferred trust, and network perspective. Selmi et al. [41] reviewed different existing TBRS and classified them by the trust type, relation, value, propagation, aggregation, context, and techniques. On the other side, Jallouli et al. [42] surveyed the trust metrics in RS by trust propagation, user interactions, and rating vectors' perspectives. Although several TBRS surveys have been performed earlier, to the best of the author's knowledge, no survey work has conducted comprehensively to review TBRS according to trust properties, measurement, evaluation, and dataset based on every category of trust. The articles are selected for this survey by considering the popularity of the trust metrics, first, and then the publication database and recency.

1.1. Paper Contribution

This paper systemically demonstrates a comprehensive review of several trust-based recommender system (TBRS) approaches. The contribution of the paper is fourfold and described as follows:

- classified the trust-based recommender system (TBRS) according to trust definition, the subject of trust measurement, and methodology.
- summarized the existing TBRS metrics and techniques.
- presented recent studies on TBRS that solve the existing issues such as data sparsity, cold start, and error of prediction accuracy.
- provided a comparative study in five aspects, such as the methodology of trust determination, properties of trust, trust measurement, evaluation metrics, and the dataset on which the experimentation is examined.

2. Trust-based Recommender System

The trust-based recommender system is the next-gen of collaborative filtering based RS. It applies the concept of trust in the traditional techniques to enhance the system's accuracy and reliability [43]. However, trust initially used in the psychology and sociology disciplines, but currently, it becomes a valuable attribute in the computer science [44] and recommender system [33] fields also. In the sociology discipline, trust determines as a required belief and an oral commitment. However, trust defines as "a commitment to believe in the smooth running of the future actions of another entity" in the computer science discipline [44]. In the RS, trust defines as one's conviction toward others in giving exact ratings relative to the inclinations of that user [33]. Usually, trust is used to scale users' similarity and express the integrity in the relationship between two users to a specific context. The value of the trust can be real or binary numbers, and the range is [-1, 1]. The trust value "1" denotes the full faith of the target user on his trusted user and "0" defines no trust. The negative trust value indicates the level of distrust of the target user has on other users.

2.1. Properties of Trust

Usually, trust is a complex manner of human, and from a sociological perspective, it requires a belief in oral commitments. As a consequence, it isn't an easy task to characterize and model trust between users by using a mathematical equation or computationally. However, in the RS, trust is specified based on some properties by utilizing the user's background, context, history of interaction, reputation, similarity, trust statement, etc. [45]. These properties indicate the existence of trust in the system and also define the way of measuring trust. As stated in trust theory, a trust relationship in the web should have the following distinct properties [13,34,46,47]:

- **Asymmetry.** Trust is asymmetric. It is personal and varies with the different users with their own opinions. A user might have distinct faiths on a certain user according to his experiences. So, if a user u trusts another user v, it is not obvious that user v trusts user u to the same extent.
- **Transitivity.** The calculated trust should be transitive. It is the most important property of the trust and also widely applied in the TBRS. It defines that if a user u trusts user, v and user v trusts another user w, then it can be concluded that user u could trust user w to some extent. In a real-life scenario, people tend to believe a companion of a companion instead of a stranger. By supporting the transitive property, it is possible to establish an indirect trust connection between users by identifying more trusted users to elevate the prediction performance of the RS. The process of the defining trusted users based on the indirect trust connection is called trust propagation [28,48], and the propagated trust is known as the inferred trust.
- **Dynamicity.** By default, trust is dynamic. It is usually built continuously and changed as the time going on with more experiences. It can be expanded or diminished with the positive or negative experiences. For example, the trust of user u on user v is $a\%$ at the time t and the $t+1$ time, the degree of trust of user u on user v could be $(a \pm 1)\%$ based on the experiences.
- **Context Dependence.** Trust explicitly depends on the context on which it has shaped. It means if a user v, who is trustworthy in movie recommendation to the user u, may not be trusted in the recommendation of IT related stuff in the same extent to the same user. In the recommender system, the context refers to which ratings are issued, for example, location, time and items' characteristics or users' profiles, etc. [34].

2.2. The Process of Recommendation Generation

The main job of any recommender system is to generate recommendations efficiently. The trust-based recommender system (TBRS) does the same thing in four phases. The initial phase is trust measurement and the most vital because the system's performance closely depends on it. Further, this phase divides into two sub-phases, and these are trust calculation and trust propagation. The output of this phase is a trust matrix denoted as $T_{U \times U}$ where U is the set of all users who have a trust relationship in the system. The cell value of the trust matrix, known as the trust value and denoted as tu, v, can be a binary or real number, positive or negative. Usually, negative trust value defines the degree of distrust between users [49]. The trust calculation sub-phase takes either user-specified trust value or user-item rating matrix into account as the input and does some analysis to generate the trust matrix, as presented in Table 1.

Table 1. Sample of Trust Matrix.

	User1	User2	User3	User4	User5
User1	-	0.52	0	1	0
User2	0.40	-	-0.65	0	0
User3	0	0.25	-	1	0
User4	0.81	0	0.30	-	-0.50
User5	0.10	0	0	1	-

By using the trust matrix, a trust network can be constructed. Usually, a trust network is a directed graph. Its nodes denote the users of the system and the connecting edge between nodes define their trust relationship. The weight of every edges determines the extent of trust or distrust that a user has on other users. However, a sample of the trust network is demonstrated in the following Figure 1.

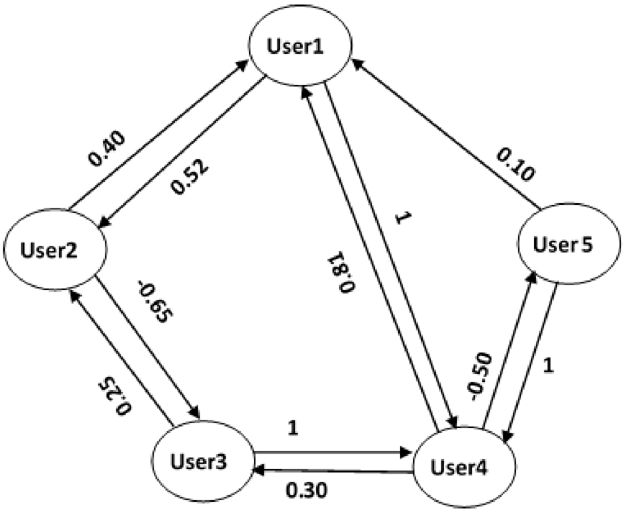

Figure 1. Trust network

Usually, the initial trust matrix is sparse, and many cells of the matrix do not contain any direct trust information between users. For reducing the sparseness of the trust matrix, the trust propagation method is used by applying the transitive property of the trust and generates an indirect trust relationship between users based on the calculated trust value of the previous sub-phase. Figure 2 demonstrates the updated trust network by applying the trust propagation. The indirect trust relation, that is deduced by the trust propagation method, is shown in the dashed arrow in the Figure 2 and the bidirectional indirect trust relation between users are represented as a double dashed arrow. Table 2 represents the final trust matrix of the trust measurement phase, where the inferred trust value denotes as $\pm x$ as it depends on the algorithm of the trust calculation and propagation.

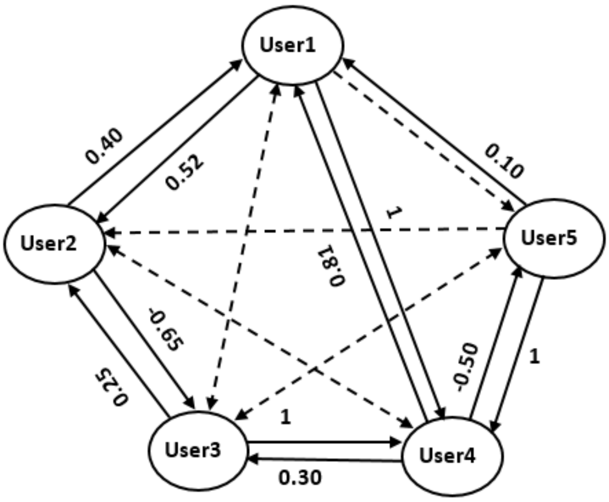

Figure 2. Trust network after propagating trust

The second phrase of TBRS is neighbourhood selection, and the selected neighbours will play an active role at the time of deducing target user's preferences. The neighbourhood selection process is usually done by filtering the top trusted users of the target user. However, the next phase is predicting user preference by aggregating neighbours' tastes. This prediction is made for an unrated item in

Table 2. The Final Trust Matrix of Trust Measurement Phase.

	User1	User2	User3	User4	User5
User1	-	0.52	$\pm x$	1	$\pm x$
User2	0.40	-	-0.65	$\pm x$	0
User3	$\pm x$	0.25	-	1	$\pm x$
User4	0.81	$\pm x$	0.30	-	-0.50
User5	0.10	$\pm x$	$\pm x$	1	-

respect of the target user. One of the popular prediction method, is Resnick [50] that is formulate as Equation 1.

$$p_{u,i} = \bar{r_u} + (r_{v,i} - \bar{r_v}) \tag{1}$$

Here, $v \in U$ is the trusted user of the target user u. Also, $p_{u,i}$ denotes the calculated predicted rating of item i for the target user u. $\bar{r_u}$ and $\bar{r_v}$ determine the average ratings of user u and v, whereas, $r_{v,i}$ indicates the actual rating of item i that is given by the user v. And, in the TBRS, $W(u,v)$ denotes the amalgamation of trust and similarity.

Finally, the last phase is presenting the output that could be either prediction or recommendation or the ranked list. In the case of providing prediction of the unrated items, the system should predict the user preferences about the item by taking active users and items into account. But, in the case of recommendations, the system should provide a list of items that are apposite to the user by taking only the active user as input. On the other side, the ranked list denotes a set of items that are more related to the active user preferences and collected for a recommendation based on predicting user's interest. Usually, a threshold sets for defining the ranked item list based on the minimum user's interest value.

2.3. Classification of Trust-based Recommender System

Usually, a trust-based recommender system (TBRS) utilizes a trust relationship of items or users for providing an accurate recommendation. However, the existence of a trust relationship is defined by a numeric value, known as trust value and that could be binary or any real number, positive or negative. Further, the TBRS divided into user-user trust and item-item trust based on the subject of trust measurement [4,51]. To calculate the trustworthiness, user-user TBRS utilizes either explicit trust information of the users [52,53] or gather implicit trust information of users from a social network [54,55]. On the other side, in item-item TBRS, the reliance of items is measured by applying users' feedback on the items [56] or studying users' activity with these items [28,57,58].However, according to the methodology of trust integration, TBRS can be categorized as memory-based [30,38,59] and model-based [20,38,60,61] approaches. Further, the TBRS can be classified based on the trust definition as either explicit [19,38,52,62] or implicit [12,13,17,18] or hybrid trust-based recommender system [35,63,64]. Figure 3 shows the classification of TBRS in a row.

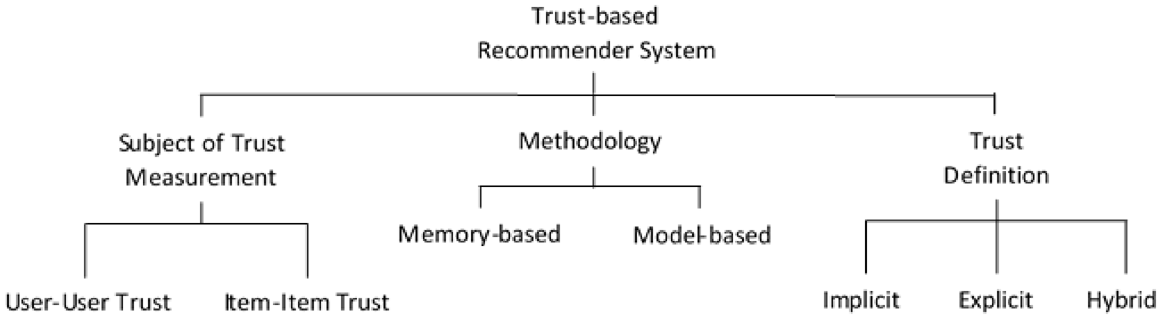

Figure 3. Classification of Trust-based Recommender System

3. Trust-based Recommender System based on Trust Definition

3.1. Commonly Used Notations

This section demonstrates the list of frequently used notation in the TBRS.

U :	a set of all users of the RS
I :	a set of whole items of the RS
R :	a set of entire items ratings that are rated by the users U
u :	individual user of the system where $u \in U$
i :	individual item that exists in the system where $i \in I$
$r_{u,i}$:	a rating of item i by user u and $r_{u,i} \in R$
I_u :	a set of every items that are rated by the user u
$I_{u,v}$:	a set of items that are commonly rated by the pair of user u and v
$\bar{r_u}$:	average rating of user u
$t_{u,v}$:	the degree of trust between user u and v
$sim_{u,v}$:	the intensity of similarity between u and v
$p_{u,i}$:	a predicted rating for user u on the item i
θ :	a threshold for defining trust or similarity
$R_{u \times i}$:	a user-item rating matrix where $u \in U$ and $i \in I$
$T_{u \times v}$:	a trust matrix where user u & $v \in U$
r_{max} :	maximum rating of a RS and the value is 5 in the 5-scale rating.
r_{min} :	minimum rating of the system which is 1 in the 5-scale rating.

3.2. Explicit Trust-based Recommender System

Usually, the explicit trust-based recommender system (ETBRS) utilizes users' predefined trust connection in the system to improve the system's performance by alleviating existing issues such as data sparsity and cold-start. The ETBRS either provides a way of its users to define their trusted users such as $web\ of\ trust$, $trust\ statement$ or incorporates users' social trust relationships in the system. As in both ways, the user plays an active role to define their trust connection, so explicit trust is asymmetric by nature. In ETBRS, the user-item rating matrix and users' explicit trust matrix are taken into account as the input, and the output of the system is the list of predicted ratings of the items that are not rated yet by the respective user. Here, Table 3 presents a sample of user-item rating matrix by assuming a 5-star rating scale system, where a cell value denotes the rating that a specific user rate a specific item, and an empty cell value defines a missing rating. And, Figure 4 demonstrates the architecture of the ETBRS.

Table 3. User-Item Rating Matrix.

	Item1	**Item2**	**Item3**	**Item4**	**Item5**
User1		5		1	3
User2	2		5		4
User3	5	5	1	2	3
User4	1	5	3		
User5				3	

Many researchers have proposed their trust metrics to enhance the system's prediction accuracy. In this study, the following explicit trust metrics have been explained and denoted as **ETM** prefix.

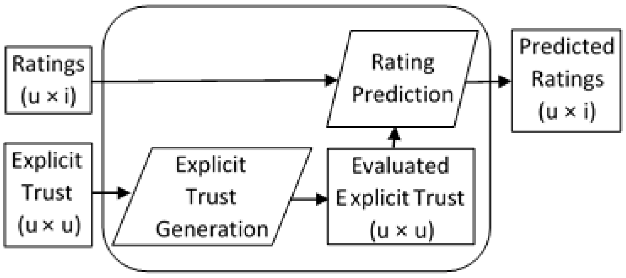

Figure 4. Structure of the Explicit trust-based recommender system (ETBRS)

ETM1 : (a) Guo et al. [65] proposed a trust metric, named *Merge*, by integrating users' social trust information within the system to solve the existing data sparsity and cold-start issues. In the proposed method, the authors first measured the rating of the target user for a specific item i based on the trusted users' ratings on the same item which is called "merging the ratings" and shown in Equation 2.

$$\check{r}_{u,i} = \frac{\sum_{v \epsilon TN_u} t_{u,v} r_{v,i}}{\sum_{v \epsilon TN_u} t_{u,v}} \tag{2}$$

Here, $\check{r}_{u,i}$ is the merge rating of item i for the target user u in respect of the ratings of the trusted users TN_u of user u. And, the same process is executed for each item i of I. The set of merge rated items denotes as $\check{I}_u$ and represents the target user u's preferences. By using the measured merge ratings, similar users are identified for the target user u. For that, Pearson correlation coefficient (PCC), which is a popular similarity detection method, is used in this proposed method. After defining the set of uniform users, another set of nearest neighbours of target user u is selected for by using the succeeding Equation 3.

$$\begin{aligned} s_{u,v} &= \frac{\sum_{i=1}^{I_{u,v}} (\check{r}_{u,i} - \bar{r_u}) \times (r_{v,i} - \bar{r_v})}{\sqrt{\sum_{i=1}^{I_{u,v}} (\check{r}_{u,i} - \bar{r_u})^2} \times \sqrt{\sum_{i=1}^{I_{u,v}} (r_{v,i} - \bar{r_v})^2}} \\ NN_u &= \{v \mid s_{u,v} > \theta, v \in U\} \end{aligned} \tag{3}$$

Where, $I_{u,v} \in \check{I}_u$ and user $v \notin TN_u$. NN_u indicates the set of nearest neighbours of the target user u. In the end, the rating prediction of unrated items for the user u is made by summing the similarity and explicit trust values as follows:

$$\hat{r}_{u,j} = \frac{\sum_{v \in NN_u} s_{u,v} r_{v,j} + \sum_{v \in TN_u} t_{u,v} r_{v,j}}{\sum_{v \in NN_u} s_{u,v} + \sum_{v \in TN_u} t_{u,v}} \tag{4}$$

(b) Guo also proposed another metric by using explicit trust in the recommender system in [33]. In [33], Guo first applied the merge method to get a merged rating by using the formula of Equation 2. Then, the quality of the merged rating is validated by taking account of the certainty of liked and disliked items, and the formula shown in Equation 5.

$$C_{u,i} = \frac{1}{2} \int_0^1 \left| \frac{x^{p_{u,i}} (1-x)^{n_{u,i}}}{\int_0^1 x^{p_{u,i}} (1-x)^{n_{u,i}} dx} - 1 \right| dx \tag{5}$$

Here, $C_{u,i}$ denotes the reliability of the merged rating, $p_{u,i}$ and $n_{u,i}$ are the amount of liked and disliked ratings of user u. After that, the Bayesian similarity measure is used to define the users' similarity by considering overall similarity, chance correlation, represented as $s''_{u,v}$, and the user bias, symbolized as δ. The formula of measuring users' similarity by using Bayesian similarity measure is presented in Equation 6.

$$s_{u,v} = max(s'_{u,v} - s''_{u,v} - \delta, 0) \tag{6}$$

$s'_{u,v}$ is the overall similarity between user u and v that is measured by inversely normalizing the user distance. The user distance is defined as the mean of the rating distance. Whereas the chance correlation is measured by the number of evidence fall in different distance levels independently, and the user bias is 0.04.

The proposed trust methods are asymmetric and transitive by nature but inferred trust identification is not taken into consideration.

ETM2 : Guo et al. [60] offered another metric that incorporates the users' social trust relationships in the RS to reduce the low accuracy and coverage issues. In [60], a clustering method had been used to cluster users according to their rating pattern' similarity and trust relation and named the applied cluster as multiview clustering method. The inferred trust is also calculated to strengthen the trust relationship, and the formula shows below by the Equation 7. And, the renowned partitional clustering method $k - medoids$ algorithm is used in the proposed approach to form a multiview cluster.

$$t_{u,v} = \frac{1}{d_{u,v}} \tag{7}$$

Here, $d_{u,v}$ is the minimum distance between user u and v that is identified by the breath-first search in the social trust network.

ETM3 : Tian et al. [66] also measured two types of trust in their proposed approach that are inferred trust and comprehensive trust of users by using their trust relationships of social networks. The authors first defined the trust as a triple, such as $T = (U, P, D)$ where U is the set of users, and T, P, and D define the trust relationship, set of trust paths and degree of trust between a pair of the user. Normally, the intensity of trust controls by the length of the trust path, and $L(P) = 2$ determines the direct trust relationship between users that gains from the social network. And, if $L(P) > 2$ then T is defined as the inferred trust relation. However, the degree of trust defines by using the formula of Equation 8.

$$D = \begin{cases} D_{u,v}, & D_{u,v} \in P_n, min(L(P_n) = 2) \\ max(\prod_{D_{u,v} \in P_n} D_{u,v}), & min(L(P_n) > 2) \\ 0, & else \end{cases} \tag{8}$$

Here, P_n indicates the possible trust path between user u and v and $D_{u,v}$ denotes the degree of direct trust in the path P_n. Tian et al. [66] also incorporated the dynamic nature of trust at the calculation of the degree of direct trust by considering the interactions of users. The formula of the dynamic update of trust in the degree of direct trust is presented as follows:

$$D_{u,v} = 1 + \sum_{i \in RI_{v,u}} \frac{r_i^a - r_i^b}{r_{max}} \tag{9}$$

Where, $RI_{v,u}$ is a set of recommended items for the user u by the user v and r_{max} is 5. Also, $r_i^a > r_i^b$ denotes user u is satisfied on the recommendation that is provided by user v and the value of $D_{u,v}$ will be increased which will positively effect on the $T_{u,v}$ and $r_i^a < r_i^b$ defines the opposite. However, $r_i^a = r_i^b$ determines complete agreement of user u on the recommendation of user v and it caused the $D_{u,v}$ and $T_{u,v}$ remain unchanged. Afterward, the authors defined the comprehensive trust between users by using Equation 10.

$$C_{u,v} = \frac{D_{u,v}(1 + s_{u,v})}{max_{k \in U_u} D_{u,k} \;\; max_{l \in U_u}(1 + s_{u,l})} \tag{10}$$

Here, $C_{u,v}$ is the comprehensive trust of user u to v, and U_u determines the set of users in the trust relationship of user u. $s_{u,v}$ is the user's similarity that is measured by using a matrix factorization method. Afterwards, $C_{u,v}$ is applied for further proceedings of rating predictions.

ETM4 : He et al. [67] proposed a metric to propagate trust for achieving inferred trust relation between users from their explicit trust network. Usually, the trust matrix that deduced from the explicit trust is sparse, so it is tough to get benefit from it. Trust propagation is a solution that defines the inferred trust between users to reduce the sparseness of a trust matrix. To measure the inferred trust, the authors first built a reciprocal trust matrix and then, applied the Dijkstra's algorithm to discover the shortest path from user u to user v. The calculation of the inferred trust measurement shown in Equation 11.

$$\hat{t}_{u,v} = \frac{1}{N \sum_{n=1}^{N-1} \frac{1}{\hat{t}_{P_n,P_{n+1}}}} \tag{11}$$

Where, N is the number of users who are exists in between the shortest path of user u and v. Also, P_1 and P_n denote user u and v and $P_1 \rightarrow P_2 \rightarrow ... \rightarrow P_n$ indicates the shortest path of from user u to v.

ETM5 : Duricic et al. [62] offered a method by utilizing explicit trust scores to address the cold-start issue of the system. They applied the direct trust connections of users to build an adjacency trust matrix. Afterwards, the Katz similarity (KS) measure is used on the adjacency trust matrix to identify the users' similarity. The formula of the KS measure as follows:

$$\sigma = \sum_{k=0}^{k_{max}} (\alpha A)^k \tag{12}$$

Where, σ denotes the users' similarity matrix, and the single value of the matrix, denoted as $\sigma_{u,v}$, represents the similarity value of user u and v. A indicates the adjacency trust matrix. Also, $\alpha < \frac{1}{\lambda_A}$ where λ_A is the is the largest eigenvalue of adjacency trust matrix. And, $k_{max} = 2$ for the proposed method. By using the following formulas, the authors also defined the users' similarity through propagation when a pair of the user is not explicitly trusted each other.

$$\begin{gathered} \hat{\sigma}_{u,v} = \begin{cases} \sigma^3_{u,v}, & if\, A_{u,v} = 0 \\ 0 & otherwise \end{cases} \\ \sigma^{(k_{max}+1)}_{Dnorm} = D^{-1}(\textstyle\sum_{k=0}^{k_{max}} (\alpha A)^k) D^{-1} \\ \sigma_{boost} = A + \hat{\sigma}_{norm} \end{gathered} \tag{13}$$

Here, D denotes the degree matrix of the trusted network. And, if $\sigma_{boost} = 1$, then it implies users' similarity that identified with the existence of an explicit trust connection in adjacency trust matrix A, otherwise it is measured through propagation.

3.3. Implicit Trust-based Recommender System

Implicit trust-based recommender system (ITBRS) takes the user-item rating matrix as the input. It detects the trust connection between users by identifying the intensity of users' rating pattern's similarity from the rating matrix. Also, the output is the list of predicted items' ratings for the users. Figure 5 shows the structure of ITBRS.

Many trust metrics have proposed to measure the implicit trust from the users' ratings to improve the recommender system performance by alleviating existing problems. In this study, thirteen implicit trust metrics are elaborated as follows and denoted as **ITM1 - ITM13**.

ITM1 : Papagelis et al. [48] defined the user-user implicit trust based on their rating similarity by using the well-known similarity measure algorithm, named Pearson correlation coefficient (PCC). After determining the direct trust of users, the trust propagation mechanism also applied to identify the indirect trust connection between users to eliminate the data sparsity problem. And, the trust propagation mechanism is used for the positive implicit trust. The calculation of direct implicit trust and inferred trust through trust propagation presented in Equation 14 and 15.

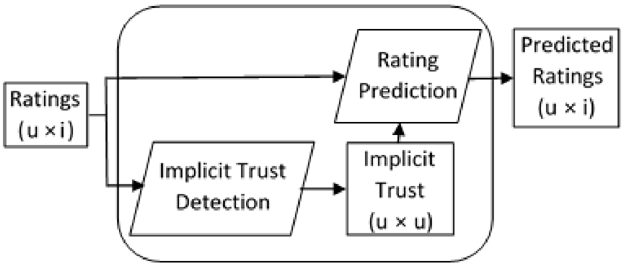

Figure 5. Structure of the Implicit trust-based recommender system (ITBRS)

$$s_{u,v} = \frac{\sum_{i=1}^{I_{u,v}} (r_{u,i} - \bar{r_u}) \times (r_{v,i} - \bar{r_v})}{\sqrt{\sum_{i=1}^{I_{u,v}} (r_{u,i} - \bar{r_u})^2} \times \sqrt{\sum_{i=1}^{I_{u,v}} (r_{v,i} - \bar{r_v})^2}} \tag{14}$$

Here, $t_{u,v} = s_{u,v}$

$$t_{u,w} = \frac{|I_{u,v}|}{|I_{u,v}| + |I_{v,w}|} t_{u,v} + \frac{|I_{v,w}|}{|I_{u,v}| + |I_{v,w}|} t_{v,w} \tag{15}$$

Here, $u, v, w \in U$ are the users and $t_{u,w}$ is computable if $t_{u,v}$ and $t_{v,w}$ are not negative. Though the metric is transitive, it is not asymmetric [34].

ITM2 : Donovan et al. [51] have defined two type of implicit trust. One of them is user-user trust, named as profile level trust and another one is item-item trust, named as item-level trust. Trust is calculated as the proportion of the correct rating set and the common rating item set, which is used for recommendation, of a pair of user. A rating is treated as correct in the correct ratings set if the prediction error is equal or lower than a conferred threshold. However, the Resnick's prediction method is used to determine the predicted ratings [50]. The predicted rating is presented in Equation 1. Whereas, the correct rating and trust measurement are shown in the following Equation 16. This metric is also not asymmetric, and the inferred trust is not taken into account.

$$\begin{gathered} correct(v) = correct(r_{u,i}, r_{v,i}) \iff |p_{u,i} - r_{u,i}| \leq \varepsilon \\ t_{u,v} = \frac{|CorrectSet(v)|}{|RecSet(v)|} \end{gathered} \tag{16}$$

ITM3 : Hwang et al. [68] also proposed a trust metric where the trust score is computed by deriving mean prediction error on the co-rated items between a pair of the user. The rating prediction is measured by the straightforward form of Resnick's prediction formula, given in Equation 1. And, the formula of the trust score measure of Hwang et al. [68] is shown in Equation 17.

$$t_{u,v} = \frac{1}{|I_{u,v}|} \sum_{i=1}^{I_{u,v}} (1 - \frac{|p_{u,i} - r_{u,i}|}{r_{max}}) \tag{17}$$

Hwang et al. [68] also measured the inferred trust value by propagating the trust score to solve the data sparsity limitation and escalate the rating coverage. The inferred trust value is determined by using Equation 15. The authors also proposed another trust named global trust that takes account of the average of direct trust scores of users. According to the trust property, the proposed trust metric only supports the criteria of transitivity [34].

ITM4 : Lathia et al. [69] offered an implicit trust metric by emphasizing the rating differences between users. This trust metric defined the trust between users if they have even a single co-rated item. Mathematically, the trust is defined in [69] as per the following Equation 18.

$$t_{u,v} = \frac{1}{|I_{u,v}|} \sum_{i=1}^{I_{u,v}} (1 - \frac{|r_{u,i} - r_{v,i}|}{r_{max}}) \tag{18}$$

According to the experiments, the authors claimed that the proposed trust metric has improved the rating coverage and fixed the data sparsity issue effectively though the trust propagation is not considered. However, this metric is also symmetric and transitive by nature but the rest of the trust properties, such as dynamicity and context dependence, are not taken into consideration.

ITM5 : Yuan et al. [70] proposed an implicit binary trust based on the similarity between users. For calculating users' similarity, they applied PCC that shows in Equation 14. After that, the binary trust is determined by setting two threshold values in Equation 19.

$$t_{u,v} = \begin{cases} 1 & \text{if } s_{u,v} > \theta_s, |I_{u,v}| > \theta_i \\ 0 & \text{otherwise} \end{cases} \tag{19}$$

Here, θ_s and θ_i are the thresholds and the value of θ_s is 0.75 because PCC becomes transitive if the value of it exceeds 0.707 [71] and θ_i is 2. The authors also considered trust propagation using following Equation 20.

$$t_{u,w} = \frac{\log n / \log k - d_{u,w} + 1}{\log n / \log k} \tag{20}$$

Where, n, k and $d_{u,w}$ denote the size, mean degree of the implicit trust, and the trust propagation span between user u and w.

ITM6 : Bedi et al. [72] have generated an implicit trust metric by combining users' similarity with the confidence measure. Usually, confidence defines the reliability between users in terms of the amount of co-rated items [48]. The users' similarity is measured by taking consideration of the positive value of PCC, shown in Equation 14. And, the confidence between users is calculated by the following Equation 21.

$$conf_{u,v} = \frac{|I_{u,v}|}{|I_v|} \tag{21}$$

After that, the implicit trust is identified by performing harmonic mean based on the users' similarity and confidence.

$$t_{u,v} = \begin{cases} \frac{2 * s_{u,v} * conf_{u,v}}{s_{u,v} + conf_{u,v}} & \text{if } s_{u,v} \neq 0 \,\&\, conf_{u,v} \neq 0 \\ k * conf_{u,v} & \text{if } s_{u,v} = 0 \,\&\, conf_{u,v} \neq 0 \\ 0 & \text{if } s_{u,v} = 0 \,\&\, conf_{u,v} = 0 \end{cases} \tag{22}$$

Here, k denotes a small constant. Since, the confidence depends on the trusted user's ratings, so $conf_{u,v}$ may not be similar to $conf_{v,u}$ which deduce asymmetric trust between a pair of user u and v. Also, the authors have used an ant colony algorithm for defining the inferred trust and applied a pheromone updating strategy for supporting the dynamic nature of trust. However, the proposed metric is asymmetric, transitive, and dynamic, but context dependent is not taken into account.

ITM7 : Shambour et al. [31] also used Resnick's prediction formula (shown in Equation 1), mean squared distance (MSD) and Jaccard for define the proposed implicit trust metric. The mean squared distance (MSD), Jaccard and computed trust is presented in following Equation 23, 24 and 25.

$$MSD_{u,v} = 1 - \frac{\sum_{i=1}^{I_{u,v}} (p_{u,i} - r_{u,i})^2}{|I_{u,v}|} \tag{23}$$

$$Jaccard_{u,v} = \frac{|I_{u,v}|}{|I_u \cup I_v|} \tag{24}$$

$$t_{u,v} = Jaccard_{u,v} * MSD_{u,v} \tag{25}$$

If the calculated trust of a pair of user is above a threshold (λ), then they are treated as a trusted neighbour and able to process in trust propagation. The authors' proposed direct trust propagation for generating inferred trust and combined trust and similarity for rating prediction. However, the proposed implicit trust is transitive, but asymmetry, dynamicity, and context dependence are not taken into consideration.

ITM8 : Roy et al. [13] defined an implicit trust metric by using Resnick's prediction method [50], mean squared distance (MSD), and confidence. The authors have modified the Resnick's prediction method by integrating users' rating time to emphasize users' current interest. The formula of modified Resnick's prediction method is presented in the succeeding Equation 26.

$$p_{u,i} = \bar{r_u} + (r_{v,i} - \bar{r_v})e^{-T\lambda} \tag{26}$$

Here, λ is a personalized constant that defines decay rate, and T denotes the time interval between user v's recent rating time and specific rating time of item i. Also, the formula of MSD and confidence are given in Equation 23 and 21. And, the formula of trust metric presents in Equation 27.

$$\begin{aligned} t_{u,v} &= MSD_{u,v} * Conf_{u,v} \\ &= \frac{I_{u,v} - \sum_{i=1}^{I_{u,v}} \left(\left(\bar{r_u} + (r_{v,i} - \bar{r_v})e^{-T\lambda} \right) - r_{u,i} \right)^2}{I_v} \end{aligned} \tag{27}$$

Since the confidence is asymmetric by nature, so the proposed trust is not symmetric. Also, the proposed trust is dynamic as it considers users' rating time in the account. On the other side, the proposed implicit trust is potentially transitive as they did not offer any method to identify the inferred trust. However, the authors did not consider the context dependence also.

ITM9 : Azadjalal et al. [73] proposed a metric by using Pareto dominance and confidence to recognize the most trusted users of a target user. At the first step, the implicit trust statements of the users are determined based on their similarity, and if the similarity exceeds the predefined threshold (θ_t) then the users are treated as the trusted users. The users' similarity is calculated by using the Pearson correlation coefficient, shown in Equation 14. After that, MoleTrust (presented in Equation 28) is applied to define the inferred trust between users.

$$t_{u,v} = \frac{d_{max} - d_{u,v} + 1}{d_{max}} \tag{28}$$

Here, $d_{u,v}$ denotes the distance of a pair of user u and v and $d_{max} \in$ [1,3] is the highest distance for propagating trust. Azadjalal et al. [73] also proposed rating imputation by estimating the new rating of the item to reduce data sparsity issue and calculate the reliability by validating the estimated ratings. The formula, mentioned by the Equation 5, is used to validated the reliability and denoted as $C_{u,i}$. Also, the formula of rating imputation is given in the following Equation 29.

$$\tilde{r}_{u,i} = \frac{\sum_{v \in T_u} t_{u,v} r_{v,i}}{\sum_{v \in T_u} t_{u,v}} \tag{29}$$

Here, $\tilde{r}_{u,i}$ denotes the estimated rating of item i for user u and T_u represents a set of trusted users of user u. Also, $C_{u,i} \in$ (0, 1] is the reliability value of the estimated rating $\tilde{r}_{u,i}$. Whereas, $p_{u,i} = \mid r_{v,i};\ r_{v,i} > r_{median};\ v \in T_u \mid$ and $n_{u,i} = \mid r_{v,i}; r_{v,i} \leq r_{median};\ v \in T_u \mid$ denote the amount of like and dislike ratings of item i that are rated by the all trusted users of user u where $r_{median} = 3$ in the 5-star rating scale recommender system. Afterward, users' confidence are computed by considering the reliability of the estimated ratings in the classical Pearson correlation coefficient, shown in Equation 30. And, the confidence values are higher than a threshold (θ_C), are taken in consideration for next proceedings.

$$UC_{u,v} = \frac{\sum_{i=1}^{I_{u,v}} C_{u,i}(r_{u,i} - \bar{r_u})C_{v,i}(r_{v,i} - \bar{r_v})}{\sqrt{\sum_{i=1}^{I_{u,v}} C_{u,i}^2(r_{u,i} - \bar{r_u})^2}\sqrt{\sum_{i=1}^{I_{u,v}} C_{v,i}^2(r_{v,i} - \bar{r_v})^2}} \tag{30}$$

After defining the confidence between the pair of user, Pareto dominance concept is applied to determine the set of most effective trusted neighbors for the target user and the final computed trust value as follows:

$$TW_{u,v} = t_{u,v} \times UC_{u,v} \tag{31}$$

Azadjalal et al. [73] used Resnick's prediction formula for predicting recommendation. Although the proposed trust metric is transitive and asymmetric, dynamicity and context dependence is not taken into account.

ITM10 : Choudhary et al. [74] introduced two types of trust metrics named similarity-based and knowledge-based trust metrics. For the similarity-based trust, the users' ratings are normalized into 0 to 1 and classified each item into three categories, such as liked, disliked, and neutral item. Afterwards, the similarity-based trust between users is defined based on the items' classification. The formulas of ratings' normalization and similarity-based trust calculation are presented in the following Equation 32

$$O(u_i) = \begin{cases} 0 & r_{u,i} = min \\ \frac{r_{u,i} - min}{max - min} & min < r_{u,i} < max \\ 1 & r_{u,i} = max \end{cases} \tag{32}$$

$$t_{u,v} = \frac{1}{2}\left[\frac{|LItem_u \bigcap LItem_v|}{|LItem_u|} + \frac{|ULItem_u \bigcap ULItem_v|}{|ULItem_u|}\right]$$

Here, $LItem$ denotes liked item where $LItem = \{i : O(u_i) > 0.5\}$ and $ULItem$ determines disliked item where $ULItem = \{i : O(u_i) < 0.5\}$. Also, neutral item defines as $NItem = \{i : O(u_i) = 0.5\}$ where $NItem$ denotes neutral item.

For the knowledge-based trust, Choudhary et al. [74] considered the rating pattern similarity between users based on the common rated items and for that, the deviation of ratings of the common items are identified first, and then normalized the deviation between 1 to 5. Then, the trust is determined by using the succeeding formula of Equation 33.

$$\dot{r}_{u,v} = \begin{cases} 5 & 0.0 \leqslant |r_{u,i} - r_{v,i}| \leqslant 0.5 \\ 4 & 0.5 < |r_{u,i} - r_{v,i}| \leqslant 1.0 \\ 3 & 1.0 < |r_{u,i} - r_{v,i}| \leqslant 2.0 \\ 2 & 2.0 < |r_{u,i} - r_{v,i}| \leqslant 2.0 \\ 1 & otherwise \end{cases} \tag{33}$$

$$Kt_{u,v} = \begin{cases} 0 & \dot{r}_{u,v} = 1 \\ \frac{\dot{r}_{u,v} - 1}{4} & 1 < \dot{r}_{u,v} < 5 | \dot{r}_{u,v} I_u \\ 1 & \dot{r}_{u,v} = 5 \end{cases}$$

Where, $\dot{r}_{u,v}$ denotes the indicator of rating pattern similarity. Both trust metrics are asymmetric as the similarity-based trust metric is not symmetric. Also, the trust metrics are potentially transitive. However, both trust metrics do not consider the dynamicity and context dependence properties of trust. Also, inferred trust is not taken into account.

ITM11 : Zahir et al. [12] also applied the liked and disliked items concept in their trust metric and calculated the trust, named as $AgreeRelTrust$, by combining users' agreements and relative activities in the system. The agreement $A_{u,v}$ of a pair of user is defined according to the positive and negative agreements in co-rated items where positive agreement denotes liked items by both users, and negative agreement determines the disliked items of both users. The formula of positive and negative agreement, and $AgreeRelTrust$ are presented in following Equation 34.

$$\begin{gathered}
posAgreement_{u,v} = |r : R_{(u,r) \in R_v} \cap R_{(v,r) \in R_u} \cap \\
R_{(u,r)} \geq \beta \cap R_{(v,r)} \geq \beta| \\[1em]
negAgreement_{u,v} = |r : R_{(u,r) \in R_v} \cap R_{(v,r) \in R_u} \\
\cap R_{(u,r)} < \beta \cap R_{(v,r)} < \beta| \\[1em]
A_{u,v} = \frac{posAgreement_{u,v} + negAgreement_{u,v}}{|R_u \cap R_v|}
\end{gathered} \tag{34}$$

Here, β is the separator of positive and negative ratings. R_u and R_v are the individual rating vectors of user u and v, and the range of the users' agreement is [0, 1] where, 0 indicates no agreement between users; similarly, 1 denotes complete agreement.

Furthermore, Zahir et al. [12] measured the relative activity of the users who have not rated an item commonly. The succeeding Equation 35 denotes the formula of measuring relative activity of user u with respect to user v.

$$RelA_{u,v} = \begin{cases} \frac{1}{1+e^{-ac}} & if \;\; |R_u| + |R_v| > 0 \; AND \;\; v \neq u \\ 0 & else \end{cases} \tag{35}$$

Where, $ac = \frac{|R_u|}{|R_u + R_v|}$ and, $|R_u|$ and $|R_v|$ denotes the lengths of the rating vectors of the users. The final trust metric is computed by using Equation 36 where λ and ε are the hyper parameters that manage the engagement of users relative activity and agreement in the final trust calculation.

$$AgreeRelTrust_{u,v} = A_{u,v}^{\lambda} + \varepsilon RelA_{u,v} \tag{36}$$

Based on the experiment, Zahir et al. [12] stated that the proposed metric had improved the prediction accuracy with the item coverage and able to define trust even the users do not contain any commonly rated item. Also, the calculated trust is asymmetric as the relative activity between the users is not symmetric.

ITM12 : Son et al. [36] proposed an implicit trust metric by considering users' relative and asymmetric trust nature of the recommender system. In the proposed metric, the authors first defined the relative similarity between a pair of user based on the average ratings of the items, that is used to generate an asymmetric trust network. After that, the trust propagation is applied to identify the inferred trust to reduce the data sparsity problem and it is done by using the shortest path method. Though the proposed metric is asymmetric and transitive, dynamic and context dependence characteristics are not taken into account. The formula of direct and inferred trust calculation are given in the Equation 37.

$$\begin{gathered}
rs_{u,v} = \begin{cases} \frac{r_{max} - |r_{u,i} - r_{v,i}|}{r_{max} - |r_{u,i} - \bar{r}_i|} & if|I| > 0 \\ 0 & otherwise \end{cases} \\[1em]
dt_{u,v} = \frac{\sum_{i \epsilon I_{u,v}} (rs_{u,v})_i}{I_{u,v}} \\[1em]
Int_{u,v} = \mathbf{max}_{p \epsilon S_{u,v}} \sum_{i=1}^{k} \frac{k-i+1}{k} . dt_{a_i, a_{i-1}}
\end{gathered} \tag{37}$$

Here, $rs_{u,v}$, $dt_{u,v}$ and $Int_{u,v}$ denote the relative similarity, direct trust and inferred trust between user u and v. Also, $p = u, u_1, u_2, ..., u_k, v$ is the set of users who exits between shortest path the user u and v. $S_{u,v}$ denotes the list of total shortest paths from user u to v in the fixed distance.

ITM13 : Barzegar et al. [17] had taken users' similarity, confidence, analogous opinion, and rating distance into account to measure the direct implicit trust of a pair of user. The trust is asymmetric as the calculation of the confidence of users is asymmetric by nature. For defining the users' similarity, the Pearson correlation coefficient (PCC) is used and presented in Equation 14 and confidence is measured by utilizing the formula of Equation 21. However, the rating distance is calculated by using the users' rating interval of the common rated items, shown in Equation 38.

$$rateDistance_{u,v} = \frac{1}{1 + (\sqrt{\sum_{i \in I_{u,v}} (r_{u,i} - r_{v,i})^2})} \tag{38}$$

However, the analogous opinion between users is computed by measuring the tendency ratio of providing similar ratings to the common rated items by the pair of user. This ratio is defined by the three aspects, such as satisfaction, dissatisfaction, and indifference toward items. In a 5-star rating scale system, the users' satisfaction is identified if the ratings of the common rated items are four or above. Whereas, if the ratings of the common rated items are below three, are accounted as the users' dissatisfaction. Also, the indifference is defined if the ratings of the common rated item is in between 3 and 4. The satisfaction, dissatisfaction, and indifference calculations are shown in Equation 39, and the analogous opinion of a pair of user is demonstrated by the Equation 40. Also, the final trust calculation is presented by Equation 41. According to the authors' statement, the trust metric had improved the system accuracy, precision, and recall by mitigating the data sparsity issues. But, dynamicity, and context dependence properties of trust are not considered at the time of trust measurement. Also, the inferred trust is not defined for a pair of user.

$$\begin{aligned} Satisfied_{u,v} &= \frac{|I^S_{u,v}|}{|I^S_u \cup I^S_v|} \\ DisSatisfied_{u,v} &= \frac{|I^D_{u,v}|}{|I^D_u \cup I^D_v|} \\ Indifference_{u,v} &= \frac{|I^I_{u,v}|}{|I^I_u \cup I^I_v|} \end{aligned} \tag{39}$$

$$similarOpinion_{u,v} = \frac{\begin{array}{c} Satisfied_{u,v} + DisSatisfied_{u,v} \\ + Indifference_{u,v} \end{array}}{3} \tag{40}$$

$$t_{u,v} = \begin{array}{c} s_{u,v} + conf_{u,v} + similarOpinion_{u,v} + \\ rateDistance_{u,v} \end{array} \tag{41}$$

3.4. Hybrid Trust-based Recommender System

However, a hybrid trust-based recommender system (HTBRS) utilizes the advantage of both explicit and implicit trust in the system by alleviating the limitations of both trusts. If a system relays only the explicit trust, then without the presence of explicit trust the system won't recommend any item to its users. Whereas, the implicit trust measurement depends on the users' ratings, and in this case, usually, a user has no control over it. So, It also causes a reliability issue of the system. Whereas, the hybrid trust is a combination of both trusts which generates a valuable and meaningful recommendations by considering both trusts' limitations. The HTBRS takes the user-item rating matrix and users' explicit trust matrix as the input of the system and provides a list of predicted items as the output. The following Figure 6 shows the architecture of the HTBRS.

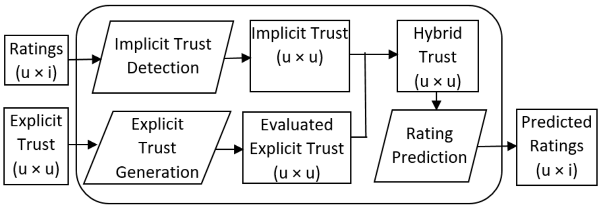

Figure 6. Structure of the Hybrid trust-based recommender system (HTBRS)

Many researches have been done on the HTBRS and proposed different hybrid trust metrics. In this study, five trust metrics are short-listed for comparative analysis based on the popularity and publication time.

HTM1 : Zheng et al. [75] proposed a hybrid trust metric for the online Community of Practices (CoPs) to incorporate the user-user explicit and implicit trust. In the online CoPs, a learner acquired votes on the own post from other learners. Also, the voting actions reflect the author's reputation, who posted the post and other learners' attitudes toward the post. This voting and user reputation defined the explicit trust connection from which the global trust can be deduced. Whereas, a learner's learning priorities can be exposed by mining own posted textual contents in the online Community of Practices. Hence, accounting of having interests in the common topic, users' implicit trust can be deduced, and that is called local trust in the CoP perspective. In the proposed method, the authors measured the global trust based on the users' (learners') reputation scores and total achieved votes and deduced the users' local trust according to the learning preferences from own question&answer histories. Afterwards, the authors proposed the hybrid trust by combining both global and local trust of users. The formula of global, local, and hybrid are shown as follows:

$$
\begin{aligned}
GT_u &= a \times Rp_u + (1-a) \times Vote_u, 0 < a < 1, \\
Rp_u &= f(x) = (logistic(\tfrac{x}{Rp_{avg}}) - 0.5) \times 2 \\
Vote_u &= f(x) = (logistic(\tfrac{x}{Vote_{avg}}) - 0.5) \times 2 \\
logistic(x) &= \tfrac{1}{1+e^{(-x)}} \\
LT_{u,v} = s_{u,v} = cos(\theta) &= \tfrac{A \cdot B}{\|A\|\|B\|} \\
&= \tfrac{\sum_{i=1}^{n} A_i \times B_i}{\sqrt{\sum_{i=1}^{n} A_i^2}\sqrt{\sum_{i=1}^{n} B_i^2}} \\
HT_{u,v} &= b \times GT_v + (1-b) \times LT_{u,v}, 0 < b < 1
\end{aligned}
\tag{42}
$$

Here, $GT_u, LT_{u,v}$ & $HT_{u,v}$ denote the global, local & hybrid trust of users. a & b are the parameters and deduced from the model training where the parameter a balanced the constitution proportions from user's reputation scores and achieved votes, and b defines the constitution proportions of the local and global trust accordingly. Rp_{avg} denotes the average reputation score of all users and $Vote_{avg}$ defines the amount of average received vote of all users. However, Latent Dirichlet Allocation (LDA) is applied to execute text mining inspection for defining local trust between users. However, the hybrid trust method is not symmetric and inferred trust, dynamicity, and context dependence are not taken into consideration.

HTM2 : Chen et al. [76] also proposed a hybrid metric to refine prediction correctness and convergence speed by using both explicit and implicit trust of users. The authors also offered a new trust, named as composite trust by using both trusts. And, the recommendation task is executed by incorporating it into probabilistic matrix factorization (PMF). Usually, explicit trust is a pre-defined or manually user-entered value. However, for the privacy concern, it is in binary format, which can not accurately state the users' trust relationship. By considering this, the authors substituted the explicit trust by measuring the incoming and outgoing trust link of a user. Afterwards, the implicit trust of users is measured by deducing users' similarity that is calculated through PCC and by applying a mapping function $f(x) = (x+1)/2$, which converted the range of the implicit trust into [0, 1] from [-1, 1]. Further, the composite trust is defined by using linear regression. The explicit (et), implicit (it) and composite trust (ct) calculation are shown in Equation 43.

$$
\begin{gathered}
et_{u,v} = \sqrt{\frac{d^{-}(V_v)}{d^{+}(V_u)+d^{+}(V_v)}} \\
it_{u,v} = s_{u,v} = \frac{\sum_{i=1}^{I_{u,v}} (r_{u,i}-\bar{r_u}) \times (r_{v,i}-\bar{r_v})}{\sqrt{\sum_{i=1}^{I_{u,v}} (r_{u,i}-\bar{r_u})^2} \times \sqrt{\sum_{i=1}^{I_{u,v}} (r_{v,i}-\bar{r_v})^2}} \\
ct_{u,v} = \beta \times et_{u,v} + (1-\beta) \times it_{u,v}, 0 < \beta < 1
\end{gathered}
\tag{43}
$$

Where, $d^{+}(V_v)$ and $d^{-}(V_v)$ represent the outgoing and incoming trust link of user v. β is parameter that is obtained from training model and it is 0.5 for the proposed model. However, $et_{u,v} \neq et_{v,u}$, so $ct_{u,v} \neq ct_{v,u}$. Afterward, Chen et al. [76] applied PMF to perform the recommendation task.

HTM3 : Wang et al. [77] used two neural models to enhance the recommendations quality by integrating the explicit and implicit trust to reduce the data sparsity and cold-start problem. The authors applied one Denoising Autoencoder (DAE) in TBRS, named as $TDAE$, to incorporate the users' ratings with the explicit trust connections of the social networks to accurately model the users' choices. Another neural network model, named $TDAE++$, for pulling out the implicit trust connections of the users by deducing their ratings' similarity. Finally, both trust values are inserted into the input and hidden layer of the neural network to gain better trust-able semantic portrayals of the users. The formula of explicit and implicit trust insertion at the input and hidden layer of the network is shown in the Equation 44.

$$
\begin{gathered}
\hat{z} = \rho(W'(\rho(W^T\{x_u, t_u\} + b)) + b') \\
s_{u,v} = \begin{cases} 1, & u = v \\ (1-\frac{1}{n})(\frac{PCC_{u,v}+1}{2}) & u \neq v \end{cases} \\
t_{u,v} = \begin{cases} 1 & if s_{u,v} \geq \theta \\ 0 & otherwise \end{cases}
\end{gathered}
\tag{44}
$$

Here, $\hat{z}$ denotes the conclusive portrayal of the output layer, and ρ defines the hyperbolic tangent function. T is the proportion of the trust value that incorporated into the input or hidden layer. $t_u \in \mathbb{R}^T$ indicates the trust information and x_u is the input vector for user u. Whereas, $b \in \mathbb{R}^H$ and $b' \in \mathbb{R}^N$ are the bias vectors. On the other side, $W' \in \mathbb{R}^{T \times H}$ and $W^T \in \mathbb{R}^{H \times (N+T)}$ are the weight matrices. And, n denotes the total co-rated items between user u and v.

HTM4 : Ayub et al. [63] introduced another hybrid metric as an integration of explicit and implicit trust with the users choices' uniformity to generate a merged rating profile for a specific user. In the proposed metric, the trusted users of the specified user are figured out first and then assembled by the explicit trust that is either delivered by the existing system users or deduced from the trust propagation. For propagating trust, the MoleTrust method is applied to give more importance to trusted users who exists in the short distance. Afterwards, the ratings of the assembled trusted users are merged into one value for every item that is not rated by the specified user but rated by minimum one trusted user of the specified user. However, if the specified user did not explicitly trusted by others, then implicit trust connections are determined by using the ratings that is given by the other users. And, the implicit trust of users is measured by applying **ITM4** method, also mentioned in Equation 18. Onward, the calculated explicit and implicit trust were combined to define the hybrid trust between users. Equation 45 demonstrates the explicit inferred trust and hybrid trust formula.

$$et_{u,v} = \frac{1}{d} \times et'_{u,v}$$
$$ht_{u,v} = et_{u,v} \times it_{u,v} \tag{45}$$

Here, $et_{u,v}, et'_{u,v}, it_{u,v}$ & $ht_{u,v}$ denote the explicit trust, inferred explicit trust, implicit and hybrid trust of a pair of user u and v respectively. d defines the trust propagation distance, and the limit is [0, 3]. Whereas, the user preference uniformity (UPU) is measured by using Jaccard and user rating preference behaviour (RPB). However, RPB is computed through a cosine function based on the users' mean rating and variance, shown in Equation 46.

$$UPU_{u,v} = Jaccard_{u,v} \times RPB_{u,v}$$
$$RPB_{u,v} = cos(|\bar{R}_u - \bar{R}_v| \times |var_u - var_v|) \tag{46}$$

HTM5 : Parvin et al. [35] proposed a metric that utilizes the trust statement as an auxiliary information with Ant Colony Optimization (ACO) method. The proposed approach contains three phases. In the first phase, users' explicit trust connection is measured based on the trust statements and inferred trust, and implicit trust is identified by calculating users' similarity through PCC. Afterwards, both trust is applied to rank the users based on trust relations. In the second phase, ACO is used on the top high ranked trusted neighbours to identify their importance values. In the last step, the prediction task is executed. Equation 47 presents the formula of explicit trust connection identification and the weight calculation for the ranked user.

$$w_{u,v} = \begin{cases} \frac{2 \times s_{u,v} \times t_{u,v}}{s_{u,v} + t_{u,v}} & s_{u,v} + t_{u,v} \neq 0 \; and \; s_{u,v} \times t_{u,v} \neq 0 \\ t_{u,v} & t_{u,v} \neq 0 \; and s_{u,v} = 0 \\ s_{u,v} & t_{u,v} = 0 \; and s_{u,v} \neq 0 \end{cases}$$
$$t_{u,v} = \frac{d_{max} - d_{u,v} + 1}{d_{max}} \tag{47}$$
$$d_{max} = \frac{ln(n)}{ln(k)}$$

Where, d_{max} determines highest propagation limit between the pair of user and $d_{u,v}$ indicates the trust propagation length of user u and v. However, k is the mean degree of the trust network, and n represents the amount of users that exists between the network.

4. Evaluation Metrics

After proposing a new metric, every author has to evaluate the performance as well as their claiming benefits of the proposed metric. Various evaluation metrics are applied to validate the efficiency of the system. And, the efficiency is measured by in terms of correctness, coverage, and diversity. However, most of the applied evaluation metrics are described here according to the following categories [78]:

4.0.1. Predictive Accuracy Metrics

Usually, the metrics belong in this category measure the closeness between the predictive and true ratings. MAE, iMAE, MAUR and RMSE are associated to this categary.

- **Mean absolute error (MAE)** is the commonly used evaluation metric and measured the level of accuracy of the proposed approach by collating the deviation of predicted and real ratings of the items [78]. Usually, the relationship between the system's performance and MAE is inverse.
- **Inverse mean absolute error (iMAE)** is the transpose of MAE that is normalized by dataset into highest and lowest rating scales [30].
- **Mean absolute user error (MAUE)** is an alternative of MAE and measures the error from user perspective [73].
- **Root-mean-square error (RMSE)** measures the accuracy of the predictions based on the root mean square difference of predicted and true ratings of the items and the lower value of RMSE denotes the higher prediction accuracy [63].

Mathematically MAE, iMAE, MAUE and RMSE are defined as follows:

$$\begin{aligned} MAE &= \frac{\sum_{i=1}^{I_u} |r_{u,i} - p_{u,i}|}{I_u} \\ iMAE &= 1 - \frac{MAE}{R_{max} - R_{min}} \\ MAUE &= \frac{\sum_{u=1}^{U_u} MAE_u}{N_u} \\ RMSE &= \sqrt{\frac{\sum_{i=1}^{N_u} |r_{u,i} - p_{u,i}|^2}{N_u}} \end{aligned} \tag{48}$$

Where, I_u signifies the amount of rated items of user u. And, U_u defines the number of users for them the proposed algorithm could predict at least one rating.

4.0.2. **Suitability metrics**

This category contains coverage and it is one of the popular metric that validate the proposed approach's performance. Usually, coverage is applied to identify the prediction percentage of the proposed approach [36]. The coverage divides into two subcategories, such as user coverage (UC) and rating coverage (RC).

- **User coverage (UC)** denotes the ratio of users for which the proposed approach could predict at least one rating.
- **Rating coverage (RC)** measures the proportion of items for which the algorithm can predict rating.

The UC and RC are mathematically defined as follows:

$$\begin{aligned} UC &= \frac{N_v}{N_U} \\ RC &= \frac{N_p}{N_R} \end{aligned} \tag{49}$$

Here, N_v denotes the users' count for which the proposed approach could predict minimum one rating and N_U is the total users who exist in the system. Whereas, N_p and N_R indicate the amount of predicted ratings and total ratings.

4.0.3. Classification Accuracy Metrics

Classification accuracy metrics assess the occurrence of accurate or inaccurate prediction of the proposed system by claiming an item is good. The following metrics are affiliated in the category.

- **Accuracy** denotes the ratio of correct prediction among entire prediction that is predicted by the proposed approach [17].

- **Precision** measures the ratio of predicted items that are matched with the users' choices in the dataset [78].
- **Recall** identifies the ratio of the existence of correct predicted items among the ranked listed items in the dataset.
- If any two evaluation metrics could not anticipate any decent validation results, then **f-measure (F1)** is applied as a weighted harmonic mean of those evaluation metrics to ensure better evaluation of the proposed approach.
- **Receiver operating characteristic (ROC)** measures the diagnostic power of the proposed approach. Usually, ROC is a curve that plotted by the recall and the 1-specificity [48].

Assuming that in a 5-star rating based RS, positive ratings belong in 3-5, and the range of the negative ratings is 1-2. The prediction of an item i could be four types as if

- $r_i \in [3,5]$ and $p_i \in [3,5]$ then it can conclude as the true positive prediction (TPP), or
- $r_i \in [1,2]$ and $p_i \in [1,2]$ then it is the true negative prediction (TNP), or
- $r_i \in [3,5]$ and $p_i \in [1,2]$ then it is called the false negative prediction (FNP), or
- $r_i \in [1,2]$ and $p_i \in [3,5]$ then it is known as the false positive prediction (FPP).

Here, r_i and p_i denote the actual and predicted rating of item i. The mathematical form of the accuracy, recall, precision, F1 and (1-specificity) present in the Equation 50.

$$\begin{gathered}
Accuracy = \frac{\sum TPP + \sum TNP}{\sum(TPP+TNP+FPP+FNP)} \\
Precision = \frac{\sum TPP}{\sum(TPP+FPP)} \\
Recall = \frac{\sum TPP}{\sum(TPP+FNP)} \qquad (50) \\
F1 = \frac{2 \times Precision \times Recall}{Precision + Recall} \\
1 - specificity = \frac{\sum FPP}{\sum(FPP+TNP)}
\end{gathered}$$

However, the relationship between the system's performance and the above mentioned metrics is proportional.

However, there is another evaluation metric exists which is used to measure the ranking correctness of the recommended items by the proposed approach and it is known as normalized discounted cumulative gain (nDCG). The mathematical formation of nDCG is as follows:

$$nDCG = \frac{\sum_{q=1}^{p} \frac{rel_q}{log_2(q+1)}}{\sum_{q=1}^{P} \frac{2^{rel_q}-1}{log_2(q+1)}} \qquad (51)$$

Here, p denotes an item that exits in the recommended items list. rel_q is the relevancy of an item i at the position q of the ranked list of recommendation. However, P indicates the list of relevant items of the ranked recommended items.

5. Discussion

This section represents the comparative analysis of twenty-four different trust metrics where the metrics are categorized according to the type of trust definition of TBRS. In the following portion, Table 4, Table 5 and Table 6 demonstrate the comparative classification of the trust metrics from the perspective of methodology, trust properties, trust measurement, evaluation metrics of TBRS.

Table 4. A comparative analysis of different explicit trust metrics (ETM)

		Trust Properties				Trust Measurement			
		Asymmetry	Transitivity	Dynamicity	Context Dependence	Trust Calculation (Direct Trust)	Trust Propagation (Inferred Trust)		
ETM1 (a) [65]	Memory-based	Yes	Yes	No	No	Yes	No	MAE & RC	FilmTrust, Flixster & Epinions
ETM1 (b) [33]	Memory & Model-based	Yes	Yes	No	No	Yes	No	MAE, RC & F1	FilmTrust, Flixster, ML-1M & BookCrossing
ETM2 [60]	Memory & Model-based	Yes	Yes	No	No	Yes	Yes	MAE, RMSE & RC	FilmTrust, Flixster & Epinions
ETM3 [66]	Memory & Model-based	Yes	Yes	Yes	No	Yes	Yes	RMSE	Epinions
ETM4 [67]	Memory-based	Yes	Yes	No	No	Yes	Yes	MAE	FilmTrust
ETM5 [62]	Model-based	Yes	Yes	No	No	Yes	Yes	nDCG, Precision & Recall	Epinions

5.1. Comparison of trust metrics: ETBRS

In Table 4, most of the trust metrics (**ETM1 (b), ETM2 & ETM3**) applied both memory and model based methodology to achieve better performance from the system.

However, all the trust metrics (**ETM1 to ETM5**) fulfil the asymmetry and transitivity property of the trust. Whereas, only **ETM3** metric supports the criteria of dynamicity property of trust by updating the trust value according to the users' interactions. Furthermore, none of the explicit trust metrics has taken the context dependence property into account. In conclusion, all the mentioned trust metrics are partially carry the trust characteristic as per the prospective of trust property.

Further, Table 4 shows that every trust metric defines the direct trust relation between users and maximum metrics, except **ETM1 (a) & (b)**, also defines the inferred trust through trust propagation method.

Furthermore, maximum trust metrics (**ETM1 (a) & (b), ETM2, ETM4**) have used the popular evaluation metrics, that is the MAE and the second most applied evaluation metric is rating coverage (RC).

And, Epinions is the most applied dataset according to Table 4 for its sufficient representation of explicit trust data.

5.2. Comparison of trust metrics: ITBRS

Every trust metrics of Table 5 used a memory-based approach to generate implicit trust relation between users in the RS except **ITM6**. **ITM6** also applied a memory-based approach with the model-based to achieve the maximum property of the trust.

Further, all trust metrics (**ITM1-ITM13**) of Table 5 are transitive. However, similarity measure based trust metrics (**ITM1, ITM5, ITM6, ITM9 & ITM13**) where users' uniformity is deduced by PCC, need to exceed a threshold to qualify the criteria of transitivity. And, the threshold value is 0.707. On the other side, **ITM1-ITM5 & ITM7** consider the implicit trust as symmetric whereas the rest of the trust metrics support the asymmetric criteria of trust. However, more than 80% trust metrics are not dynamic except **ITM6 & ITM8** and none of the metrics qualify the criteria of context dependence. So according to the trust properties, it can be claimed that the trust metrics, which are listed in the Table 5, do not fully contain every characteristic of trust.

However, in terms of trust measurement, every implicit trust metric calculates trust to form direct trust between users whereas almost 50% trust metrics of Table 5 are not consider inferred trust between users.

Furthermore, 10 metrics out of 13 have used mean absolute error (MAE) to validate the performance and the second most applied evaluation metric is coverage (UC and/or RC).

And, according to Table 5, maximum implicit trust metrics have applied different popular MovieLens (ML) datasets such as ML-100k, ML-1M, and ML-20M for verification. However, other known datasets like Epinions, Yahoo, FilmTrust are also used to measuring the benefit of proposed trust metrics.

5.3. Comparison of trust metrics: HTBRS

Table 6 demonstrates a comparative analysis of five different hybrid trust metrics where **HTM4** only implemented by memory-based method and **HTM5** used both memory and model-based method. And, the rest of the metrics applied model-based method.

However, every trust metrics are asymmetric and transitive by nature. And, none of the trust metrics has taken the dynamic and context dependence criteria of trust property into account.

Further, all the hybrid trust metrics determine the direct trust among the users, and only **HTM4** metric measures the inferred trust between users.

As like explicit and implicit trust metric, maximum trust metrics of Table 6 applied the MAE and RMSE as the assessment metric to verify the performance improvement that the authors' claimed.

In Table 6, Epinions is the most used dataset for the experiment. And, FilmTrust is the second highest used dataset.

6. Conclusion

This paper represents a systematic comprehensive review of different known and upgraded approaches of the trust-based recommender system. However, it also surveyed the task of recommendation and the definition of trust from different aspects with the computational properties of trust. Afterward, different trust metrics are examined by categorizing them into explicit, implicit, and hybrid TBRS. Total twenty-four trust metrics are reviewed and compared according to the methodology, trust properties & measurement, evaluation metrics, and datasets.

From the Table 4, 5 and 6, it can be conclude that all trust metrics are partially carry the trust characteristic according to trust properties. Only three trust metrics out of twenty-four have qualified the dynamicity criteria of trust whereas none of the trust metrics has taken the context dependence criteria into account. Moreover, only 50% of metrics have applied trust propagation to deduce inferred trust between users.

After analyzing all the metrics, the following points are advisable to take consideration.

- To qualify the dynamicity criteria of trust, the rating time should be considered along with the item rating information at the trust metrics formation.
- To carry the context dependence criteria, some auxiliary information such as contextual and behavioral information of users and items should be incorporated in the trust metrics.
- To resolve the data sparsity and cold-start issues efficiently, the trust propagation technique should be implemented in all trust metrics.

However, developing a new trust metrics by incorporating user-item interaction time and demographic information of the users is considered as the next direction of the work.

References

1. Gantz, J.; Reinsel, D. The digital universe in 2020: Big data, bigger digital shadows, and biggest growth in the far east. *IDC iView: IDC Analyze the future* **2012**, *2007*, 1–16.
2. Wang, H.; Wang, N.; Yeung, D.Y. Collaborative deep learning for recommender systems. Proceedings of the 21th ACM SIGKDD international conference on knowledge discovery and data mining, 2015, pp. 1235–1244.
3. Goldberg, D.; Nichols, D.; Oki, B.M.; Terry, D. Using collaborative filtering to weave an information tapestry. *Communications of the ACM* **1992**, *35*, 61–70.
4. Bobadilla, J.; Ortega, F.; Hernando, A.; Gutiérrez, A. Recommender systems survey. *Knowledge-based systems* **2013**, *46*, 109–132.
5. Smith, B.; Linden, G. Two Decades of Recommender Systems at Amazon.com. *IEEE Internet Computing* **2017**, *21*, 12–18.
6. Gomez-Uribe, C.A.; Hunt, N. The netflix recommender system: Algorithms, business value, and innovation. *ACM Transactions on Management Information Systems (TMIS)* **2015**, *6*, 1–19.
7. Logesh, R.; Subramaniyaswamy, V. Exploring hybrid recommender systems for personalized travel applications. In *Cognitive informatics and soft computing*; Springer, 2019; pp. 535–544.
8. George, G.; Lal, A.M. Review of ontology-based recommender systems in e-learning. *Computers & Education* **2019**, *142*, 103642.
9. Ayachi, R.; Boukhris, I.; Mellouli, S.; Amor, N.B.; Elouedi, Z. Proactive and reactive e-government services recommendation. *Universal Access in the Information Society* **2016**, *15*, 681–697.
10. Lu, J.; Wu, D.; Mao, M.; Wang, W.; Zhang, G. Recommender system application developments: a survey. *Decision Support Systems* **2015**, *74*, 12–32.
11. Shambour, Q.; Lu, J. An effective recommender system by unifying user and item trust information for B2B applications. *Journal of Computer and System Sciences* **2015**, *81*, 1110–1126.
12. Zahir, A.; Yuan, Y.; Moniz, K. AgreeRelTrust—A Simple Implicit Trust Inference Model for Memory-Based Collaborative Filtering Recommendation Systems. *Electronics* **2019**, *8*, 427.
13. Roy, F.; Sarwar, S.M.; Hasan, M. User similarity computation for collaborative filtering using dynamic implicit trust. International Conference on Analysis of Images, Social Networks and Texts. Springer, 2015, pp. 224–235.
14. Son, J.; Kim, S.B. Content-based filtering for recommendation systems using multiattribute networks. *Expert Systems with Applications* **2017**, *89*, 404–412.
15. McNee, S.M.; Riedl, J.; Konstan, J.A. Being accurate is not enough: how accuracy metrics have hurt recommender systems. CHI'06 extended abstracts on Human factors in computing systems, 2006, pp. 1097–1101.
16. Shokeen, J.; Rana, C. A study on features of social recommender systems. *Artificial Intelligence Review* **2020**, *53*, 965–988.
17. Barzegar Nozari, R.; Koohi, H.; Mahmodi, E. A novel trust computation method based on user ratings to improve the recommendation. *International Journal of Engineering* **2020**, *33*, 377–386.
18. Gohari, F.S.; Aliee, F.S.; Haghighi, H. A new confidence-based recommendation approach: Combining trust and certainty. *Information Sciences* **2018**, *422*, 21–50.
19. Wang, X.; Liu, Y.; Lu, J.; Xiong, F.; Zhang, G. TruGRC: trust-aware group recommendation with virtual coordinators. *Future Generation Computer Systems* **2019**, *94*, 224–236.
20. Guo, G.; Zhang, J.; Yorke-Smith, N. Trustsvd: Collaborative filtering with both the explicit and implicit influence of user trust and of item ratings. Twenty-Ninth AAAI Conference on Artificial Intelligence, 2015, pp. 123–129.
21. Pan, Y.; He, F.; Yu, H.; Li, H. Learning adaptive trust strength with user roles of truster and trustee for trust-aware recommender systems. *Applied Intelligence* **2020**, *50*, 314–327.
22. Miyahara, K.; Pazzani, M.J. Collaborative filtering with the simple Bayesian classifier. Pacific Rim International conference on artificial intelligence. Springer, 2000, pp. 679–689.

23. Koohi, H.; Kiani, K. User based Collaborative Filtering using fuzzy C-means. *Measurement* **2016**, *91*, 134–139.
24. Ar, Y.; Bostanci, E. A genetic algorithm solution to the collaborative filtering problem. *Expert Systems with Applications* **2016**, *61*, 122–128.
25. Lv, G.; Hu, C.; Chen, S. Research on recommender system based on ontology and genetic algorithm. *Neurocomputing* **2016**, *187*, 92–97.
26. Kardan, A.A.; Ebrahimi, M. A novel approach to hybrid recommendation systems based on association rules mining for content recommendation in asynchronous discussion groups. *Information Sciences* **2013**, *219*, 93–110.
27. Isinkaye, F.; Folajimi, Y.; Ojokoh, B. Recommendation systems: Principles, methods and evaluation. *Egyptian Informatics Journal* **2015**, *16*, 261–273.
28. Hasan, M.; Roy, F. An Item–Item Collaborative Filtering Recommender System Using Trust and Genre to Address the Cold-Start Problem. *Big Data and Cognitive Computing* **2019**, *3*, 39.
29. Nobahari, V.; Jalali, M.; Mahdavi, S.J.S. ISoTrustSeq: a social recommender system based on implicit interest, trust and sequential behaviors of users using matrix factorization. *Journal of Intelligent Information Systems* **2019**, *52*, 239–268.
30. Guo, G.; Zhang, J.; Thalmann, D. Merging trust in collaborative filtering to alleviate data sparsity and cold start. *Knowledge-Based Systems* **2014**, *57*, 57–68.
31. Shambour, Q.; Lu, J. A trust-semantic fusion-based recommendation approach for e-business applications. *Decision Support Systems* **2012**, *54*, 768–780.
32. Bobadilla, J.; Ortega, F.; Hernando, A.; Bernal, J. A collaborative filtering approach to mitigate the new user cold start problem. *Knowledge-based systems* **2012**, *26*, 225–238.
33. Guo, G. Integrating trust and similarity to ameliorate the data sparsity and cold start for recommender systems. Proceedings of the 7th ACM conference on Recommender systems, 2013, pp. 451–454.
34. Guo, G.; Zhang, J.; Thalmann, D.; Basu, A.; Yorke-Smith, N. From ratings to trust: an empirical study of implicit trust in recommender systems. Proceedings of the 29th annual acm symposium on applied computing, 2014, pp. 248–253.
35. Parvin, H.; Moradi, P.; Esmaeili, S. TCFACO: Trust-aware collaborative filtering method based on ant colony optimization. *Expert Systems with Applications* **2019**, *118*, 152–168.
36. Son, J.; Choi, W.; Choi, S.M. Trust information network in social Internet of things using trust-aware recommender systems. *International Journal of Distributed Sensor Networks* **2020**, *16*, 1550147720908773.
37. Zhang, Z.; Liu, Y.; Jin, Z.; Zhang, R. A dynamic trust based two-layer neighbor selection scheme towards online recommender systems. *Neurocomputing* **2018**, *285*, 94–103.
38. Guo, G.; Zhang, J.; Zhu, F.; Wang, X. Factored similarity models with social trust for top-N item recommendation. *Knowledge-Based Systems* **2017**, *122*, 17–25.
39. Gupta, S.; Nagpal, S. Trust aware recommender systems: a survey on implicit trust generation techniques. *International Journal of Computer Science and Information Technologies* **2015**, *6*, 3594–3599.
40. Yadav, A.; Chakraverty, S.; Sibal, R. A survey of implicit trust on social networks. 2015 International Conference on Green Computing and Internet of Things (ICGCIoT). IEEE, 2015, pp. 1511–1515.
41. Selmi, A.; Brahmi, Z.; Gammoudi, M.M. Trust-based recommender systems: an overview. Proceedings of 27th International Business Information Management Association (IBIMA) Conference, Milan, Italy, 2016.
42. Jallouli, M.; Lajmi, S.; Amous, I. Similarity and trust metrics used in Recommender Systems: A survey. International Conference on Intelligent Systems Design and Applications. Springer, 2016, pp. 1041–1050.
43. Moghaddam, M.G.; Mustapha, N.; Elahian, A. A Review on Similarity Measurement Methods in Trust-based Recommender Systems. *International Journal of Information Science and Management (IJISM)* **2014**, pp. 13–22.
44. Golbeck, J.A. Computing and applying trust in web-based social networks (Doctoral dissertation). PhD thesis, 2005.
45. Golbeck, J. Tutorial on using social trust for recommender systems. Proceedings of the third ACM conference on Recommender systems, 2009, pp. 425–426.
46. Castelfranchi, C.; Falcone, R. *Trust theory: A socio-cognitive and computational model*; Vol. 18, John Wiley & Sons, 2010.

47. Gohari, F.S.; Haghighi, H.; Aliee, F.S. A semantic-enhanced trust based recommender system using ant colony optimization. *Applied Intelligence* **2017**, *46*, 328–364.
48. Papagelis, M.; Plexousakis, D.; Kutsuras, T. Alleviating the sparsity problem of collaborative filtering using trust inferences. International conference on trust management. Springer, 2005, pp. 224–239.
49. Gao, P.; Miao, H.; Baras, J.S.; Golbeck, J. Star: Semiring trust inference for trust-aware social recommenders. Proceedings of the 10th ACM conference on Recommender systems, 2016, pp. 301–308.
50. Resnick, P.; Iacovou, N.; Suchak, M.; Bergstrom, P.; Riedl, J. GroupLens: an open architecture for collaborative filtering of netnews. Proceedings of the 1994 ACM conference on Computer supported cooperative work, 1994, pp. 175–186.
51. O'Donovan, J.; Smyth, B. Trust in recommender systems. Proceedings of the 10th international conference on Intelligent user interfaces, 2005, pp. 167–174.
52. Li, Y.M.; Kao, C.P. TREPPS: A trust-based recommender system for peer production services. *Expert systems with applications* **2009**, *36*, 3263–3277.
53. Yuan, W.; Guan, D.; Lee, Y.K.; Lee, S.; Hur, S.J. Improved trust-aware recommender system using small-worldness of trust networks. *Knowledge-Based Systems* **2010**, *23*, 232–238.
54. Massa, P.; Avesani, P. Trust-aware collaborative filtering for recommender systems. OTM Confederated International Conferences" On the Move to Meaningful Internet Systems". Springer, 2004, pp. 492–508.
55. Park, M.H.; Hong, J.H.; Cho, S.B. Location-based recommendation system using bayesian user's preference model in mobile devices. International conference on ubiquitous intelligence and computing. Springer, 2007, pp. 1130–1139.
56. Ma, H.; King, I.; Lyu, M.R. Learning to recommend with explicit and implicit social relations. *ACM Transactions on Intelligent Systems and Technology (TIST)* **2011**, *2*, 1–19.
57. Kitisin, S.; Neuman, C. Reputation-based trust-aware recommender system. 2006 Securecomm and Workshops. IEEE, 2006, pp. 1–7.
58. Cho, J.; Kwon, K.; Park, Y. Q-rater: A collaborative reputation system based on source credibility theory. *Expert Systems with Applications* **2009**, *36*, 3751–3760.
59. Golbeck, J. Generating predictive movie recommendations from trust in social networks. International Conference on Trust Management. Springer, 2006, pp. 93–104.
60. Guo, G.; Zhang, J.; Yorke-Smith, N. Leveraging multiviews of trust and similarity to enhance clustering-based recommender systems. *Knowledge-Based Systems* **2015**, *74*, 14–27.
61. Yao, W.; He, J.; Huang, G.; Zhang, Y. Modeling dual role preferences for trust-aware recommendation. Proceedings of the 37th international ACM SIGIR conference on Research & development in information retrieval, 2014, pp. 975–978.
62. Duricic, T.; Lacic, E.; Kowald, D.; Lex, E. Trust-based collaborative filtering: Tackling the cold start problem using regular equivalence. Proceedings of the 12th ACM Conference on Recommender Systems, 2018, pp. 446–450.
63. Ayub, M.; Ghazanfar, M.A.; Mehmood, Z.; Alyoubi, K.H.; Alfakeeh, A.S. Unifying user similarity and social trust to generate powerful recommendations for smart cities using collaborating filtering-based recommender systems. *Soft Computing* **2019**, pp. 1–24.
64. Davoudi, A.; Chatterjee, M. Social trust model for rating prediction in recommender systems: Effects of similarity, centrality, and social ties. *Online Social Networks and Media* **2018**, *7*, 1–11.
65. Guo, G.; Zhang, J.; Thalmann, D. A simple but effective method to incorporate trusted neighbors in recommender systems. International conference on user modeling, adaptation, and personalization. Springer, 2012, pp. 114–125.
66. Tian, H.; Liang, P. Improved recommendations based on trust relationships in social networks. *Future Internet* **2017**, *9*, 9.
67. He, X.; Liu, B.; Chen, K. ITrace: an implicit trust inference method for trust-aware collaborative filtering. AIP conference proceedings. AIP Publishing LLC, 2018, Vol. 1955, p. 040102.
68. Hwang, C.S.; Chen, Y.P. Using trust in collaborative filtering recommendation. International conference on industrial, engineering and other applications of applied intelligent systems. Springer, 2007, pp. 1052–1060.
69. Lathia, N.; Hailes, S.; Capra, L. Trust-based collaborative filtering. IFIP international conference on trust management. Springer, 2008, pp. 119–134.

70. Yuan, W.; Shu, L.; Chao, H.C.; Guan, D.; Lee, Y.K.; Lee, S. ITARS: trust-aware recommender system using implicit trust networks. *IET communications* **2010**, *4*, 1709–1721.
71. Castro Sotos, A.E.; Vanhoof, S.; Van Den Noortgate, W.; Onghena, P. THE TRANSITIVITY MISCONCEPTION OF PEARSON'S CORRELATION COEFFICIENT. *Statistics Education Research Journal* **2009**, *8*.
72. Bedi, P.; Sharma, R. Trust based recommender system using ant colony for trust computation. *Expert Systems with Applications* **2012**, *39*, 1183–1190.
73. Azadjalal, M.M.; Moradi, P.; Abdollahpouri, A.; Jalili, M. A trust-aware recommendation method based on Pareto dominance and confidence concepts. *Knowledge-Based Systems* **2017**, *116*, 130–143.
74. Choudhary, N.; Bharadwaj, K. Leveraging trust behaviour of users for group recommender systems in social networks. In *Integrated intelligent computing, communication and security*; Springer, 2019; pp. 41–47.
75. Zheng, X.L.; Chen, C.C.; Hung, J.L.; He, W.; Hong, F.X.; Lin, Z. A hybrid trust-based recommender system for online communities of practice. *IEEE Transactions on Learning Technologies* **2015**, *8*, 345–356.
76. Chen, C.; Zheng, X.; Zhu, M.; Xiao, L. Recommender system with composite social trust networks. *International Journal of Web Services Research (IJWSR)* **2016**, *13*, 56–73.
77. Wang, M.; Wu, Z.; Sun, X.; Feng, G.; Zhang, B. Trust-aware collaborative filtering with a denoising autoencoder. *Neural Processing Letters* **2019**, *49*, 835–849.
78. Herlocker, J.L.; Konstan, J.A.; Terveen, L.G.; Riedl, J.T. Evaluating collaborative filtering recommender systems. *ACM Transactions on Information Systems (TOIS)* **2004**, *22*, 5–53.

Table 5. A comparative analysis of different implicit trust metrics (ITM)

		Trust Properties				Trust Measurement			
		Asymmetry	Transitivity	Dynamicity	Context Dependence	Trust Calculation (Direct Trust)	Trust Propagation (Inferred Trust)		
ITM1 [48]	Memory-based	No	Yes	No	No	Yes	Yes (if the direct trust is positive)	MAE & ROC	movie recommendation data (MRS)
ITM2 [51]	Memory-based	No	Yes	No	No	Yes	No	MAE	ML
ITM3 [68]	Memory-based	No	Yes	No	No	Yes	Yes	MAE & Coverage	ML-100k
ITM4 [69]	Memory-based	No	Yes	No	No	Yes	No	MAE & Coverage	ML
ITM5 [70]	Memory-based	No	Yes	No	No	Yes	Yes	MAE & UC	Epinions
ITM6 [72]	Memory & Model-based	Yes	Yes	Yes	No	Yes	Yes	Precision, Recall & F1	ML-100k & Jester
ITM7 [31]	Memory-based	No	Yes	No	No	Yes	Yes	MAE & Coverage	ML-100k & Yahoo
ITM8 [13]	Memory-based	Yes	Yes	Yes	No	Yes	No	MAE	ML-1M
ITM9 [73]	Memory-based	Yes	Yes	No	No	Yes	Yes	MAE, MAUE, UC & RC	Epinions & FilmTrust
ITM10 [74]	Memory-based	Yes	Yes	No	No	Yes	No	nDCG	ML-100k
ITM11 [12]	Memory-based	Yes	Yes	No	No	Yes	No	MAE & RMSE	ML-20M, ML-100k & Jester
ITM12 [36]	Memory-based	Yes	Yes	No	No	Yes	Yes	MAE, RMSE, UC & RC	FilmTrust
ITM13 [17]	Memory-based	Yes	Yes	No	No	Yes	No	Accuracy, Precision & Recall	ML-100k & ML-1M

Table 6. A comparative analysis of different hybrid trust metrics (HTM)

		Trust Properties				Trust Measurement			
		Asymmetry	Transitivity	Dynamicity	Context Dependence	Trust Calculation (Direct Trust)	Trust Propagation (Inferred Trust)		
HTM1 [75]	Model-based	Yes	Yes	No	No	Yes	No	Precision & Recall	Stack Overflow
HTM2 [76]	Model-based	Yes	Yes	No	No	Yes	No	MAE	Epinions
HTM3 [77]	Model-based	Yes	Yes	No	No	Yes	No	MAE & RMSE	FilmTrust, Epinions & Douban
HTM4 [63]	Memory-based	Yes	Yes	No	No	Yes	Yes	MAE, RMSE, RC, iMAE & F1	FilmTrust, CiaoDVD & Epinions
HTM5 [35]	Model & Memory-based	Yes	Yes	No	No	Yes	No	MAE, RMSE & RC	FilmTrust, Epinions & Ciao