# Enhance Reputation System Using Trust Model

Anjana Patel[1], Mital Panchal[2]

[1] *P.G. Student, Department of Information Technology L.D. College of Engineering Ahmedabad, Gujarat, India*
[2] *Assistant Professor, Department of Information Technology, L.D College of Engineering 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 provide security to user message rating through homomorphic crypto system and convert their message rating into weighted trust rating using trust metrix.*

**Keyword** : *Reputation, Trust, Peer to Peer network, Database Security, Homomorphic crypto system.*

## 1. INTRODUCTION

Reputation system computes and publishes reputation score for set of object within community or domain , based on collection of opinions that other entities hold about the objects. The opinion is typically passed as message rating to a central place where all perceptions, opinions and message rating can be accumulated. A reputation system used specific algorithm to compute reputation score based on receiving ratings. Reputation is a sign of trustworthiness manifested as testimony by other people.

Trust and reputation model being used to improve the security and commitment in distributed environments. Privacy is one of the concern in trust based system. In particular ,the feedback of an agent about another agent should be kept private in order to prevent a dishonest report due to social pressure and fear of the consequence. Aggregation of trust reports should be performed in such a way that the individual report remain private. This enhances the accuracy of the report and the aggregate trust value, subsequently. Hence, privacy in trust-based decision making is of a vital importance, as honest trust reports will lead to incorrect decisions. Privacy is related to the feedback providers reputation system because anonymity deal with genuine feedback.[6]

## 2. Definations

### 2.1 centralized reputation system:

In Centralized reputation system the feedback value is collected from agents in the community. The central authority collects all the values and Computes a reputation score on the basis of collected Value publically avail it.[9]

### 2.2 Decentralized reputation system:

In Centralized reputation system the feedback value is collected from agents in the community. The central authority collects all the values and Computes a reputation score on the basis of collected Value publically avail it.[9]

## 3. Background

### 3.1 Survey on stature system:

Table 1 Present the comparison within the literature survey done with various papers centralized system and decentralized system pros, cons and the scenario its is suitable for.

Table 1 Comparision on various survey done.

| | **Paper Title** | **Pros** | **Cons** | **Suitable for** |
|---|---|---|---|---|
| 3.1 | A Decentralized Privacy Preserving Reputation Protocol for the Malicious Adversarial Model [3] IEEE-2013 | Zero knowledge transferred secure, robust | Can't preserve slandering | Malicious adversarial reputation system. |
| 3.2 | Efficient Privacy Preserving Reputation Protocols Inspired by Secure Sum.[4] IEEE-2010 | Provide privacy to message rating. | it provided limited choice of selecting agent. | Compute reputation in privacy preserving manner. |
| 3.3 | Multi-Party Trust Computation in Decentralized Environments[5] IEEE-2012 | secure multiparty trust sum computation. | can not provide trusted user. | Suitable for compute multi arty trust in decentralized environment. |
| 3.4 | CR-SMTC: Privacy Preserving Collusion-Resistant Multi-Party Trust Computation[6] | trust computation private manner under adversarial model. | Can't protect the trust computation against malicious agents who provide false information. | Trust remain private. |

| | | | | |
|---|---|---|---|---|
| | IEEE-2014 | | | |
| 3.5 | Reputation Measurement and Malicious Feedback Rating Prevention in Web Service Recommendation Systems[7] IEEE-2015 | Detect malicious feedback rating. | The detection are fail when the intensity of malicious feedback ratings is very low. | Detection and prevention of malicious feedback rating. |
| 3.6 | Centralized Collaborative Reputation Model for B2C E-Commerce[8] IEEE-2014 | Provide enhances users trust on reputation information and biasedness can also be removed. | Biggest hurdle is wide scale adoption of this system. | Suitable for independent reputation system |
| 3.7 | Enhancing privacy preservation of stature system through homomorphic system [9] Springer 2015 | Provide security to message rating | Can't provide trusted user | Message rating privacy preservation system |

## 4. Proposed System:

### 4.1 Proposed Methodology Framework

The ideas of trust recommendation and privacy are hard to reconcile since by definition trust recommendation is the disclosure of a feedback value to another agent. However, we can imagine approximations of the trust recommendation technique that are better at preserving the privacy of the source agent.

One such technique is as follows: Instead of reporting the feedback value, the source agent may only respond to a query that demands whether his trust in the target agent is higher (or equal to) or lower than a given level. For example, Alice could ask Bob whether his trust in Carol is higher (or equal to) or lower than 0.8. A binary response of higher or lower may be sufficient for Alice to make a decision whether to trust Carol or not. The disadvantages of this technique are that: 1) the privacy of the source agent is not completely preserved, that is, the querying agent gains partial information about the feedback value; 2) an adversary could make repeated queries in order to narrow down on the feedback value. This attack may be prevented if the source agent is able to identify repeated queries by the adversary (and any members in his clique).

Another technique is to perturb the feedback value before providing it to the querying agent. This technique also has the potential to divulge partial information about the feedback value. An attacker could also sabotage this technique by repeated queries. If the value is perturbed randomly each time, then the attacker can use distribution reconstruction to derive the feedback value. However, this may be prevented if the perturbation is kept constant for a feedback value.

### 4.2 Proposed flow

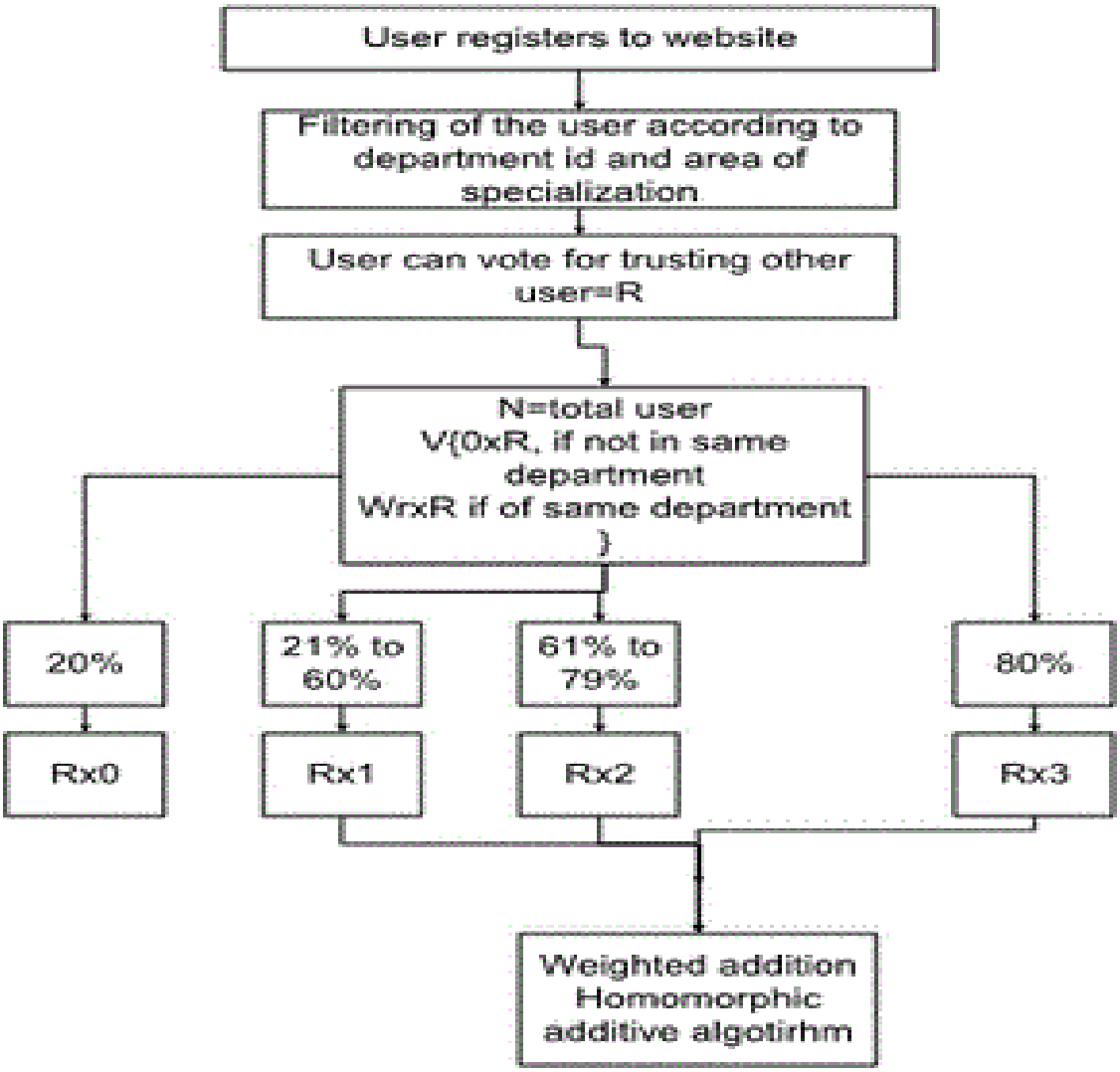


Fig:1 flow of proposed work

**4.2 Theoretical analysis:**

**4.2.1 Weighted Ratings:**

The trust among the peers can only be considered for the agents of the same department then only the can rate for trust each other. If consider agent a as Alice if there are are 10 people in the department we can use the words master , Journeyer and apprentice.

Master =70% and above. Weight =3

Journeyer= 40% to 70%. Weight=2

Apprentice= upto 40% Weight=1(NONE)

That means if alice is is the person for which out of 7 person or more trust then the weight will b added to alice which is 3. Except for the input value 0. All other value will be altered and multiplied by 3 suppose alice rated an article which is owned by bob even though bob does not trust alice if the alice rates as 3. The weight added will be 3 so the rating considered will be 9.

Suppose if the user of other department tried to rate the rating the rating will be accepted still the rating will not be reflected in the final score. As being of the other department that person cannot rate the article.

TABLE 2TRUST MATRIX OR THE WIEGHTS

| USERS/TRUST | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | X | | | | | | | | | X |
| 2 | | x | | | | | | X | X | |
| 3 | | | x | | X | | | X | X | X |
| 4 | | | | X | | | | X | X | |
| 5 | | | | | X | | | X | | X |
| 6 | | | | | | X | | X | | X |
| 7 | | | | | | X | x | | | X |
| 8 | | | | X | | X | | X | | X |
| 9 | | | | X | | X | | X | X | |
| 10 | | | | | | X | | X | | X |
| Overall trust level(Percentage) | 10 | 10 | 10 | 30 | 20 | 50 | 10 | 80 | 40 | 70 |

User 8: 8/10 rates article as 2 so weight is 3 hence 2*3 =6 Is the rating

User 6: 5/10 rates article as 2 so weight is 2 hence 2*2 =4 Is the rating

Other users: rates article as 2 so weight is 1 hence 2*1 =2 Is the rating

In the table above the symbol x represents that the user is trusted. Each and every user has trust on its self . In last we can see the total percentage for each here we have just considered the case for 10 users for ease else the percentage is calculated each time user increases.

### 4.2.2 Experimental Result

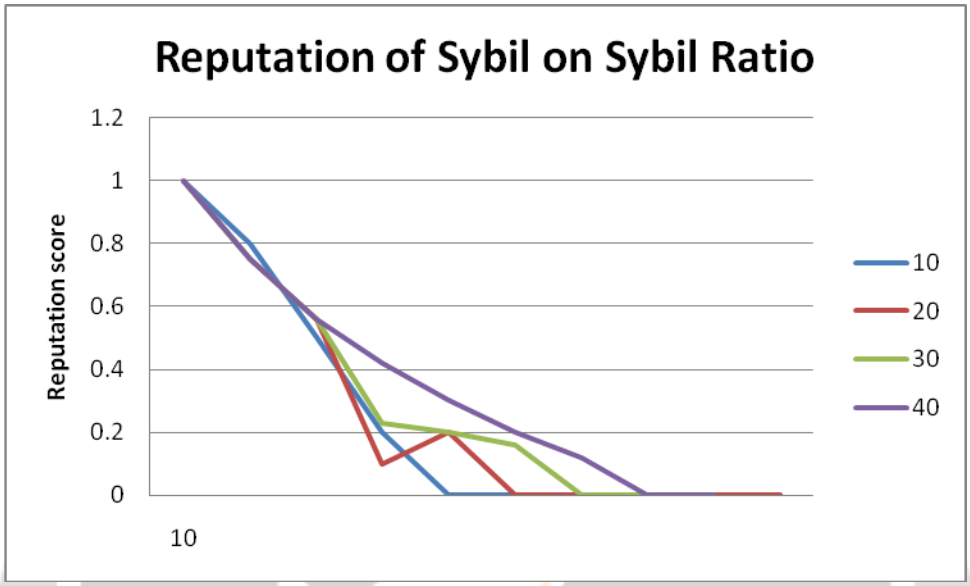


Fig 2 Repuutation of Sybil

The reputation Sybil on Sybil ration are show in diagram they describe reputation Score through Sybil ratio.

Experimental Result

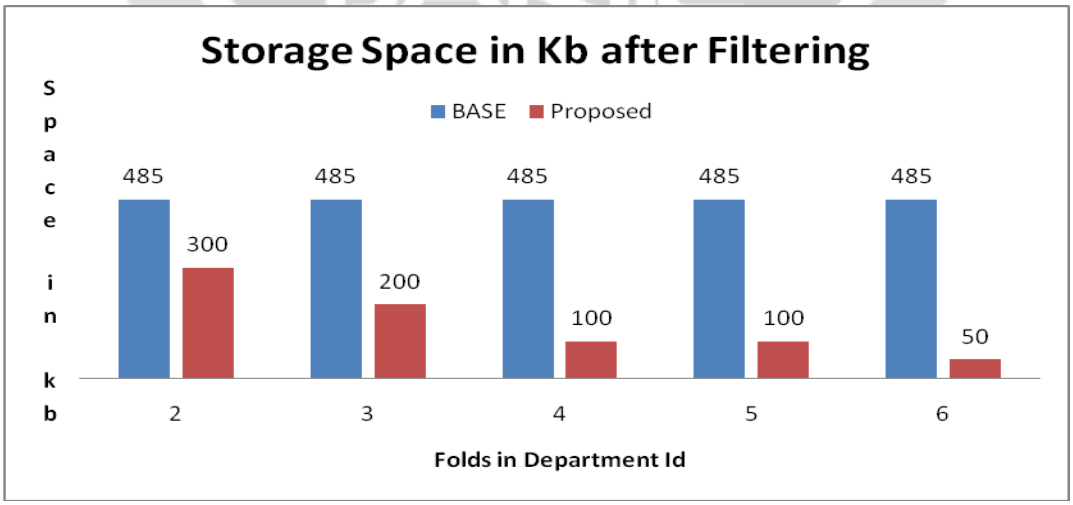


Fig 3:storage space in kb after filtering

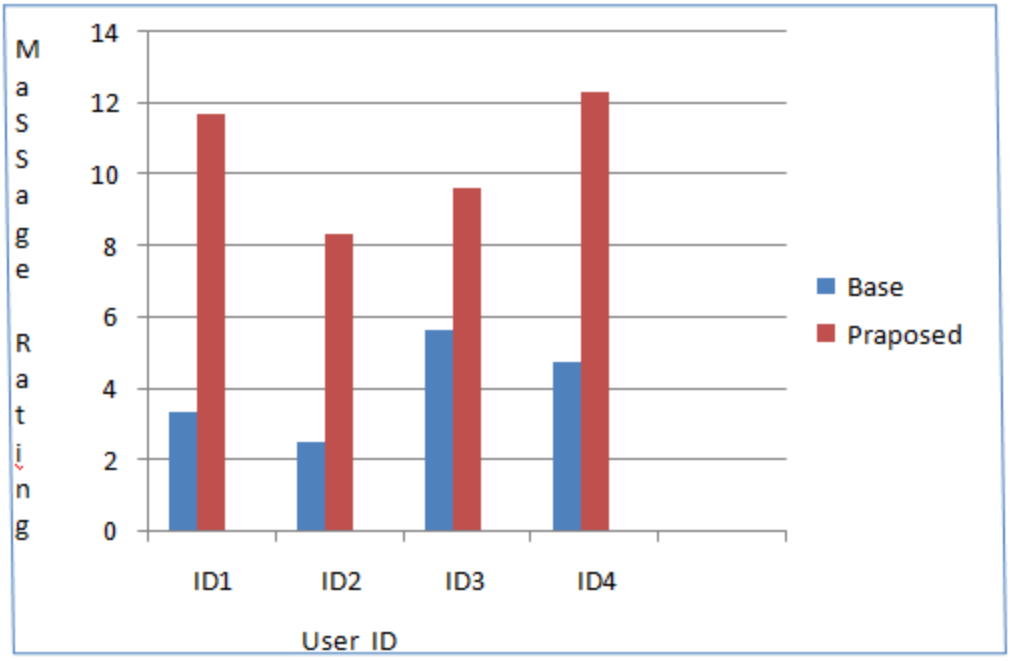


Fig 4: comparison message rating

## 5. CONCLUSIONS

The studied variety of methods, their advantages and disadvantages. In this paer, we focused on privacy preserving reputation systems. These systems compute reputation scores without revealing the individual feedback of any user. Preserving the privacy of users gives them the freedom to provide truthful feedback. Our objective was to construct privacy preserving reputation protocols they compute the reputation message rating and convert trusted user rating in weighted rating that are decentralized, they required less storage space and high reputation score than base work. So, the proposed system provide enhance reputation system.

## 6. REFERENCES

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

[2] 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

[3] Hasan, "Adecentralized privacy preserving reputation protocol for the malicious Adversarial model",IEEE data transaction on knowledge and data engineering year- 2013.

[4] Omar Hasan,Elisa Bertino, Lionel Brunie,"Efficient pvivacy preserving reputation protocol inspired by secure sum",IEEE-2010.

[5] Tassos Dimitrios, Antonis Michalas,"multi-party trust computation in decentralized environment ",IEEE-2012.

[6] Zohre fath Fathabadi, Sadegh Dorri Nogoorani, Ali Mohammad Hemmatyar,"CR- SMTCprivacy preserving collusion resistant multi-party computation: "IEEE-2014.

[7] Shangguang Wang, Zibin Zheng, Zhengping Wu, Michael R. Lyu, Fangchu Yang, "Reputation measurement and malicious feedback rating prevention in web service recommendation system", IEEE TRANSACTIONS ON SERVICES COMPUTING, VOL. 8, NO. 5, SEPTEMBER/OCTOBER 2015

[8] Muhammad muneeb Kiani , Arif Raza, Kanwal Daud Gill, "centalized collaborative reputation model for B2C E-commerc" ,IEEE-2014.

[9] Ankita Thadani, Vinit Gupta,"enhance privacy preservation of stature system through homomorphic crypto system",Springer-2015.