© 2015 IJSRSET | Volume 1 | Issue 6 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

A Survey on Trust regarding Reputation System

Anjana Patel, Mital Panchal
Department of Information Technology, L. D. Engineering College Ahmedabad, Gujarat, India

ABSTRACT

In digital world there are various websites presently has the situations where people transact with unknown agents and take decision for these agents for by considering the reputation score. Central idea of this paper is to compare online Trust and reputation models that are particularly suitable for the peer to peer network but uses different approaches for calculating for getting towards the trust of an entity. This paper describes how the trust for the entity is works of, their properties and various parameters advantages disadvantages. Finally, it concludes by comparison of all these protocols

Keywords: Reputation, Trust, Peer to Peer network, Database Security, Homomorphic system.

I. INTRODUCTION

The concept of trust in many different domains, such as sociology, philosophy, social psychology, economics, and computer science.

From Gambetta's definition, we infer that trust has the following characteristics:
We find it useful to use the following trust definition by Gambetta: “trust (or, symmetrically, distrust) is a particular level of the subjective probability with which an agent will perform a particular action, both before we can monitor such action (or independently of his capacity of ever to be able to monitor it) and in a context in which it affects our own action” [1]

Stature

An entity’s capability and reliability based on recommendation from other peers. It is perception that an agent creates Through past actions about its intentions and norms.[1] Reputation is a social quantity calculated based on actions by a given agent a_i and observations made by Others Reputation can be centralized, computed by a trusted third party, like a Better Business Bureau; or it can be decentralized, computed independently by each peer after asking other peers for recommendation.

II. TERMIOGY RELATED TO TRUST

A. Characteristics of trust

Binary-Relational and Directional : Trust is a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action . From this excerpt, it is evident that trust is a relationship between two entities. Moreover, it is also clear that trust is directional. The trust entity is an agent who has trust in a second entity which may be another agent or a group of agents”.

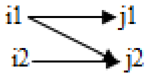
Contextual Is regarding the situation dependent on any situation subjective probability with which an agent assesses that another agent or group of agents will perform a particular action.

Peer trust is exacting altitude of the individual in a context likelihood by having it an entity evaluate various entities will act upon a exacting way in that context, in cooperation previous to keep an eye on the way in a perspective relates to one’s action. [2]

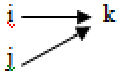
B. Definitions and Terminologies Related to Reputation:

Considering the trust in an unknown entity by the trust recommendation and propagation Guha et al. [3] identified propagations: as following:

Direct Propagation : As the names suggests the direct trust. Consider I trusts j, j trusts k, then we can conclude that i trusts k.
i=j, j=k,i=k
Co-Citation : i_1 trusts j_1 and j_2 , andi_2 trustsj_2. Under co-citation, it is concluded thati_2 also trustsj_1 .



then we can infer i2 → j1
Transpose Trust**.** Imples that I trusts j then there j can develop some level of trust towards i. We can infer i trusts j, then transpose trust implies that j should also trust i.
i → j then j → i
Trust Coupling. i and j both trust k, then trust coupling leads us to infer that i and j should trust each other since they both trust k.



then i → j
Let q be an agent be a querying agent to receive the trust recommendation from an agent as lat where a is the source agent and t a target agent about whom the trust is being transposition. Considering after this recommendation consequence of the trust, agent q
P (perform (q, t, ψ) = true) = lat .
Then this act of q establishing trust in t as a consequence of a trust recommendation from **a** is said to be a simple trust propagation from **a** to q about t.
The newly established trust value P (perform (q, t, ψ) = true) is said to be simple propagated trust from **a** to q about t.

III. SOME REPUTATIO PROTOCOL

A. Optimism and pessimism in trust [4]

The paper has the discussion regarding 'dispositions' of trusting behaviour, which here is base on three categories "Optimism, Pessimism and Realism" and includes the memory in picture for trusting agents, also briefly suggest some ways in which the size of memory can affect the decision agents, with different dispositions

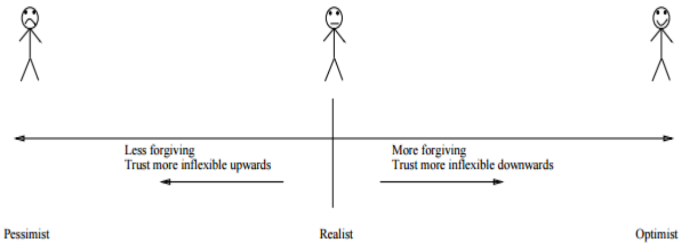

Less forgiving
Trust more inflexible upwards
More forgiving
Trust more inflexible downwards
Pessimist
Realist
Optimist

Figure 1: Spectrum of Realism

Consider agent x and y, x's trust in y Tx(y,α) where α is situation

Situational Trust:

$$Tx(y,a)=Tdx(y)Ux(\alpha)Ix(\alpha) \qquad (1)$$

Tdx(y)= an estimate x has of how much he can trust y.
Ux(α)=utility(cost/benefit) of situation for
x ε [1; 1] — we normalise utility to be in this range.
Ix(α)= importance of a situation

Realism As the name suggests realism is related to real world and real things and also includes two methods of obtain a realist estimate: the mean and the mode[5]. To find a mean value for use as the estimate,. The equation is:

$$Tx(y,a)=1/|A| \sum \text{for } a\varepsilon A \; Tx(y,a) \qquad (2)$$

A=. set of situation to decide which situations the agent can remember.
Optimistic Approach:
Tx(y,a)=Tdx(y)Ux(α)Ix(α)

$$Tdx(y)= max_{a \varepsilon a} Tx(y,a) \qquad (3)$$

for example $\{0.54_a,0:21_b,0:25_c,0:34_d;0.98_e\}$,
subscripts are simply identifiers for situations, then
If situations b and c were similar to situation that x is presently in. The resultant Tdx(y) is thus 0:25.

As the approach is optimist

Pessimistic Approach:

$$Tdx(y) = min_{a \varepsilon a} Tx(y,a) \qquad (4)$$

for $\{0.54_a,0:21_b,0:25_c,0:34_d;0.98_e\}$, The resultant Tdx(y) is thus 0:21.

B. trust for Detecting Deceitful Agents [6]

This models contains trust to be presented as the Boolean value which is either good or bad, a concept of Prisoner’s dilemma is added which is a game dealing with the fact why two completely "rational" individuals might not cooperate, even if they do so it will be win win situation for both the agents. In game every agent without communicating with each other both gets sentenced to a year in prison police offers both of them bargain. They get the opportunity to betray or be loyal to other agent committed the crime, or to cooperate with the other by remaining silent.

After receiving the result of the game played by agent and also included the result of game played by subsets of all agents in the community neighboring agents. Outcome of an interaction is reputation about honesty of the partner like what one claimed while selecting the partner.

This model is dependent on probability theory. The equation to calculate the trust for the reliability of agent Q to agent A is, the probability that the agent A be honest in the next interaction

$$T(A, Q) = e\ n \qquad (5)$$

n =the number of situations observed
e =the number of times the agent A was honest.

The results are from direct interaction, an agent can also check other agents trust even if they have interacted before.

“TrustNet” data structure is used by every agent which is a directed graph where nodes are the witnesses and edges has information on the observations that the parent node agent told the owner of the net (the root node of the TrustNet) about the child node agents.

Each agent is checked for honesty by adding up the noise value in also with the possibility the source of information is biased in the data. The answer of witness is the set of observed experiences. A witness will not say that other agent is not honest. The model has assumption that witnesses never lie but that can any hide positive to make other agents appear less trustworthy. Now hiding information is solved by stochastic approach where:

P= probability of agent decides to inform about a positive fact of another agent

(1 − p)= probability of hiding information

Then Probability theory is used to estimate the hidden amount of positive information. This process can be applied recursively from the target agent through all its ancestors up to the root node of the Trust Net. The information from the witnesses comprises the list of observations it can be collated to eliminate the “correlated evidence” problem. The proposed solution in this case is based on the assumption that the in relation of overlapping of the data in reported and non reported (hidden) information is constant. No information is given about how to combine direct experiences with information coming from witnesses. The trust value is a subjective property assigned particularly by each individual and it does not depend on the context

C. How Agents Make Friends [7]

This paper consists of two one-on-one trust acquisition mechanisms are proposed.

First model is on Peer observation The Bayesian network is proposed is used for acquiring trust by Bayesian learning. In the simplest case of a known structure and a fully observable Bayesian network, the learning task is reduced to statistical considerations.

Considering agents A and B,
D= delegation situation,
S= observed performance statistic trust Tobs as follows:

$$Tobs(A,B) = P(S|D) \qquad (6)$$

The second mechanism is based on interaction. Protocols of interaction is present, where the agent asks the other agent about things known to estimate the degree of trust and A simple way to calculate the interaction-based trust during the exploratory stage is using the formula

Tinter (A,B) = number of correct replies/total number of replies.

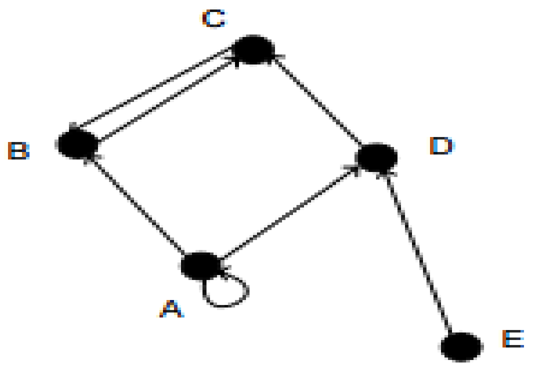


Figure 2: Directed graph for trustable agents

Every agent builds a labeled graph where nodes represent agents and where an (a,b) edge represents the trust value that a has on b. For missing edges trust value is unknown. So the possibility of having cycle in the graph decreases the trust value and different paths that give contradictory values.

A single value for trust the model is not used rather a trust interval determined by the minimum and maximum value of all paths without cycles that connect two agents. The authors claim that the calculation of this trust interval is equivalent to the problem of routing in a communication network and, therefore, known distributed algorithms used to solve that problem can be successfully applied to this situation.

Propose the use of colored edges, with a color per task or type of trust. Trust would only propagate through edges of the same color.

D. Afras[8]

Afras stands for “A Fuzzy Reputation Agent System”. A fuzzy definition for the stature is considered which shows the degree of satisfaction for the last interaction with other agent from the community the old reputation value and the new satisfaction value are added by weighted aggregation. The weights are calculated from a single value memory.

It is distributed approach, where each agent has its own opinion about the rest of the agents in the system. Each user can anytime act as seller, consumer or recommender. Reputation is then built as a result of all the actions hold, irrespective of the role that the agent is currently playing.

Memory allows the agent to give more importance to the latest interaction or to the old reputation value. As the previous reputation and the satisfaction of the last interaction and the previous remembrance value. If the satisfaction of the last interaction and the reputation assigned to the partner are similar, the relevance of past experiences is increased. If the satisfaction of the last interaction and the reputation value are different, then it is the relevance of the last experience what is increased. Fuzzy set represents a high degree of uncertainty and a narrow a reliable value. Recommendation by other agents is added directly by the direct experiences. Both old reputation value and new opinion are weighted and are dependent on the reputation that the recommender has.

Recommendations coming from a recommender with a high reputation have the same degree of reliability as a direct experience. The agent compares the recommendation with the real behaviour of the recommended agent after the interaction and increases or decreases the reputation of the recommender accordingly.

E. Bayesian network model [9]

This model consists a trust model based on Bayesian network for reputation system which works on the principle of recommendations in peer-to-peer networks. But the trust is the factor which depends on the multiple parameter peers need to various different aspects of the trust are maintained by each peer on each peers’ capability. As per situation, they may need to consider trust in a specific aspect of another peer’s capability or in multiple aspects. Bayesian networks provide a flexible method to present differentiated trust and combine different aspects of trust.

Trust adds to the performance in terms of percentage of successful interactions. The peer to peer network uses statistic methods to represent probability relationships between different elements [10].

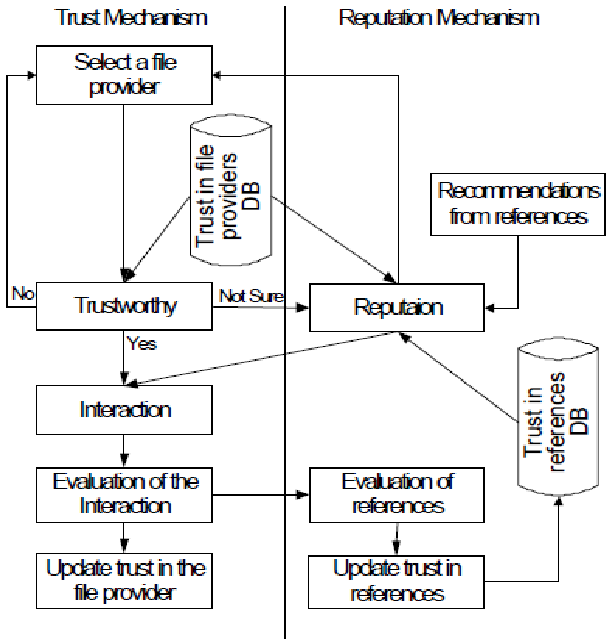


Figure 3: Functionality of the trust and reputation mechanism on board of the peer.

The trust of an agent for the peer providing file is done by developing a naive Bayesian network for each file provider that it has direct interaction with. Each Bayesian network in the Figure has a root node T that represents the peer's trust in the file provider's capability in providing files. The percentage of interactions that are satisfying. The leaf nodes under the root node represent the file provider's capability in different aspects. FT is set of file types. Suppose it includes example "Music", "Movie", "Document", "Image" and "Software". DS is set of download speeds. It has three values, "Fast", "Medium" and "Slow", each of which covers a range of download speeds. FQisset of file qualities can be categorized as, "High", "Medium" and "Low".

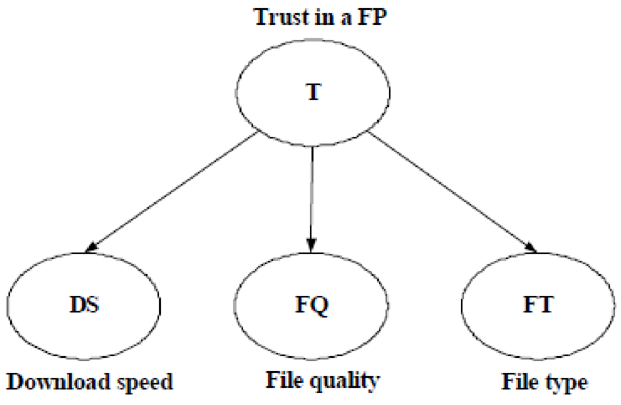


Figure 4: Bayesian network model

Evaluating interactions and updating trust in file providers: After every interaction, peers evaluate it they may different views to judge an interaction. They can even have different evaluations of the same interaction. The overall evaluation of an interaction is a combination of evaluations of every parameter related to the interaction, such as download speeds, file quality.

The result of the overall evaluation, "the interaction is satisfying" or "not satisfying", is used to update the peer 'trust in the file provider involved. The update is implemented by adding the new experience into the peer's corresponding Bayesian network.

F. A Reputation-Based Trust Model for Peer-to-Peer eCommerce Communities [11]

STEP1:

Parameters for trust here are formalized and general trust metric both adds upon on a coherent manner.

U= peer

I(u)= Total number of transactions performed by peer.

P(u,i)= peer participation in ith transaction

S(U,i)= normalized amount of satisfaction peer u receives from

Cr(P(u,i))= creditability of feedback submitted by the peer.

TF(u,i)= adaptive transaction context factor for peer u.

CF(u)= adaptive community context factor for peer u.

$$T(u) = \alpha * \frac{\sum_{i=1}^{I(u)} S(u,i) * CR(p(u,i)) * TF(u,i)}{I(u)} + \beta * \mathrm{CF}(u) \qquad (7)$$

Metric has two parts. The first part contains average amount of credible satisfaction a peer receives for each transaction. And considers that transaction context factor for capturing the characteristics of transaction. Its likelihood of a successful transaction in the future. A confidence value can be computed and associated with the trust metric that may reflect the number of transactions, the standard deviation of the ratings depending on different communities.

Whereas the next part of the metric adjusts the first part by an increase or decrease of the trust value based on other peers in the community characteristics and situations. Alpha and beta are the normalized weight factors.

STEP2:

Basic form is obtained from the general metric by turning off the transaction context factor =1 and community context factor alpha=1 beta=0.which makes the equation to be:

$$T(u) = \frac{\sum_{i=1}^{I(u)} S(u,i) * CR(p(u,i)) * TF(u,i)}{I(u)} \quad (8)$$

STEP3:

Incorporating Transaction Contexts:

As the above both the steps include the matrix formation but that matrix needed to be adapted for the business point of view for that the general trust metric is changed by the weight the feedback for that transaction. Transaction context need to be on as the transaction is included a must for the business needs and purpose and also the community context factor is kept off as it is not needed terms of dollar amount is added as D(u,i).

$$T(u) = \frac{\sum_{i=1}^{I(u)} S(u,i) * CR(p(u,i)) * D(u,i)}{I(u)} \quad (9)$$

And the similar adaption's can be done for the different contexts related to trust. for P2P electronic communities. Combining trust management with intrusion detection to address concerns of sudden and malicious attacks.

G. Zhou et. al. The PowerTrust System Concept [12]

The Power Trust system is inspired by the power-law Use Bayesian method to generate local trust scores where few power nodes are dynamically selected based on stature by using a distributed ranking mechanism is implemented by Distributed Hash Table (DHT) such as Chord [13] globally. Good stature for the power nodes is gathered by the running history of the system.

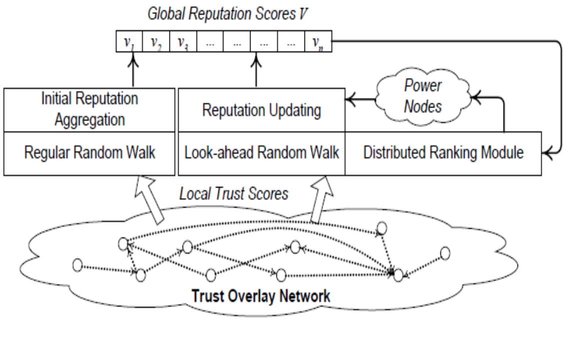


Figure 5 : the control flow pattern in local trust score collection and global stature aggregation

A trust overlay network abbreviated as TON is built for all peers a P2P system. All peers evaluate each other, whenever a transaction takes place between a peer pair.

All global scores form a stature vector, V = (v1, v2, v3, …..,v_n), which is the output of the Power Trust system. All global scores are the normalized.

The regular random walk module is initial stature aggregation. The look-ahead random walk is used to update the stature score, periodically works with a distributed ranking module to identify the power nodes.

Feedback frequency f_d is the number of nodes with feedback amount d.

The ranking index θ_d indicates the order of d in a decreasing list of feedback amounts.

Selection of top-m peers (Power nodes)

Global statures stored among score managers are input for each node i score manager j calculates, hash stature value H(v_i) using locality preserving hash and insert the (v_i, i, j) to the successor node of H(v_i) stored in the ascending order of their stature values in the DHT hash space due to the property of LPH.

Initialize node x = successor node of the maximum hash value.

Global Stature Aggregation

Local trust scores stored in the nodes are given as input to this step for each node i & node j,the out-degree neighbor of node i is feed with score message (r_{ij}, i) to the score manager of node j temporary variable pre=0 is initialized; the error threshold ε and global stature v_k of node k For all received score pair (r_{jk}, j), where j is an in-degree neighbor of node k Receive the global stature v_j from the score manger of node j

$v_k = v_k + v_j\ r_{jk}$

Compute $\delta = |\ v_k - \text{pre}|$ until $\delta <$ εoutput is Global stature for every node

Global Stature Updating Procedure:

The score managers collaborate with each other to find the power nodes by step 1.

If node x stores the triplet (i,v_i, j) and finds i as a power node, node x will notify to node j.

Local trust scores stored among nodes is the input to this step for each i & all node j Aggregate local trust scores from node j Send the score message (r_{ij}, i) to the score manager of node j

temporary variable pre=0; error threshold εglobal stature v_k of node k

Initialize pre= v_k; $v_k = 0$
For all received score pair (r_{jk}, j), where j is an in-degree neighbour of node k do

Receive node j global stature v_j from score manager of node j
For node k be a power node,
$v_k=(1-\alpha)\Sigma\ (v_j \times r_{jk}) +\alpha/m$
else $v_k=(1-\alpha)\Sigma\ (v_j \times r_{jk})$
$\delta = |\ v_k - \text{pre}|$, until $\delta < \varepsilon$

Global stature scores for all nodes for use by score managers collaboratively to find the m most reputable nodes using is the output here.

Zhou et al Gossiptrust for fast reputation aggregation
Gossiptrust deals with the fast aggregation of global stature scores. It deals with two steps within i.e. local score aggregation and global score dissemination are Performed.

Mathematically, for stature calculation we need to compute the weighted sum of all local scores s_{ij} score given by I for node j for each peer j= 1, 2, …,n , where the values of the feedback score normalized global scores and weights are applied.

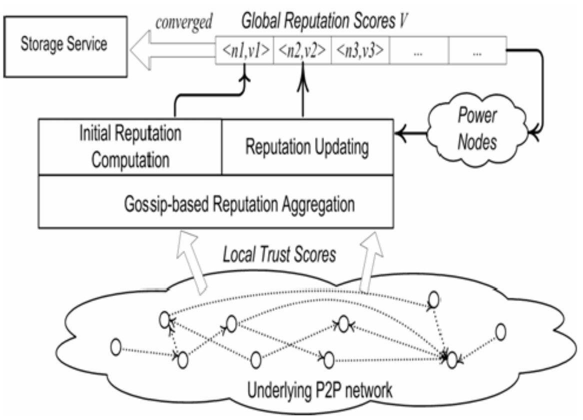


Figure 6: working of gossip group protocol [14]

Consider it for node N, here each node keeps a row vector of trust matrix S based on its outbound local trust scores.

At each node the global reputation vector V (t) is which has {node_id,score} pair.

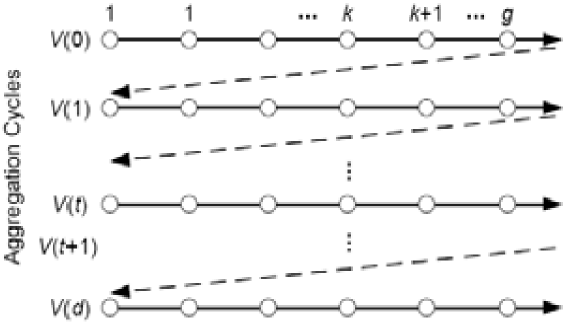


Figure 7 : Working of Gossip trust reputation aggregation cycle[14]

Vector initialization
Initially the global reputation vector is V(0)

Recursive matrix vector calculation
Then matrix vector is calculated by aggregation process recursively,
$V(t+1) = S^T \times V(t)$
T is the iterative cycle. S is global score and T is trust parameter

Exchange of global reputation:

Vectors are exchanged from every node to other, which are combined with current reputation vector, and the updated score is sent to a random node in the network.

Gossip aggregation of reputation:

local score s_{ij}, global score $v_i(t-1)$
for i = 1,2,…,n and gossip threshold ε
xi ← $s_{ij} \times v_i(t-1)$ weighted score x_i is initalized
if (i == j), set wi ← 1, else wi = 0 consensus factor wi
k ← 0 k is gossip step
u ← x_i/w_i is previous score {(x_r, w_r)} is gossip pair sent to i in previous step
$x_i \leftarrow \Sigma_r\ x_r$, $w_i \leftarrow \Sigma_r\ w_r$ Update the score and weight
updated score is sent to a random node in the network (½ x_i, ½ w_i) to node it and itself
k ← k+1 Next gossip step
until $|x_i/w_i - u| \le \varepsilon$
$v_j(t) \leftarrow x_i/w_i$

Storage of global reputation

For achieving the memory efficiency on each node, Bloom-filter scheme for storage and retrieval of ranked global scores is used . A Bloom filter is a space-efficient data structure for membership queries they store the global scores. Each Bloom filter requires m bits to hold multiple hashed encodings into the same class.

H. Hasan, et al decentralized privacy preserving reputation protocol [15]

Each source agent s relies on at most k agents to preserve its privacy. On its own knowledge of their trustworthiness in the context of preserving privacy and sends each of them an additive share of his private feedback value

Initiation & Select Trustworthy Agents: Is done by querying agent for computation of the reputation of a target agent .Source agent gets the feedback providers in a context.(advogato trust metric[16] is used here for this purpose). Each agent can selects up to k other agents with the probability that the selected agents will break agent's privacy is low.

Prepare Shares : At a time the source agent makes the k other feedback providing agents the number one decides is stated as K.Agent prepares k + 1 share for secret feedback the k shares are random numbers uniformly distributed over a large interval.but the last k+1 share (Fat-∑ individual feedback) mod M.M is publically known Fat be feedback of a source agent a about a target agent t.

Encrypt Shares: The list of all shares is implemented by agents own public key so that only agent can open it also each kth share is encrypted by public key of the feedback agent so that only one can have access to its own share by once private key.

Generate Zero-Knowledge Proofs: Agent a computes: for an agent the zp(zero knowledge proof) zp=(E(1) x…xE(k+1))mon n2 public rsa modulus.The output of this product is then further encrypted sum of agents shares,Ea (additive homomorphic property).

Two zero knowledge proof are there non-interactive set membership zero-knowledge proof: its non interative as interaction is not needed and proves to a that the ciphertext has an encrypted value that lies in that is the ciphertext contains feedback value within range.

non-interactive plaintext equality zero-knowledgeproofs. here the two ciphertexts, encrypted with the public key of feedback provider and other encrypted with the public key of whole list, contain the same plaintext.assuring that agent a has prepared the shares such that they add up to a correct feedback value and are trustworthy agents correspond to those correct shares.

Send Encrypted Shares and Proofs
All encrypted shares & zero-knowledge proofs are sent simply for feedback providing based ton trusted agents.

Verify the Proofs
Each agent computes zp and verifies proofs received from agent that shares are prepared correctly.

Relay the Encrypted Shares. Agent relays to each agent a, the encrypted shares received for it from trustworthy agents.where, each encrypted share is combined, any agent who drops a message would be detected without learning any of the shares.

Compute Sum of the Shares. Each agent receives the encrypted shares of trustworthy feedback providers. Agent computes as the product of those encrypted shares along with the ciphertext of its own k + 1th share by additive homomorphic property. Agent decrypts to obtain the plaintext sum and by adding the ka + 1'th share provides security

Send Encrypted Sum and Proof. Agent a sends the encrypted

Encrypt the Sum. Agent a then encrypts the sum with k+1 from previous step the sum of the shares correctly And Compute Reputation

Generate Zero-Knowledge Proof. Agent generates a non interactive plaintext equality zero-knowledge proof, assures proof has the correct sum of the shares. sum and the zero-knowledge proof to query agent

Verify the Proof. Query agent computes a and verifies the zero-knowledge proof received from each agent a.which assure agent has computed.

I. Thadani, Ankita, and Vinit Gupta. "Enhancing Privacy Preservation of Stature System Through Homomorphic cryprosystem [16]

FORMAL DEFINITION

Let t be the target agent for the stature is going to be computed. Where in input K trusted other agents must be there selected on basis on some context ψ. the trusted agents can be {ta1, ta2,..,tak} those who gives there feedback value privately for the target agent {f1,f2…fn}and the output is the final stature score of the target agent.[19] But considering the case where some agents can be malicious for the network may deviate from the protocol[20]. The protocol is to be decentralized and security is provided by homomorphism cryptosystem because it proves the randomized encryption. But it can only support the additive homomorphism but to increase the systems security even making the system work for fully homomorphic. [21]. Fig 2 gives the flow of the basic stature system

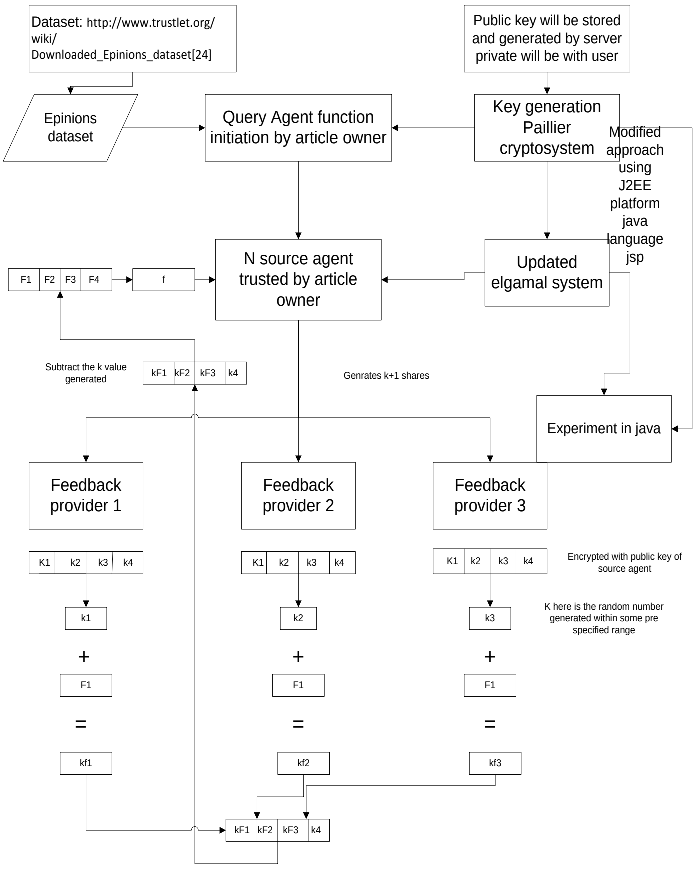

Dataset: http://www.trustlet.org/wiki/Downloaded_Epinions_dataset[24]
Public key will be stored and generated by server private will be with user
Epinions dataset
Query Agent function initiation by article owner
Key generation Paillier cryptosystem
Modified approach using J2EE platform java language jsp
F1
F2
F3
F4
f
N source agent trusted by article owner
Updated elgamal system
Subtract the k value generated
kF1
kF2
kF3
k4
Genrates k+1 shares
Experiment in java
Feedback provider 1
Feedback provider 2
Feedback provider 3
K1
k2
k3
k4
Encrypted with public key of source agent
k1
k2
k3
K here is the random number generated within some pre specified range
+
F1
=
kf1
kf2
kf3
kF1
kF2
kF3
k4

Figure 8 : Stature System

Initiation & Select Trustworthy Agents:By querying agent for computation of the reputation of a target agent .Source agent gets the feedback providers in a context(advogato trust metric[22] is used here for this purpose). Each agent can selects up to k agents.

Prepare Shares :At a time the source agent makes the k other feedback providing agents the number one decides is stated as K. Agent prepares k + 1 share for secret feedback the k shares are random numbers uniformly distributed over a large interval. But the last k+1 share (Fat-∑ individual feedback) mod M.M is publically known Fat be feedback of a source agent a about a target agent t.

Encrypt Shares: The list of all shares is implemented by agents own public key so that only agent can open it also each k th share is encrypted by public key of the feedback agent so that only one can have access to its own share by once private key. Send Encrypted Shares and Proofs: All encrypted shares & zero-knowledge proofs are sent simply for feedback providing based on trusted agents.

Verify the Proofs: Each agent computes zp and verifies proofs received from agent that shares are prepared correctly.

Relay the Encrypted Shares: Agent relays to each agent a, the encrypted shares received for it from trustworthy agents. Where, each encrypted share is combined, any agent who drops a message would be detected without learning any of the shares.

Compute Sum of the Shares: Each agent receives the encrypted shares of trustworthy feedback providers. Agent computes as the product of those encrypted shares along with the ciphertext of its own k + 1th .Agent decrypts to obtain the plaintext sum and by adding the ka + 1'th share provides security.

Encrypt the Sum: Agent a then encrypts the sum with k+1 and Compute Reputation.

Send Encrypted Sum and Proof: Agent a sends the encrypted sum and the zero-knowledge proof to query agent verify the Proof. Query agent computes and verifies the zero-knowledge proof received from each agent a. which agent has computed.

COMPARISION:

	System/ Protocol	Pros	Cons
3.1	Optimism and pessimism in trust[4] 1994	precise discussion of trust.	Development of the formalization for trust is not yet complete changing identities
3.2	trust for detecting deceitful agents[6]2000	subjective property assigned particularly by each individual and it does not depend on the context	Deals with Boolean value Uses witness No information to combine direct experiences by witnesses
3.3	How Agents Make Friends 2001[7]	Trust acquisition based on both observation and interaction	No mechanism for combining both approaches.
3.4	Afras[8] 2002	sensitivity to last experiences reduce the computational space	agent with bad reputation are not taken into account.
3.5	Bayesian network model[9] 2003	Flexible in inferring the trust of a peer for different needs	Cannot be used in large networks until large converted to small
3.6	ReputationBased Trust Model for Peer-to-Peer eCommerce Communities[11]	robust against malicious behaviors such as collusion among peers.	No mechanism for combining approaches
3.7	Zhou et alThe PowerTrust System Concept[12]	Low overhead in using locality-preserving hashing to locate power nodes. robust with dynamic peer join and leave and malicious peers	Complicated local and global computation
3.8	Hasan, et al [15] decentralized privacy preserving reputation protocol for the malicious adversarial	Zero knowledge transferred Secure ,robust	Can't prevent slandering
3.9	Enhancing privacy preservation of stature system through homomorphic system	Provide security to trust rating	Can't provide trusted user

IV. CONCLUSION

This paper has surveyed the literatures on reputation models across diverse disciplines. The centralized as well as decentralized different aggregation methods for peer to peer network. Disadvantage of each of the protocol has been pointed out. We have attempted to integrate our understanding across the surveyed literatures any tried to find out the one system proving the privacy and with strong cryptography building block.

V. REFERENCES

[1] Gambetta, Diego. "Per amore o per forza." Le decisioni scolastiche individuali(1990).

[2] D. Gambetta. Trust: Making and Breaking Cooperative Relatioins, chap- ter Can We Trust Trust?, pages 213 – 237. Department of Sociology, University of Oxford, 2000.

[3] R. Guha, R. Kumar, P. Raghavan, and A. Tomkins. Propagation of trust and distrust. In Proceedings of the International World Wide Web Con- ference (WWW 2004), 2004.

[4] Marsh, Stephen. "Optimism and pessimism in trust." Proceedings of the Ibero-American Conference on Artificial Intelligence (IBERAMIA'94). 1994.

[5] Thimbleby, Harold, Marsh, Steve, Jones, Steve, & Cockburn, Andy. 1994. Trust in CSCW. In: Scrivener, Steve (ed), Computer Supported Cooperative Work. Ashgate Publishing.

[6] Schillo, Michael, Petra Funk, and Michael Rovatsos. "Using trust for detecting deceitful agents in artificial societies." Applied Artificial Intelligence 14.8 (2000): 825-848.

[7] Esfandiari, Babak, and Sanjay Chandrasekharan. "On how agents make friends: Mechanisms for trust acquisition." Proceedings of the fourth workshop on deception, fraud and trust in agent societies. Vol. 222. 2001.

[8] Wang, Yao, and Julita Vassileva. "Trust and reputation model in peer-to-peer networks." Peer-to-Peer Computing, 2003.(P2P 2003). Proceedings. Third International Conference on. IEEE, 2003.

[9] Xiong, Li, and Ling Liu. "A reputation-based trust model for peer-to-peer e-commerce communities." E-Commerce, 2003. CEC 2003. IEEE International Conference on. IEEE, 2003.

[10] Heckerman, D. "A Tutorial on Learning with Bayesian
Networks", Microsoft Research report MSR-TR-95-06, 1995

[11] A Reputation-Based Trust Model for Peer-to-Peer eCommerce Communities, IEEE,2003.

[12] Zhou, Runfang, and Kai Hwang. "Powertrust: A robust and scalable stature system for trusted peer-to-peer computing." Parallel and Distributed Systems, IEEE Transactions on 18.4 ,2007.

[13] I. Stoica, R. Morris, D. Nowell, D.Karger, M. Kaashoek, F. Dabek, and H. Balakrishnan, "Chord: A Scalable Peer-to-Peer Lookup Protocol for Internet applications", Proceedings of ACM SIGCOMM, San Diego, Aug. 2001

[14] Zhou, Runfang, and Kai Hwang. "Gossip-based reputation aggregation for unstructured peer-to-peer networks." Parallel and Distributed Processing Symposium, 2007. IPDPS 2007. IEEE International. IEEE, 2007

[15] Hasan, et al decentralized privacy preserving reputation protocol,IEEE data transaction 2013

[16] Thadani, Ankita, and Vinit Gupta. "Enhancing Privacy Preservation of Stature System Through Homomorphic