

Community Trust Stores for Peer-to-Peer e-Commerce Applications

Ahmad H. Fauzi and Hamish Taylor

School of Mathematical and Computer Sciences
Heriot-Watt University,
Edinburgh, United Kingdom
{ahf4,h.taylor}@hw.ac.uk

Abstract. E-commerce applications have evolved from web-based selling via the Internet to selling in a P2P manner. P2P can enhance e-commerce applications to create lower cost systems compared to conventional client-server systems. However, P2P e-commerce applications will only be acceptable to users if they can provide robust, secure and equitable services to the peers involved during commercial transactions. In this paper, we propose use of a P2P shared store for trust information to support community based e-commerce applications. Nowadays, it can be economical and cheap to implement either in the cloud or in a distributed manner over the platforms of participating peers. Usage of a cheap and secure community store for trust data provides an effective alternative to conventional trusted third party support services for e-commerce transactions.

Keywords: P2P, secure, cloud computing, trading forum, inexpensive.

1 Introduction

Peer-to-peer (P2P) offers decentralization, reduced cost of ownership and scalability compared to the client-server model. It organises service delivery around mutual provision of common services among peer computers, not communal service provision via dedicated shared providers. To achieve this, control has to be more decentralized which can make for greater complexity in the design of the P2P software architecture than for client-server systems.

The aim of this paper is to propose and justify the use of a secure community store for trust data which is collaboratively controlled by a group of peers. It can be used for e-commerce applications that involve groups of like minded people who congregate virtually to trade with each other. Such trading forums can be expected to be structured by a number of commonly agreed rules and to have memberships to help ensure that trading conforms to these rules. Trading within these forums might be in the form of sales, auctions or swap sessions depending on their common purposes. Items for trading might be second hand goods, hobby items like stamps, spare tickets or electronic resources like music recordings, movie clips or e-books.

In such a context, a community repository stores trust related information needed by trading forums such as lists of membership, trading contracts among peers, reputation reports on transactions and public key certificates used to verify the identity of peers. All other non-trust related data such as proposed deals, offers and general communication is passed through the P2P system's messaging service.

Since the store is controlled by a group of peers, it is not considered as a third party. Instead it is the trust support base of the peers themselves. The store is used to support various levels of trust that are related to the dissemination of the identity, status and reputation of a peer in relation to his e-commerce trading. The advent of widespread third party hosting of computer user's data and software on the Internet has reduced to low levels the cost of hosting a community store which holds modest amounts of trust data, is infrequently accessed and has low performance requirements. Cloud computing service providers can securely and cheaply host software that supports such a remotely accessible data repository sitting over a moderate sized storage space. Alternatively, the community store can be hosted in a distributed fashion across the platforms of participating peers under certain assumptions about their availability.

Community trust stores (CTS) are needed to foster trust among peers so that peers can mitigate perceived risks in trading with each other. They need to be available for access whenever trading might take place. Since their function is to store trust information, that data needs to be credible. That can be achieved through supporting joint updates by all concerned parties where the data purports to express the shared knowledge or intent of these parties. However, where the store stores personal opinions, they can be added by a single forum member after verifying his identity as the author of that opinion. Using a community trust store addresses the problem of secure access to trust data among peers. It is also able to tackle the problem of different peers being online at different times. The trust store is not accessed all that frequently but should be available when access is required to it.

The rest of the paper is organized as follows: Section 2 discusses problems and the motivation for a P2P community trust store. Section 3 explains the proposed model for P2P e-commerce and community trust stores. Section 4 outlines the strategy, criteria, roles, benefits, downsides, and architecture of the community store's storage mechanisms. Section 5 describes an example scenario of the P2P trading. Section 6 discusses related P2P research. A summary and conclusion follow in Section 7.

2 Problem Statement and Motivation

Updates of communally agreed trust data to the community store can be limited to joint operations by the concerned parties to ensure that stored data accurately expresses their shared belief or will. Contracts between contracting parties can be limited to being added only by a joint operation of both parties. Membership additions can be constrained to being limited to joint operations of all their

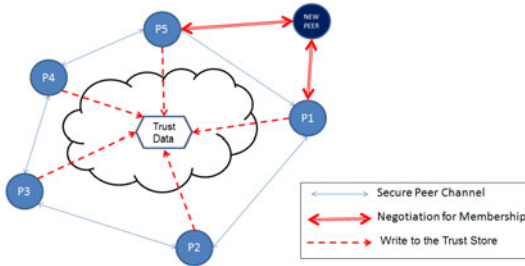


Fig. 1. The Proposed Framework for P2P e-Commerce and Customer Trust Stores

required sponsors. Identity certificates can be limited to being added jointly by all their signatories who are forum members and so on. Other trust data like deal evaluations by one trader of another trader’s deal with him are not collective verdicts but personal opinions so they can be added individually so long as the member’s identity is suitably verified by his digital signature.

However, there still remains an open issue of how best to combat various forms of unethical collusion in such non-hierarchical communities. For example multiple peers may gang up together to create fictitious trading contracts which are favorably evaluated in bogus reputation reports by the colluding parties. Or they may conspire together in sufficient numbers to succeed in voting for the exclusion of a bona fide member on trumped up grounds. However, these are not problems especial to online trading. They are general problems for all forms of community trading.

3 Proposed Model for P2P e-Commerce and Community Trust Stores

Peer-to-peer computing benefits e-commerce applications since it is cheaper to implement compared to conventional client-server e-commerce applications. The overall proposed framework using P2P and cloud computing technologies in e-commerce applications is depicted in Figure 1. P2P is used as the whole network infrastructure and cloud computing as a subnetwork infrastructure for supporting the CTS. Details of this framework are discussed in following subsections.

An online community trust store can support various types of trading including direct selling, auctions (open-cry or sealed bid), barter trade and lowest offers for solicited services among others. The type of trading determines how goods, cash and services are exchanged with each other. Important issues concern how well contracts are made binding between the trading parties and how well contracts protect the interests of both parties fairly and securely. In direct selling of second hand goods, a peer would typically expect to inspect the item before going ahead with buying it. However for never previously used services offered by a vendor, peers cannot assess the quality of a service before it is rendered and have to rely on feedback or testimonials from other peers that have used that

service from that vendor before. For example, in relation to a cleaning service offered by a vendor, other peers would expect to be able to consider feedback from peers that have used that vendor's service before agreeing to hire that cleaner. Different types of trade will have their own distinct requirements and challenges.

3.1 Using P2P for e-Commerce Applications

The proposed model for P2P e-commerce model takes several criteria into consideration:

- Accessibility: Although two peers may not be online at the same time, trust information from each peer should be easily accessed by the other peer on demand.
- Reliability: The trust store system should provide required trust data upon request.
- Tamper proof: Only authorized and involved parties can update and modify trust data.
- Auditable: An audit trail is maintained for all transactions with the trust store.
- Trustable: These properties make the store a trustable source for information provided by authorized parties.
- Confidentiality: Only authorized peers can access confidential information.

The proposed P2P e-commerce trading model starts with at least three peers that have an initial trusted mutual understanding to trade amongst each other. In order to realise this framework, the peers need to 1) store identity certificates of recognised peers; 2) record trading contracts of proposed deals; 3) store transactions stating agreed outcomes of proposed deals; 4) record reputation reports about peer deals; and 5) store membership status of peers. All of the above information are stored in the CTS.

3.2 Using Cloud Computing for the Community Trust Store

The general idea of a CTS is based on the use of shared memory space among the peers. One option to achieve this is to require peers to contribute their file space and hours of online time in return for continued membership of the P2P community. A peer that fails to comply can be threatened with having its membership revoked. Another option is to adopt a cloud computing approach by storing trust data in the cloud. When the trust data is in the cloud, it is not necessary for some peers to be online so that the trust store can be immediately accessed. The cloud space can either be very cheap or free commercially supported storage or voluntarily contributed unused space on networked machines controlled by some participants in the trading community.

A secure CTS using cloud computing network technology is proposed as the more desirable way of implementing the model since it provides the most available way of accessing the latest version of trust related trading and reputation information. It offers:

- Accessibility, the store is the hub for various data operations in e-commerce applications. When using the store, member credentials based on the identity they present in the digital world can be checked. Identity will be established using public key certificates.
- Cheapness, by using each other's resources or cheap computing in the cloud, P2P stores should be able to support an inexpensive system compared to conventional client-server systems.
- Scalability, a cloud implementation of the shared trust store would limit how many peers can use it at the same time. However, that usage will not be frequent or intensive. It is rather more likely that the social dynamics of a very large community will cause it to split into sub-communities with their own community trust stores before the community size grows to the point of saturating usage of a single trust store. Storage requirements will grow linearly with peer numbers.
- Availability, a cloud implementation of the store could be expected to be available 24/7. However, a P2P implementation of the store over the storage space of peers would be dependent on enough peers remaining online at the same time to host the required data. In such cases the community might have to limit trading to communal sessions where a high enough participation rate could be guaranteed so that relevant trust data would be immediately available.

Cloud computing involves applications being delivered as services over the Internet where the hardware in the cloud provides those services [16]. Cloud computing consists of infrastructure, platform, storage, application and services. It allows the application to run in the cloud instead of being run locally on a dedicated machine. However there is always a security risk involved when running an application or storing data in the cloud. As it involves data transactions in and out of the cloud, the possibility of data tampering and loss is a significant risk. There will be issues of trusting the cloud and the reliability of the application hosted in the cloud. A reasonable strategy has to be planned to ensure accessibility of the store within the cloud. However, use of cloud computing technology means that data can be synchronized and updated without having to have cooperating peers online at the same time.

The downside of a using a CTS is its shared nature. Its operation may not be fully reliable and extra assurance would be needed as to whether a third party hosting the cloud is to be trusted. It will have issues of availability when network connectivity is disrupted due to attacks or interruptions of connections or peers disconnect from the peer network. We will discuss later on the elimination of the third party roles to validate and verify a peer. Other issues and weaknesses of using a CTS are trust and safety issues with the store itself.

4 Strategy and Criteria for the Community Trust Store

There are several characteristics for the CTS which need to be manifested in order to manage P2P trading efficiently. The store has to keep relatively small

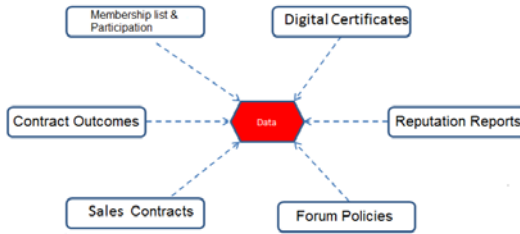


Fig. 2. Data Stored in the P2P Community Trust Store

items of data. Maintaining a small size item in the store will not impose much of space burden as long as the number of such items is not large. It will also ensure that they are easy to replicate or back up and recover quickly. The CTS should always be available when needed but is only likely to be infrequently accessed. The items that will be kept in the CTS are list of current, former and expelled members; digital certificates of members; trade contracts and agreed outcomes; reputation reports of present and past members; trading forum rules and policies; and member's participation data.

As depicted in Figure 2, these items are related to each other. For example, an operation to update the membership list must be signed by the private keys of the minimum number of members required by trading forum policies in order to update the list. Sales contracts are written with feedback signed by the persons involved in the transaction in a hierarchical format so that we can trace back the feedback to specific past transactions. The reputation reports of peers are based on data gathered from transaction feedbacks. Forum policies will be agreed by members in accordance with their collective decision making procedures.

The integrity of content in the store is protected using the private keys of peers. They collectively or individually sign each item they want to store and place it in the trusted community store. There is no general necessity for peers to encrypt the content that they want to write to the store. However there will be exceptions for types of selling such as sealed bid auctions where a bidder needs to encrypt their sealed bid using the auctioneer's public key to stop other peers from discovering their bid. The replication strategy is another way to protect the CTS content. When the content is backed up multiply, the possibility of losing the content is lower.

The decentralized nature of a peer-to-peer system leads to security vulnerabilities in peer-to-peer applications. In order to ensure the store is secure, a security management strategy has to be put in place. It will use preventative measures to reduce the risk of attack and would be expected to include a recovery plan if a security breach is detected. Only peers that are members of the P2P community should be allowed to write data to the store. So, unauthorized peers should have no chance to add anything to the community trust store. Although members are allowed to write new data, they should only be able to append to existing data and only able to edit their own feedback.

A recovery strategy can be used if the store is compromised. If a storage host is compromised such as data being tampered with or becoming inaccessible, the CTS could restore the missing or invalid data from data backups that are stored among member peers. This will ensure that the data is up-to-date and available. Providing a recovery strategy for the P2P system supports fault tolerance and resistance against denial of service attacks. Peers can access the latest data from the CTS each time they are online. That is the reason the size of files in the store should be small in order for quick data backup, replication, updating and recovery. The overall size of the stored data can be constrained by archiving or maybe deleting old records beyond suitable time to live periods. Security strategies that should be implemented include:

- Using public key infrastructure to ensure messages and files exchanged between peers and the CTS are tamper proof
- Regular backup of CTS contents; replication and backup of the CTS contents into other clouds or into distributed storage solutions with the agreement of the peer community
- Validation of P2P software by the peers to avoid malware in the software
- Enforcing punishment for peers that breach security and privacy of others
- Protecting the trust content of the CTS using cryptographic methods that are strong yet efficient in term of performance
- Recording and tracking of trust content being accessed, updated and modified by peers in the CTS

These security strategies will be implemented jointly in accordance with trading forum policies. These address the following risks, weaknesses and threats :

- Security of the application (application level): How can we be sure the application is safe to use? Does it contain malicious code or Trojan horses? How confident are we to install and use the peer application? These are important issues in developing a trusted application. Peers must have adequate assurance it is safe to use the application if using it entails security risks. The software application should use established techniques like signed code and digital watermarks so that it can to be verified and endorsed by the peers. If the source code is made publicly available, compilation of the application can be made by the peer themselves. Apart from peer's endorsement, the endorsement by well known or reliable third parties can be implemented as well to eliminate sceptical doubts related to security of the application. Although publishing the source code publicly ensures transparency of the code in terms of proving there are no malicious code in it, it is acknowledged that this also gives opportunities to attackers to study the code and finds its vulnerabilities.
- Security of communication (network level): These are issues of message confidentiality, peer's identities and ensuring peers are communicating with the person whom the person claims. It deals with ensuring confidentiality and integrity of communication. By using public and private keys as ways to communicate with each other, peers and the CTS should be able to prevent

tampering and modification of trust data. The CTS can identify itself with its own public and private key pairs by signing its sources and messages to peers. By communicating directly with the CTS, peers also eliminate the risk of relying on other peers to obtain trust data thus minimizing the chances of modification of data through the man-in-the-middle attacks, spoofing and masquerading. This issue also includes access to the CTS, which can be blocked by denial of service attacks. Peers will not be able to get the trust data stored in the CTS if the content cannot be delivered due to network failures caused by attackers.

- Security of the environment (user level): In order to create a secure environment, there are issues related to trust among peers, bandwidth limitations, protection against threats, safe backup, recovery and bootstrapping and policies governing peers membership. The peers have to ensure their own machines are secure and safe from malicious code. Peers that are unable to comply with the trading community security policy can be removed from the membership list.

Where the CTS is supported by a third party cloud storage service, we assume that a reputable service provider should be able to ensure a secure environment for the CTS. However, with a proper backup and recovery strategy as proposed, it seems reasonable to expect that the availability of the trust data can be ensured with minimal threat and guarantee with reasonable service downtime. Regular backup of the trust data to different cloud or distributed P2P storage facilities should be able to provide additional assurance that the data in the CTS is safe, recoverable and secure.

5 Scenario of Trading in Proposed P2P e-Commerce Model

Various trading scenarios can be supported by P2P e-commerce. However one of especial interest is low valued good sales in community markets. The proposed P2P trading model suits such low valued good sales. Low valued goods sales often happen in venues like flea markets, garage sales, car boot sales, Sunday markets and charity sales. Characteristics of such trading are low price items; second hand or used items; cash sales for on the spot delivery; no refunds and slim chance of legal redress; buy as seen with no provenance or warranty; prior inspection of goods for sale; and price of item being negotiable.

This type of sale attracts a wide audience as the items are seen as cheap, value for money and potentially a good bargain. However, its characteristics also encourage fraud, fencing, misrepresentation and breach of intellectual property rights (IPR). Nevertheless, it is a popular method of buying and selling worldwide. This type of trading is envisaged as a viable application area for P2P e-commerce. When such trading is done online, it has its own limitations. For example, items which are advertised online are usually described initially using text and pictures via a chosen platform. The description based on text

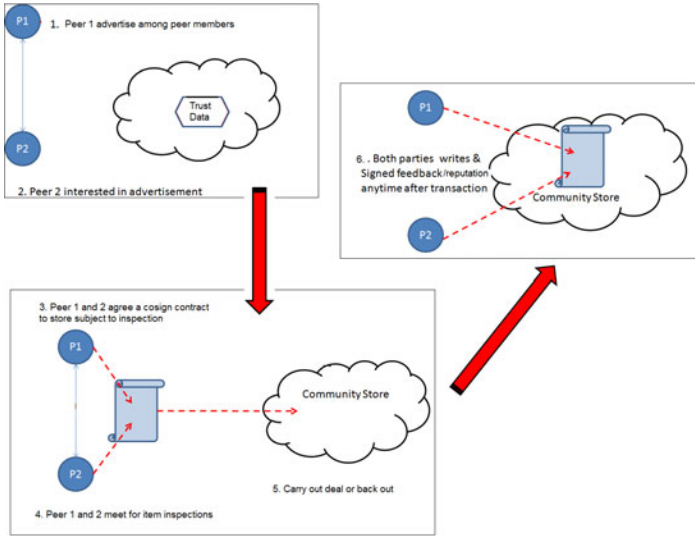


Fig. 3. Sample Scenario in the Proposed P2P Community Trading Model

and pictures can sometimes mislead buyers. Inspection of items is still needed. Buyers will expect to be able to inspect the item and decide if they want to accept the ‘as is’ condition of the item. Only if the buyer is satisfied with the inspection, will payment be made. Else, the deal is off and the seller will have to find another potential buyer.

The proposed type of scenario for P2P trading involves agreement to buy and then inspection before completing the sale of the advertised goods. Referring to Figure 3, assume that there are two existing peer members, P1 and P2. P1 is selling a second hand text book and posts an advertisement through the P2P messaging service with his digital signature. P2 sees the advertisement and informs P1 he is interested in buying the book. P1 sends a contract to P2 to buy the book as described for a certain price subject to quality inspection arranged with P1. P1 accepts the proposal or negotiates a revised proposal and then both parties sign the contract, agree where and when to meet, and submit the contract to the CTS. Upon meeting P1, P2 inspects the book in order to decide whether it meets the terms of his contract to buy it and P1 assures himself that P2 has the money to pay for it. Whether the transaction goes through or not, P1 and P2 are expected to exchange reputation reports in the P2P trading community by updating the CTS jointly and report on the outcome of their meeting.

The reputation report could be a positive or negative comment related to the transaction. For a specific reputation report on a transaction, only the trading peers will be allowed to contribute reputation reports if they have previously committed a joint contract to the CTS. In the future, other peers that wish to perform trades with P1, can gather feedback on P1 via the CTS and use it to help them to decide whether to initiate a trading transaction with P1.

Some back of the envelope calculations can be used to estimate the use of bandwidth and the data footprint of a CTS being used in P2P e-commerce trading. Trade contracts, reputation reports and contract outcomes will have a size of around 1000 bytes each. PGP digital certificates might average 10000 bytes in size. A transaction might involve access to something like 40 reputation reports, 20 certificates, 10 contracts and 10 contract outcomes on the CTS. It will upload 1 contract, 2 reputation reports and 1 outcome. So it will involve the downloading of 260 Kbytes of data and the uploading of less than 5 Kbytes.

If the trading community comprises 1000 members and each performs 5 transactions per week, 260 Mbytes will be uploaded and less than 5 Mbytes downloaded per week. If the store holds 1 years worth of transactions then it will hold 260 contracts and outcomes, 520 reputation reports and 1000 certificates. This will occupy approximately 11 Mbytes. Together with ancillary data like testimonials, forum policies, logs and so on lets say a total of 20 Mbytes. Even if these are underestimates by 10 times, it is clear that data traffic to and from the CTS and the size of the communal trust database are modest in scale. Hence the CTS should be easy to support in a typical cloud computing environment.

6 Related Work

In this section, we review cloud formations; P2P storage systems; identity and reputation issues; Web of Trust and Public Key Infrastructure.

6.1 Cloud Formations to Support a CTS

Cloud services can be obtained in several ways. One way is by using an existing commercial cloud service such as offered by Amazon Elastic Compute Cloud (EC2)¹, Windows Azure² and Google Apps³. These providers offer to run code from users on their cloud facilities. They also guarantee security of data stored or applications run within their cloud. However, all three charge money to provide cloud services to customers.

Other than that, a cloud can be formed using existing machines in an organisation such as with in an ad hoc cloud computing approach [1]. This approach uses computing resources harvested from machines within an existing enterprise. For example a P2P trading forum exclusively for staff and student of a university could use available unused computing resources from the university's computing facilities or labs.

6.2 P2P Store

In P2P research, several P2P storage systems have been proposed such as PAST [2], PeerStore [3], Wuala⁴ and OceanStore [4].

¹ <http://aws.amazon.com/ec2/>

² <http://www.microsoft.com/windowsazure/>

³ <http://www.google.com/apps/>

⁴ <http://www.wuala.com>

PAST storage is formed over peers that are connected with each other over the Internet. Each peer can initiate and route client requests to update or retrieve files. Peers are also able to contribute storage to the PAST system. The files on peers can be replicated on multiple peers to increase their availability. The CTS only needs to store a modest amount of data but it needs to be able to update and to access all data quickly. PAST is rather more suitable for backup of data than supporting CTS contents. PAST is a non-incentives based system which does not reward peers that contribute storage to other peers. PAST nodes and users can use smartcards to authenticate entities and assure the integrity and confidentiality of data. The client can encrypt the content of file using their smartcard before inserting the file into PAST.

The relevant contribution of PeerStore related to peer-to-peer backup systems is its safekeeping and fair contribution scheme. Peers regularly challenge each other to verify their partners are still storing the blocks entrusted to them by asking them to prove they are still storing all block replicas. A partner that fails to answer a challenge is punished by discarding information that the peer has stored on the challenging peers. However, punishing a peer that fails to answer a single challenge might lead to peers experiencing technical failure or downtime losing their backup. On the other hand, a more lenient strategy might encourage free riding among the participating peers. Although PeerStore's intention is to improve high long-term availability instead of short-term availability, the strategy could result in possibly long waiting times for a restore operation to take place. Another problem is that there is no way to decide whether a partner is temporarily off-line or has permanently left the network. A further challenge for Peerstore is that a peer has to look for and find a sufficient and suitable number of partners that can store their data otherwise it will be unable to guarantee the backup of its data. The task of finding suitable partnering peers might also take time.

In Wuala, users can trade local machine storage for online storage. If a user gives up a certain amount of storage space on his computer, he will be given a certain amount of space in the Wuala online storage on the condition that peers have to be online at least 4 hours per day (17%). The amount of online space given is calculated based on the online time. For example, if a user donates 100GB of space, the given online space will be a multiple of the online time percentage and the space contributed. If the online time is 50%, then the online storage will be 50GB. Wuala supports access permissions and client side encryption but could only be used as a community trust store if it was augmented by reliable mechanisms to constrain collective updates to community data by sets of authorised parties. Wuala supports data replication in order to improve data availability where much of its storage facility is offline most of the time. However, it doesn't support incremental encryption which slows down access to recently updated files. For this reason Wuala is more suitable for personal data backup than serving as the host for a CTS.

OceanStore is a global-scale decentralized storage system where many computers collaborate and communicate across the Internet [4]. It uses the Tapestry [5]

overlay network which enables it to overcome problems of fault tolerance. The infrastructure is comprised of untrusted servers. However, data is protected through redundancy and cryptographic techniques. It also intended for data to be in a nomadic state where it is not tied to one physical location and is passed freely among hosting machines. An incremental cryptographic technique is used in OceanStore. It avoids the hassle of data decryption, updating and re-encryption. Incremental cryptography makes it possible to quickly update an encrypted document, rather than have to re-compute it from scratch [6]. Only users with the right encryption keys are able to decrypt and read the data. Read and write access of users are managed through the access control list of the OceanStore system. In OceanStore, each data object has a globally unique identifier (GUID). When an object is written into the system, replications of it are created and saved in different locations. These replicas are called floating replicas, because they can be transferred from one location to another. There are two forms of object in OceanStore, the active form and an archival form. Archival forms are spread over many servers and in a stable state where no further updates are necessary. The active or current form of object can be updated. Objects are modified via updates (versioning system) and data is not overwritten. This guarantees faster synchronization among the peers because there is no necessity to overwrite the whole object which would take much longer. A versioning system also allows a more efficient recovery process by only focusing on the update rather than recovering the whole data. It has to search and verify the latest version of data before initiating any necessary recovery process.

OceanStore is a better distributed storage solution for a community trust store than Wuala because of its use of incremental encryption even though it does not address incentives for users to contribute storage space. It would also need to be augmented with mechanisms to enforce trading forum rules and to support shared updates on commonly agreed data.

6.3 Reputation Issues

In general, reputation is the opinion of the public towards a person, a group of people, an organization or a resource. It is the memory and summary of behaviour from previous transactions [7]. Reputation can be used to set expectations when considering future transactions. In the context of peer-to-peer applications, reputation represents the opinion of nodes in the system towards their peers and resource providers [8]. It also allows peers to build trust and confidence which can lead them to make a decision. By harnessing feedback from peers, a reputation based system can help other peers to decide who should be trusted, can encourage trustworthy behaviour and can deter dishonest participants [9]. Without a credible reputation service, dishonest peers will erode the foundations of collaborative applications and generate peer mistrust and application failure [10]. Recent research has shown the significant extent to which a reputation system facilitates fraud avoidance and supports better buyer satisfaction [11], [12], [13], [14]. Here we discuss three relevant reputation issues which are multi dimension feedback, defending peer reputation and peers without previous transactions.

Multi Dimension Feedback. The feedback from peers can be positive, negative or neutral after a transaction. Positive feedback can easily be kept by the parties involved as they will want to use them in promoting their own reputation. Many reputation systems only handle positive reputation reports [9]. Some couple privileges to accumulated good reputation, for example reputation earned from exchange of gaming items or auctioning [15]. However, in trading users are also interested in knowing about the negative reputation of another trader. Negative reputation is a potent indicator to avoid or be cautious about dealing with a particular trader.

We propose using the CTS to store reputation reports on peers. Then, if anyone wants to check on a peer's reputation, such information can be reliably obtained from the CTS. The peer that gives feedback on another peer can store the feedback from his transaction in the CTS and sign it with his digital signature to ensure that the feedback is tamper proof. Dissemination of the reputation report from the CTS across the peer's community provides an alternative source of data if reputation records at the CTS become inaccessible and its signature prevents modification by the assessed peers. It also provides a backup of a peer's reputation.

Reputation based on feedback can implement an expiry date or duration of validity if CTS storage space is tight. Only the more recent transactions of other peers would be kept and any feedback more than that limit would be removed or archived to conserve space. Each feedback will also be logged to keep track of the last transaction, validity and modification. The reputation system will hold two main types of records - reputation reports about individual trades and testimonials about a trader's general trustworthiness to trade with. Apart from direct feedback from peers, transaction logs can serve as a third factor for peers to use to judge a peer's tradeworthiness. Logs contain a summary of specific transactions, its timeline and the outcome of the trading. Peers with little recent transaction history or high non-completion rates or with long average transaction durations may be peers to be wary of when doing business. In order to have a reasonably informative assessment of reputation data, we propose using a multi dimensional reputation system. It covers transaction ratings by other peers using several standard criteria based on Likert scales and free text comments as well as general recommendations by others (testimonials). Standardized ratings using multi dimensional scales can be aggregated and averaged to produce overall reputation values. Together with individual text comments and testimonials they can be used to judge or evaluate whether to deal with a peer.

Defending Peer Reputation. Apart from having an accessible and accurate reputation system, the content of the reputation data needs to be protected and guarded against any threat of unauthorized modification either from the peer itself or by others. As the reputation data is stored in the CTS, it should be invulnerable from being tampered by any peers as long as the information and CTS are well managed. Each feedback will be signed by peers that give the feedback and time stamped by the CTS. If we can match and synchronize the time stamp of peers signing with the time the feedback was created, we should

be able to verify whether the feedback is likely to have come from the person that gives the feedback.

Peers should also be given the chance to defend themselves against unfair feedback. As the feedback can be hierarchically added and tracked, peer can give comments on feedback received about them. It is important to have check and balance features to be fair to both trading parties. They can even defend themselves with proof by referring to the trading contract or other reputation reports if they think the feedback is incorrect or misleading to others.

Peers Without Previous Transactions. Since we are aiming to have a CTS for local trading, we assume some peers might know a new peer in-person and based on this knowledge, they can recommend or become the point of reference for the peers by issuing testimonials.

7 Conclusion

We have presented a framework for community trust stores to support P2P e-commerce applications. It uses trading forum membership to control access to the community trust store. We have addressed the problems of trust in P2P e-commerce and proposed a solution that ensures the availability of the store using cloud computing services. The proposed use of cloud computing to host community trusted store (CTS) is able to service P2P user needs and requirements. The CTS is hardened and secured to ensure the trustworthiness of its content to the P2P trading community. Access to the trust content in the CTS by the peers is recorded and logged. A reputation system and jointly signed trading contracts with trading outcomes provide the trading records of peers. The use of tamper proof evidence and endorsement methods in the CTS which are checkable and guaranteed to nurture trust in the contents of the CTS. They also help to build the trust among peers that use P2P e-commerce applications based on use of a CTS. We are developing a prototype of this type of application based on using CTS stored in an Azure cloud. We will use it to validate our approach.

References

1. Kirby, G.N.C., Dearle, A., Macdonald, A., Fernandes, A.: An Approach to Ad hoc Cloud Computing. Computing Research Repository, abs/1002.4738 (2010)
2. Druschel, P., Rowstron, A.: PAST: A Large-Scale, Persistent Peer-to-Peer Storage Utility. In: Proceedings of the Eighth Workshop on Hot Topics in Operating Systems (HOTOS 2001), p. 75. IEEE Computer Society, Washington, DC, USA (2001)
3. Landers, M., Zhang, H., Tan, K.L.: Peerstore: Better Performance by Relaxing in Peer-to-peer Backup. In: Proceedings of the Fourth International Conference on Peer-to-Peer Computing, pp. 72–79. IEEE Computer Society, Washington, DC, USA (2004)

4. Kubiataowicz, J., Bindel, D., Chen, Y., Czerwinski, S., Eaton, P., Geels, D., Gummadi, R., Rhea, S., Weatherspoon, H., Weimer, W., Wells, C., Zhao, B.: Oceanstore: An Architecture for Global-scale Persistent Storage. *SIGPLAN Not.* 35, 190–201 (2000)
5. Zhao, B.Y., Kubiataowicz, J.D., Joseph, A.D.: Tapestry: An Infrastructure for Fault-tolerant Wide-area Location and Routing. Technical report, Berkeley, CA, USA (2001)
6. Bellare, M., Goldreich, O., Goldwasser, S.: Incremental Cryptography: The Case of Hashing and Signing. In: Desmedt, Y.G. (ed.) *CRYPTO 1994*. LNCS, vol. 839, pp. 216–233. Springer, Heidelberg (1994)
7. Oram, A.: *Peer-to-Peer, Harnessing the Power of Disruptive Technologies*. O'Reilly Media (2001)
8. Hoffman, K., Zage, D., Nita-Rotaru, C.: A Survey of Attack and Defense Techniques for Reputation Systems. *ACM Computing Surveys* 42, 1–31 (2009)
9. Resnick, P., Kuwabara, K., Zeckhauser, R., Friedman, E.: Reputation Systems. *ACM Communications* 43, 45–48 (2000)
10. Akerlof, G.A.: The Market for 'Lemons': Quality Uncertainty and the Market Mechanism. *The Quarterly Journal of Economics* 84, 488–500 (1970)
11. Houser, D., Wooders, J.: Reputation in Auctions: Theory, and Evidence from eBay. *Journal of Economics & Management Strategy* 15, 353–369 (2006)
12. Resnick, P., Zeckhauser, R., Swanson, J., Lockwood, K.: The Value of Reputation on eBay: A Controlled Experiment. *Experimental Economics* 9, 79–101 (2006)
13. Xiong, L., Liu, L.: A Reputation-based Trust Model for Peer-to-peer E-commerce Communities. In: *Proceedings of the 4th ACM Conference on Electronic Commerce*, pp. 228–229. ACM, New York (2003)
14. Lin, K.J., Lu, H., Yu, T., Tai, C.E.: A Reputation and Trust Management Broker Framework for Web Applications. In: *Proceedings of the IEEE International Conference on e-Technology, e-Commerce and e-Service*, pp. 262–269. IEEE Computer Society, Washington, DC, USA (2005)
15. Resnick, P., Zeckhauser, R.: Trust Among Strangers in Internet Transactions: Empirical Analysis of eBay's Reputation System. In: The Baye, M.R. (ed.) *The Economics of the Internet and E-Commerce*. *Advances in Applied Microeconomics*, vol. 11, pp. 127–157. Elsevier Science (2002)
16. Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., Zaharia, M.: A View of Cloud Computing. *ACM Communication* 53, 50–58 (2010)