Secure Community Trust Stores for Peer-to-Peer e-Commerce Applications Using Cloud Services

Ahmad H. Fauzi, School of Mathematical and Computer Sciences, Heriot-Watt University, Edinburgh, UK

Hamish Taylor, School of Mathematical and Computer Sciences, Heriot-Watt University, Edinburgh, UK

ABSTRACT
P2P e-commerce applications have much lower operational costs and are inherently more scalable than conventional client-server online trading. Community Trust Stores (CTS) provide reliable and secure storage services for peers involved in P2P e-trading by storing trust data for the peers. Freely available cloud services can host the Community Trust Store and provide 24/7 availability to participating trading peers avoiding the need to pay for commercial trusted third party services. However, the community store must provide a certain level of assurance and support suitable security measures in order to support e-trading within the P2P application. It must also support community management of the store including jointly signed trading contract. The Community Trust Stores also stores reputation report and trading outcomes as future reference for others. New membership for P2P e-commerce group must be sponsored by current members.

Keywords: Cloud Computing, E-Trading, Inexpensive, Peer-to-Peer (P2P), Secure, Server-Less

INTRODUCTION
Ways of trading over the Internet have evolved over time resulting in varieties of trading schemes. Successful e-commerce providers such as eBay, Amazon and Alibaba.com use the client-server approach to provide centralized services to customers who wish to trade with each other. They provide the service globally through their dedicated servers. Users are charged accordingly when trading using their services. They act as a trusted third party in supporting security mechanisms and services and providing assurance to users that it is safe to trade within their environment.

A different approach to trading involves a group of parties who get together to establish a common trading framework and share responsi-
bility for providing supporting services. On this approach no single party or small minority of persons organise the marketplace. Organisation is decentralized and communally achieved. The trading model is supported by common use of the same software in a deployment configured to serve communal interests. This paper adopts this type of peer-to-peer approach and specifies a peer-to-peer design framework to achieve it.

Peer-to-peer technology is generally cheaper to run and should be more scalable compared to conventional client-server systems. However, the participation of peers in a peer-to-peer network is often unreliable, as each peer can be online at different times and delays can be expected with real-time peer-to-peer transactions.

All e-commerce involves risk taking by participating parties. These risks are various but include being cheated, being taken unfair advantage of and being deprived of fair opportunities to trade advantageously. E-commerce traders need assurance that they can mitigate these risks to a sufficient degree otherwise it becomes unwise of them to engage in such e-commerce. Part of that assurance is provided in P2P e-commerce systems by their trading model. Another part is provided by its security services.

The latter includes trustworthy means of identifying trading parties and reliable storage of all trust data needed during trading to evaluate transactions and judge the trustworthiness of trading parties. In this approach a Community Trust Store (CTS) stores all trust related data of the trading parties, including peer identity credentials, trading contracts, trading outcomes and reputation reports.

Due to the uncertain availability of peer computing platforms, the CTS need to be hosted by a means which is available whenever it is needed. A cloud provides one solution to this problem. It is able to host the CTS and support continuously accessible storage of trust data for trading activities for P2P e-commerce trading parties. A cloud provides a cheap solution for hosting the CTS compared to one or more conventional dedicated servers provided by a trusted third party e-commerce service provider. Typical cloud services offer to host applications with a small data footprint, modest throughput and moderate use of bandwidth for free.

This research confines its attention to the overall design and security issues for P2P e-commerce trading to support local trading for low valued goods. Low valued item includes second hand items gift such as clothes, books, electrical appliances, toys and DVDs. It is less problematic compared with e-commerce trading in general because the items which are being traded are low valued and the proximity of the trading parties means that the buyer can inspect the item before buying and the parties can exchange the money and goods directly at the same time. It avoids the problems of services like eBay of buying without inspecting at first hand, unsynchronised exchanges of money and goods, insecure remote payment, high charges for remote delivery of goods and the risks of suffering a large loss in a single transaction through fraud or mishap.

Existing online local trading sites such as Gumtree.com, which provide some level of free service for a local community to advertise items, lack features to report the outcomes of their trade and reputation reports of traders’ previous trading history.

A P2P-CTS provides a free service for the members of a trading community to trade in a P2P style by providing history of previous trades and reputation reports that is made available to the members via the publicly available CTS which is hosted in the cloud.

This paper is structured as follows: Scenario of P2P trading with CTS, security issues for the P2P trading system, implementation model for P2P local trading and Community Trust Stores, related works of the research, discussion, future works and conclusion.
SCENARIO OF TRADING IN P2P-CTS APPLICATIONS MODEL

A trading scenario in Figure 1 illustrates how P2P local trading applications can exploit the CTS. Generally, the trading process takes several steps:

1. Buyer (Bob) searches for items and seller (Sue) advertises a desired item through the P2P messaging service of the online trading forum. After looking around they find each other;
2. Bob and Sue look up reputation reports in the CTS stored in the cloud on each other’s trading history;
3. Via the P2P messaging service Sue and Bob agree on a price and to trade money for the item at a meeting subject to a satisfactory inspection. They draw up a contract with these terms;
4. Bob signs the contract, authenticates with the CTS and submits the trading contract. Sue authenticates with the CTS and co-signs the contract submitted by Bob;
5. Bob and Sue meet for inspection of the item and after inspection decided to go ahead with the trade on the agreed terms;
6. Bob and Sue authenticate in turn with the CTS and co-sign trading outcome that they lodge with the CTS;
7. Bob authenticates with the CTS, is authorized to access the trading contract, and adds his reputation report on the outcome;
8. Sue authenticates with the CTS, is authorized to access the trading contract, and adds her reputation report on the outcome.

Alternative outcomes for step 5 could be that no trade is done or the trade goes ahead with an adjusted price or other altered terms. Contract adjustments would have to be jointly

Figure 1. Overall view of the P2P-CTS system
signed and lodged. Whether the trade goes ahead or not, Bob and Sue still need to provide reputation reports on each other’s behaviour.

Reputation reports stored with the CTS become a point of reference for others that might wish to trade with Bob and Sue in the future. Reputation reports deter peers from doing dodgy things as their activities will be reported and stored in the CTS which will affect their overall reputation and ability to trade in the future.

SECURITY ISSUES FOR P2P-CTS

There are several factors which create vulnerabilities to threats from attackers for P2P-CTS systems. As the CTS is stored in the cloud and accessed by the Internet, attackers can try to access the CTS and its contents from anywhere. Furthermore, there is no central authority that controls the CTS. A self-managed community system creates opportunities for attackers to blend in with the community and orchestrate actions with the intention of defrauding other peers. Decision making and rules that are made collectively by the P2P community can be subverted if malicious peers can gerrymander sufficient votes to alter membership or pervert rules to subvert fair and open trading.

What Needs to be Secured and Protected?

In the P2P-CTS, an important asset is reputation reports on prior trades which are stored in the cloud. It is valuable background for peers before engaging in any trading transaction with another peer. However, reports on a peer’s prior behaviour have to be bound with their real identity. Later, other reputation reports also have to be linked with the previous trading transactions because a reputation report cannot be made without a previous trading engagement. The reputation reports must have some sort of relation with previous trading contract and trading outcomes, as it will be meaningless without them.

The trust data items that need to be secured and protected include:

- Reputation reports;
- Identity of peers;
- Trading contracts and outcomes;
- Membership status;
- Community rules.

Trust data stored in the cloud is co-related with other data but cannot be trusted piecemeal. It has to be evaluated and cross-checked with other data before deciding to trust it as a whole.

Threat Model for P2P-CTS

We anticipate the following threats to the CTS below based on the STRIDE(Howard & LeBlanc, 2001) security model:

- **Spoofing identity**: Unauthorized use of another peer’s identity to access the CTS. Any malicious act by the attacker will be blamed on the peer whose identity is stolen. Identity spoofing can happen when security secrets such as X.509 private keys are compromised;
- **Identity churn**: To escape their poor reputations peers may acquire a new identity with no prior trading history and join as a fresh member with a novice’s presumed good trading intentions;
- **Unauthorized tampering with trust data**: Trading contracts stored on the CTS should only be able to be added, modified or deleted by the trading parties involved with their joint agreement. Any modification by anyone other than the parties involved is unauthorized modification of data in the CTS. Modification of such data by either party without the other’s consent is also unauthorized modification;
- **False repudiation**: Denial of the act of accessing or updating trust data without the CTS being able to prove the user did so. It can happen with a poorly designed or insecure logging system;
Unauthorized information disclosure: Access to data in the CTS by unauthorized parties such as non-members. It can also involve breach of privacy for peers who agreed to confidentiality about the trade;

Denial of services: Although the CTS is not meant for frequent access, it has to be available when needed. A DOS attack on the CTS could cause its unavailability to peers;

Unauthorized elevation of privileges: It could happen if peers such as the CTS founding members gain privileged access to the CTS and are able to modify any data inside the CTS. Poor design of the bootstrapping process, authentication, authorization and access control would contribute towards this threat;

Fraud Collusion: Two or more peers may collaborate to fake trades, outcomes and reputation reports to whitewash their trading histories as a prelude to cheating others;

Sybil Attack: When a peer uses multiple identities (existing identity, alternate identities and third party identities) to manipulate or modify trust data;

Man in Middle Attack: Malicious peers intercept messages between two communicating peers, modify messages and masquerade as peers to others;

Blackening reputations: By issuing false reputation reports or unauthorized modifications of existing reputations to ruin the reputation of a peer in good standing;

Whitewashing reputations: By deleting or modifying existing bad reputation reports and replacing them with good reputation reports;

Off Record Dealing: Peers may avoid acquiring a poor reputation in dodgy deals by suggesting to counterparties that recording their transactions is not worth the effort;

CTS Subversion by Cloud Hosting Service: Technical support staff of the cloud service may interfere with the operation, software or data stored in the CTS.

The possible threats might also arise from a combination of two or more of the above threats which could make it more complex to handle.

Security Requirements for P2P-CTS

Security requirements for the P2P local trading system can be distinguished into the following aspects (ITU-T, 1991):

Access control: Only members are allowed to participate in the trading forum community. Non-members are kept out from P2P-CTS community facilities;

Authorization: Membership is controlled and limited by community collective decision making;

Integrity: Trust data consistency in the CTS is preserved and protected;

Confidentiality: Trust information is protected against disclosure to unauthorized peers;

Non-repudiation: The originator of a message, trading contract or reputation report cannot credibly deny its role in its origins;

Availability: Members have access to the CTS whenever they need it.

Security Solutions to Resolve Security Issues in P2P-CTS

Proposed solutions to satisfy the security requirements of the P2P-CTS are as follows:

A mechanism is provided to securely bind a peer’s real identity with their trading identity and provide assurance of it through a digital signature. In order to record transactions during trading, outcomes of the trading, reputation reports and membership status, the peers have to bind their personal identity with the trading identity used in P2P-CTS system. The trading identity is initially established using an X.509 cer-
tificate signed by the CTS and warranted by the peer’s community sponsors. The identity of peers can also be re-verified in the same way during the meet up between the buyer and seller;

- Protecting the trust data of the system using identity credentials such as encryption with peers’ public keys or limiting access only to authorized members of the P2P-CTS. Without the trust data, the P2P-CTS will become useless in terms of securing transactions against fraud. As each trading transaction is required to be recorded, the recording helps prevent fraudulent activities by existing members who want to hide their dodgy dealing from affecting their current membership reputation;

- Securing communication among peers and the cloud using encryption. The data or messages shared, transferred and sent among these parties are digitally signed and may also use encrypted communication channels (SSL/TLS) to pass messages to ensure their confidentiality. X.509 certificates are able to fulfill these requirements;

- Transactional data in the store is jointly signed before being stored in the CTS. It will make sure that the data has integrity and is undeniable by peers that sign the trading contract or outcome report. Reputation reports by one party on another party’s trading behaviours can be individually signed. In peer community membership, community decision making decides the type of rules and their parameters to control membership creation, withdrawal and renewal and the software enforces these constraints;

- Badly behaving P2P members will be reported to the community. Cancellation and revocation of their membership could be done immediately by inserting the peer’s identity in the CTS certificate revocation list after an ad-hoc community vote. More usually it will be done by a community refusal to renew their membership when it falls due. Lack of sufficient sponsors or a sufficient weight of blackballers will ensure this. The required thresholds of each will be a community rule making matter;

- Enforcing the security of the cloud itself with a strict logging and membership system and strategies of backup and replications. The cloud that is being used to store the information has to be secure against threats and able to be accessed without disruption by peer members. Services can be unavailable because of denial of service attacks directed at the peers and the CTS. Their unavailability will discourage people from using a P2P-CTS trading system. Judicious choice of the hosting cloud service can provide reasonable protection against malicious manipulation of the CTS by their technical personnel.

Referring to Figure 2, the Community Trust Stores, Peer and Communication medium are the protected domain that needs to be secured against threat. We have identified the security requirement of each entity and we already implement security measure based on their requirement and possible threats.

**X.509 Certificate for P2P-CTS**

A self-signed X.509 certificate created by a peer applying for membership will be signed by the CTS’s private key once his sponsors have satisfied community membership proposal rules and attest to having carried out due diligence on the X.509 certificate. The certificate and private key can be readily created by users using Java keytools and openssl software. The X.509 certificate allows secure connections to be established between the peers and the cloud store using SSL/TLS with two ended authentication. It can also be used with its corresponding private key to digitally sign messages, trading contracts or reputation reports. In Figure 3, the peers’ X.509 certificate is signed by its own private key.
Figure 2. Security requirement P2P-CTS system

Figure 3. Certificate X.509 P2P-CTS system
In the public key infrastructure system, the digital signature used by the CTS to sign the peer’s certificate attests that the peer’s X.509 certificate is valid and contains correct information. This X.509 certificate signed by the CTS will attest both the peer’s identity and public key and their current membership status.

IMPLEMENTATION MODEL FOR P2P LOCAL TRADING AND COMMUNITY TRUST STORES

Peer-to-peer computing benefits local trading applications since it is cheaper to participate in compared to conventional client-server e-commerce applications. No third party service provider needs to be compensated for providing support.

The overall proposed framework for 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 sub-network infrastructure for supporting the CTS. Details of this framework are discussed in a previous paper (Fauzi & Taylor, 2011). The CTS enables peers to:

- Jointly record trading contracts with the CTS;
- Jointly add trading outcomes based on agreed contract;
- Record reputation reports on trades;
- Store data on the status of peers such as membership of the P2P-CTS systems.

In local trading, important issues are how well traders honour contracts between trading parties and how well contracts protect the interests of both parties fairly and securely. In direct selling of pre-owned 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, recommendation or testimonials from other peers that have used that kind of service from that vendor before. For example, in relation to a local cleaning service offered by a trader, other peers would expect to be able to consider feedback from peers that have used that trader’s service before agreeing to hire that cleaner. Different types of trade will have their own distinct requirements and challenges.

Cloud computing is a cheap and scalable approach to support applications like a CTS. A cloud service such as Google Cloud Storage (GCS) stores and accesses data on Google’s infrastructure combining the performance and scalability of Google’s cloud. Google Apps Engine (GAE) is a web application service provided by Google which allows the building and hosting of application on platforms provided by Google infrastructure (Fisher, Pant, & Edberg, 2010). Using applications built on the cloud provides robust and usable ways for peers to access the cloud.

Peers have public keys (Zimmerman, 1995) and CTS signed X.509 certificates to identify themselves. Peers sign their messages with their X.509 certificate as well as use them to provide secure two end authentication SSL/TLS connections with the CTS.

Bootstrapping P2P e-Commerce Community Applications

A P2P community is a group of peers with a common purpose, similarity, and interest (Vassileva, 2003). In a P2P e-commerce community of the kind we envisage, the group of peers collaboratively communicate with each other and manage their trust store to achieve the common purpose and interest of trading with each other. They have a set of policies and rules agreed by the community to ensure trading is done fairly and reasonably. The community starts with two or more peers creating a storage space in the cloud and loading the software application to manage it. Policies and rules are outlined, updated and enhanced with agreement from the two or more members which are needed to authorize them and stored in the CTS. Once the CTS is set up in the original user’s name, the
software then changes his password to a random values and encrypts it in a secure store that can only be jointly unlocked by the trustees of the CTS so that no user has privileged access to CTS operations. From then on all peers who are members are equal and changes to store data can only be made in accordance with what the software permits. Then the community can grow by inviting more peers to join the community membership with the recommendation or at the invitation of existing members. Membership must be agreed in accordance with existing community policies and rules. Membership can be revoked if an existing member breaches the policies and rules, and is voted out by a certain number of peers as outlined in the community rules.

In order to join the community, a new member has to agree to abide by existing policies and rules of the community. However, after joining, if he can gather sufficient support among other peers, it is possible for them to vote to abandon or modify existing rules, create new rules or even vote for other peers to be cast out. This problem is unavoidable in such a type of self-managed system. The design and architecture of the P2P community has to be fair to peers yet secure against threats. Peer logs not only provide evidence of good behaviour and good reputation but also evidence of malicious activities such as concerted fraud, whitewashing (Kudtarkar & Umamaheswari, 2009) and reputation blacking.

In general, free riders (Feldman, Papadimitriou, Chuang, & Stoica, 2006; Feldman & Chuang, 2005; Karakaya, Korpeoglu & Ulusoy, 2009) are a serious problem for P2P systems. In the P2P-CTS application, free riders are peers who only use existing data like contract outcomes and reputation reports in the CTS but are reluctant to contribute anything back to the CTS such as writing reputation reports or transaction outcomes after trading with other peers. Positive and negative incentives are proposed as ways to overcome the free rider’s problem. Members who fail to contribute will have their membership expired eventually for inactivity. A rule such as membership without contribution to the shared data or reputation module in a given period like three months can be expired automatically. Furthermore, the trading forum may also choose to have a policy such as to forbid private deals between members without using the P2P-CTS.

**Membership Management**

The preferred P2P-CTS membership policy is a closed membership scheme with new peer membership being based on the invitation and voting of existing members. The membership will be limited to a period such as a year and then be open to being renewed by lightweight or full procedures. Inactive membership can be expired after a shorter period such as three months. Community voting support includes:

- Creating a new member;
- Removing an existing member;
- Changing community rules;
- Renewal of membership.

A lightweight process should exist for renewal subject to the member being in good standing (i.e. low percentage of complaints among recorded trades). For example, those lacking a good reputation should need a larger amount of voting members to renew their membership. Voting rules for the P2P-CTS should specify the quorum required for a valid vote, the number of votes or proportion of membership needed and whether blackballing is allowed and by what threshold.

**Membership Expiration and Incentives**

The membership expiration rules are important in this application to encourage active contribution from peers that use the system. The disadvantages of having too many inactive members include consumption of physical space in the CTS, management burden of membership and effects on voting percentages. Membership needs to be expired after a set term to weed out
non-participants. Apart from membership expiration, in order to encourage peers to contribute and participate, incentives should be introduced for members to trade with each other.

P2P systems generally use a variety of incentives including financial rewards (Golle, Leyton-Brown, Mironov, & Lillibridge, 2001) and social recognition such as star ratings of members. P2P-CTS is different from other P2P systems such as BitTorrent. BitTorrent file sharing space encourages users to contribute by rewarding the activity (Cohen, 2003). The more a peer shares its space, the more it can download from others (Anagnostakis & Greenwald, 2004). As the space usage of the P2P-CTS is not the issue, other incentives will be used. By giving incentives, it should be possible to encourage peers to behave well in the community and deter them from doing bad things (Zghaibeh & Anagnostakis, 2007). The incentives could be limited immunity against membership exclusion or extra voting power (such as one vote that counts as two) for members who have recent trading history with good average reputation report ratings. We do not expect all P2P local trading communities will want to operate the same rules, so our implementation is designed to support a policy module which can allow each community to set its own rules to reward active and well regarded participation within the range of variation of the rules allowed by the software.

Scheme for Handling Policies and Voting in P2P-CTS

In order to create new policies, a peer has to propose the change to the community for approval and consent. One method for getting approval is by a voting process. Such a process was proposed in PeerVote (Bocek, Peric, Hecht, Hausheer, & Stiller, 2009). Although the aims of the voting process are the same, the approach for P2P-CTS will differ due to its different requirements and attributes. P2P environments create a challenge if everyone is expected to cast vote at the same time. However a voting scheme that can support a decentralized environment is possible. The CTS will play a major role as the mediator in the voting process for new policies. Below is a summary of proposed voting process for new policies:

1. Peer submits proposal for a vote to CTS signed by required number of other member;
2. CTS inform members via P2P messaging system of new policy to be voted to all members;
3. The votes are limited to two choices, either agree or disagree. Non-voting members are considered to be neutral;
4. Duration for voting such as 7 days is set to give peers enough chance to be well informed about the policy issue and to address their different online times;
5. The vote ends after the set duration or when a sufficient number of votes are reached;
6. Number of votes for endorsement or rejection of new policies is set before hand, for example, if 20% of members vote and positive votes outweigh negative by 2 to 1;
7. Peers vote by giving their choice (agree or not) signed with their digital signature to the CTS;
8. The voting can ends early if more than 50% of members vote for or against the new proposed policy;
9. If the voting duration ends and the required threshold for change are not met, the proposed new policy will be discarded as it failed to gain sufficient consent of the community members.

Reputation Report Scheme

In a P2P e-commerce community, reputation is important as it help other peer to judge the reliability and trustworthiness of a peer. If peers are highly reputable, the peer can get good feedback from others and positive testimonials from them. The reputation report scheme
includes reputation reports on previous trades, testimonials and complaints. Other peers will refer to reputation reports on previous trading deals before making any trading engagement with a peer.

Apart from the reputation report contents, other factors that might affect reputation analysis include the most recent reports and the numbers of previous transactions involved. Reputation reports may cover several factors such as the satisfaction level of participating peers, perceived trustworthiness of peers, terms fulfilled as agreed in previous agreement and additional or extra bonus items which might be included in the deals.

We would suggest that a reputation report should use a multi dimension rating scheme for a peer to rate others. The rating would then consist of marks which might be on a Likert scale such as between 0-10 and free text comments. In order to encourage peers to have good reputation community star ratings can be added to distinguish members who have passed certain limits of positive overall feedback. The reputation report can be sorted in term of total average marks, positive rates, most recent transaction and number of star recognitions. The history of activities related to reputation reports such as numbers of peers being rated or numbers of peers’ reputation report made by others. Rating activities can also show the activeness and participation of peers in writing reputation reports on others after meeting of item inspections and writing the transaction outcomes.

As summary of the overall reputation report can show the aggregated trustworthiness of a peer. Two major problems with reputation systems are reputation whitewashing; where peers tries to use illegitimate ways to improve reputation such as by deleting or blocking bad reputation reports and reputation blackening, where peers try to ruin the good reputation of another peer by submitting unfair bad reputation report of the peer. This is a challenge that needs consideration in the design of the P2P-CTS including ways to protect the integrity of reputation reports by hardening the modification process and enforcing access control to updates and submission of reputation reports.

Related Works

Several advanced approaches have been suggested regarding how to evaluate trust based on the reputation of peers (Houser & Wooders, 2006; Teacy, Patel, Jennings, & Luck, 2006; Resnick & Zeckhauser, 2002; Regan, Poupart & Cohen, 2006; Khosravifar, Gomrokchi, Bentahar & Thiran, 2009; Zhang & Cohen, 2008; Fang, Zhang, Sensoy, & Thalmann, 2011. These approaches have several weaknesses and challenges. However, most of the proposed reputation systems have limited dimensions which are unable to evaluate and qualify a peers’ reputation adequately. Too many dimensions also create another problem of too much data to key-in and different ways of aggregating reputation data which might be too complicated for a P2P trading system.

Existing reputation report systems also assume that the peer’s feedback is always honest and non-biased. However, there is always the possibility that although a transaction went well between peers, a peer still can get a low rating from others which doesn’t reflect the real nature of transactions. There is also the possibility that good peers can be maliciously rated badly by a peer in order to ruin the peer’s reputation. It is an issue of the credibility of the feedback given by the peers. For example, how do we deal with trusting reputation reports given by a peer who has previously had dodgy trading transactions and bad reputation records.

The storage of the system is an issue regarding its security and the accessibility of the reputation information. Using a cloud as storage to store trust data also creates challenges of its own. There are cloud based products such as Dropbox and Google Cloud. There are also P2P storage alternatives such as Wuala, PeerStore (Landers, Zhang, & Tan, 2004) and OceanStore (Kubiatowicz et al., 2000). For our prototype
system, selection of the cloud provider is based on their well known reputation, wide accessibility and minimal subscription cost.

In our approach, there is no single controller or single super user of the cloud account. The cloud is publicly available and accessible to community member which is the main reason for using the cloud to allow accessibility to the trust data stored in it. By using existing cloud products peers we do not need to worry on how to setup the cloud. The main concerns are related to how control of the information stored in the cloud is determined by the provider.

**DISCUSSION AND FUTURE WORK**

There are several key features which differentiate the P2P-CTS compared to other client-server e-commerce application which include:

- P2P rather than a client-server approach;
- Decentralized distributed management rather than management of trusted third party;
- Policy and rules proposed by peers and agreed by the community;
- Membership used to limit access to more trustworthy parties;
- Joint signing and storage of trading outcomes;
- Dynamicity, evolutionary, changeability and expandability of overall operations;
- Using cloud service as the trust data storage platform;
- Using CTS as a virtual trusted third party.

The P2P-CTS applications framework is being implemented on a third party platform so that it can be purely managed by the peers. The third party platform is unable to control the internal management of the CTS as it is only being used as the hosting platform of the CTS. The implementation success depends on the peers and whether they endorse the functionality and strength of the security mechanisms put in place. We intend to calculate and measure that assurance using methods like voting. The same goes with trust in the use of P2P-CTS stored reputation reports or recommendations by peers. The number of votes and ratings awarded by the peers can be aggregated to assess community opinion on the P2P-CTS system.

With transparent logging in the CTS, evidence can be followed and traced until the source of any issues is revealed. Peers can independently check the evidence and make their own decisions based on their findings. Reporting on the outcomes of transactions and reputation reports are one of the key factors for the implementation. Issues such as misleading wording, improper categorization of ratings, misinterpretation of comments, accidental and unintentional grading are human factors that might affect the P2P-CTS application outcomes apart from the protection mechanisms of the CTS. It can be improved as part of further enhancement for the P2P-CTS application. The P2P-CTS design includes support for convenient Public Key Infrastructure (PKI) and X.509 certificate generation. The CTS will also have its own private keys and self-signed X.509 certificate. All transactions with the CTS take place via SSL/TLS with two ended authentication by using X.509 certificates. In the near future, the P2P-CTS prototype will be validated with a series of tests to prove its viability to support local P2P trading.

**Contribution to the Area**

The contribution of this research to the area includes providing an economical and effective solution towards supporting peer-to-peer e-commerce without relying on centralized servers. The updates of communal related 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 required sponsors. Identity certificates can be limited
to being added jointly by all their signatories who are group members. Other trust data such as reputation report 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 verified by his digital identity.

**Impact for Business and Entrepreneurship**

With this cheaper solution to operate trading within the community and being managed collectively among the trading parties, business can runs of a bigger scale with a lower operational cost. The security measure implemented protect peers from being manipulated and taken advantage from as the trading members are being rated and evaluated by each other based on their behaviour and reputation. Jointly sponsored membership scheme also ensure only chosen and highly rated peers are accepted into the P2P e-commerce group. Jointly dismissal of existing member ensures fairness and prevents misuse of single authority decision.

**Prototype**

This system prototype is developed with open source application development model. The contribution and feedback from open source community members ensures transparency and integrity of the code. We also emphasized that this system is also communally managed and trading model is operated within the closed community group. It is economically viable and cheaper to run within the community and much more scalable in term of increasing trading members.

**CONCLUSION**

From the list of threats which would be encountered by a CTS, suitable security strategies has been outlined which are able to protect the contents of the community trust store and provide reliable access to it. Apart from protecting the contents in the CTS, this research also outlined the methods being employed to protect the identity of the CTS itself. It has been described as well regarding the peer access to the CTS service and how threats should be handled. Although the P2P-CTS are hosted by cloud services, it is still managed and monitored collectively by the participating peers’ community members. Monitoring changes in the P2P-CTS by the peers for unusual patterns will be a key part of collaborative efforts towards ensuring the security of the CTS. Community assurances by the peer’s community underpin use of the P2P-CTS. Collective and collaborative decisions and actions to overcome problems and administer issues related to the CTS will ensure increase trust and confidence towards use of the application.

However, all the trust data stored in the cloud is co-related with each other and should not be trusted as one single entity. It has to be hierarchically evaluated and checked before deciding to trust it. In conclusion, security requirements and an overall design for a Cloud based Community Trust Stores for local P2P e-commerce has been explained. These security requirements can be added, modified, removed and changed according to the rules agreed by the peer community. The framework used for developing and implementing this P2P e-commerce application supports community based management scheme, provides threats identification and handling, scalable information service and secure methods for data storage in the cloud.

**REFERENCES**


Hamish Taylor is a lecturer in Computer Science at Heriot-Watt University in Edinburgh. Prior to that he worked as a research assistant at QMW in London formalizing automated reasoning and before that at Heriot-Watt on implementing parallel logic programming languages. He holds an MA and MLitt from Cambridge University in Philosophy and an MSc and PhD in Computer Science from Heriot-Watt University. He lectures on distributed systems, network applications and Internet technologies. He has held research grants on modelling parallel databases, visualising web data from shared caches and intelligent information discovery. His current research interests are in the design of distributed systems especially peer to peer architectures and ad hoc networked applications.

Ahmad H. Fauzi is a lecturer at Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak, Malaysia. He holds Bachelor Degree in Computer Science from University Technology Malaysia, Malaysia and Master in Network Computing, Monash University, Melbourne, Australia. Currently he is pursuing his PhD at Heriot-Watt University, Edinburgh, United Kingdom. His current research interest covers from secure peer-to-peer application, P2P e-commerce and cloud computing.