Using the Wisdom of Crowds to Prevent Internet Frauds

Hai-Tao Zheng, Yong Jiang, and Lei Zhang
Tsinghua-Southampton Web Science Laboratory at Shenzhen, Graduate School at Shenzhen,
Tsinghua University, China
{zheng.haitao,jiangy, zhanglei}@sz.tsinghua.edu.cn

ABSTRACT

With the rapid growth of the netizen population in China, more and more internet frauds are committed. Many people suffer from internet frauds by losing wealth or other valuable things. To prevent internet frauds, we first need to discover the methods in which internet frauds are conducted. In this paper, we investigate and categorize the internet frauds in China. So far, there are typically six kinds of internet frauds, including email fraud, website fraud, e-commerce fraud, virus fraud, password fraud, and message fraud. To prevent these internet frauds, many approaches, such as intrusion detection and access control, have been proposed to help users. However, most of these methods are limited to detecting a small volume of internet frauds. To address this issue, we propose a methodology to use the wisdom of crowds, with the help of Semantic Web and Web 2.0 technologies, to detect a large volume of internet frauds. The proposed framework is composed of eight modules: internet fraud report module, key element extraction module, linked data generation module, linked data repository, query interface, query interpretation module, SPARQL module, and answer generation module. Based on the framework, users are able to input the internet fraud reports in a controlled natural language. The internet fraud reports are converted into linked data automatically. Then, the users can query the linked data in a semantic fashion. A case study and a survey preliminarily indicate that the proposed method is able to help users share and identify the internet frauds effectively.

Keywords

Internet Fraud, Wisdom of Crowd, Semantic Web, Linked Data, Controlled Natural Language

1. INTRODUCTION

The number of netizens in China has reached 384 millions by 2009, making it the largest in the world. As shown in Figure 1, the number of internet frauds has increased to more than 13,000 on July, 2009 [15]. With the rapid growth of the netizen population in China, frauds on the internet are continuously increasing. Many people suffer from the internet frauds by losing wealth or other valuable things. Since internet frauds are becoming rampant, many methods are proposed to prevent internet frauds. Most of the methods suggest people to be cautious of various internet frauds based on the social scientific perspective. These methods analyze the behavior of swindlers to help people better understand how the swindlers work and what actions might be taken by users [5, 6, 9, 13]. However, these methods do not provide any system to aid users in avoiding the trap of internet frauds.

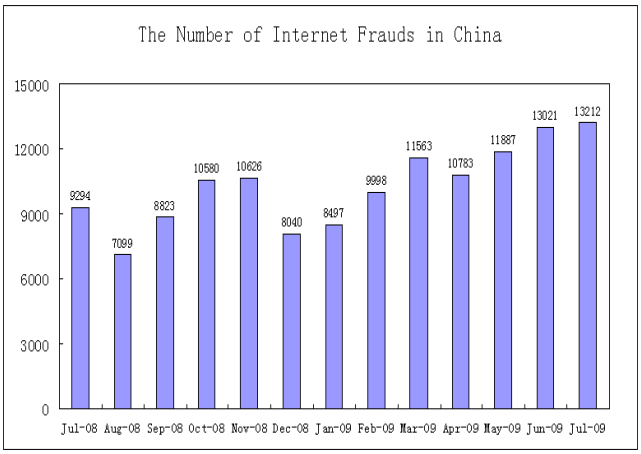

Figure 1: The number of internet frauds in China

To develop the system for supporting users to detect internet frauds, a number of approaches have been developed based on the computer scientific point of view. Most of the approaches use computer security techniques, such as intrusion detection and access control, to prevent the internet frauds [1, 2, 3, 17, 29]. Since the methods of internet frauds are changing constantly, it is hard to develop algorithms to identify these methods although numerous intelligent computing techniques are developed. Therefore, the existing computer security techniques are limited to detecting a small volume of internet frauds. To move a forward step for detecting and preventing a large volume of internet frauds, we believe that it should neither merely rely on the users' effort, nor merely lean upon the computer systems. On the contrary, we think that it should combine the power of human users and computer intelligence to prevent internet frauds.

The phrases "wisdom of crowds" or "collective intelligence" refer to the value created by the collective contributions of all the people writing articles, publishing photos or

Web Science Conf. 2010, April 26-27, 2010, Raleigh, NC, USA.

videos, tagging articles or photos into the open seas of social web. As the Web 2.0 and Semantic Web matures, numerous paradigms indicate the power of the wisdom of crowds. They include Wikipedia [27], MySpace [20], Facebook [10], YouTube [28], Flickr [11], Del.icio.us [8], and DBpedia [7] etc. The potential for knowledge sharing is so huge that we cannot imagine. However, there are few studies using the wisdom of crowds to prevent internet frauds. To address this issue, we proposed a framework to tag into the power of collective intelligence for detecting and preventing internet frauds.

In this paper, we firstly investigate the current status of the internet frauds in China. Based on the investigation, we categorize the methods in which internet frauds are conducted to help people better understand the characteristics of the internet frauds in China. Afterwards, we focus on developing a framework that uses the wisdom of crowds to discover large-scale internet frauds. Based on the proposed framework, users are able to share the internet fraud information with others. The shared information is processed into a computer understandable format, i.e., Semantic Web files. With Semantic Web files, machines are able to process the shared information in a deep level, such as reasoning, semantic search, and data mining etc. In addition, users can query the shared information to identify the internet frauds they might encounter. To build the framework, we develop the modules that support users to share the internet fraud information as Semantic Web files as well as query this information in a natural way. The main contribution of the paper includes:

1. We investigate and categorize the internet frauds in China to help people better comprehend the features of the internet frauds in China.

2. We develop a framework that uses the wisdom of crowds to collect the information about the internet frauds and translate it into a machine understandable format.

3. We develop a system that utilizes the collected information to enable users to query and identify the internet frauds.

The rest of the study is organized as follows: Section 2 gives the overview of the internet fraud methods in China; Section 3 elaborates the proposed methodology including the linked data generation, query processing, and answer generation; We describe a case study to evaluate the effectiveness of the framework in section 4; Section 5 utilizes a survey to analyze the necessity, the usability, and the limitation of the proposed method; Section 6 reviews the related work and section 7 gives the conclusion with a discussion of future works.

2. OVERVIEW

In China, the term "internet fishing" refers to using deceitful emails, websites or other information to obtain peoples' financial information for stealing their money. According to the official statistics in 2009, among the cases of internet frauds, internet fishing cases are over 90%. Based on our investigation, there are mainly six kinds of approaches to conducting internet fishing:

1. Sending fraudulent email to bring people to the lure. On one hand, the emails sent by the perpetrators tempt people to input their bank accounts and passwords by telling them they are winning a prize in a lottery or other deceitful reasons. On the other hand, these emails use some emergent reasons to ask the recipients to access websites and submit their personal information, such as identity card number, credit card number, bank account, and so on. Then, the perpetrators are able to use the personal information to purloin users' money.

2. Establishing fake websites to defraud people of bank accounts and passwords. First, the perpetrators simulate the real internet bank system or the internet securities trading platform to build similar websites. The fake websites generally have very similar URLs to those of the real websites. When the users access these website to process their financial transaction, their financial information will be stolen.

3. Using e-commerce for defrauding. Perpetrators in well-known e-commerce websites fabricate information into the so-called "super cheap", "duty free", "contraband good", and "charity" as the name of selling goods to require payment. There are typically four kinds of scams in e-commerce frauds:

1) Network transaction prices of goods provided by swindlers are often lower than the market price by more than half. The swindlers use "smuggled goods confiscated by Customs, gifts given by friends" as the reasons to obtain the purchasers' trust. When the consumers buy the goods, they will find the quality of those goods to be much worse than the real goods. Sometimes, the goods sold by the swindlers are good at the beginning, but after some time, they will easily malfunction.

2) Some illegal websites use prizes to lure consumers to browse the web, and buy goods. There are points in exchange for the use of gifts or prizes to attract consumers. The consumers need to register for websites, visit some websites, or introduce other buyers to obtain the points. However, any prizes still require money to buy.

3) Product descriptions offered by some websites are exaggerated or even false propaganda. When the consumers enter these websites and purchase the goods, they will find that the physical goods are different from the on-line pictures, or even worse than the product descriptions. In many cases, a number of online shops were closed after the money was cheated. Then, the swindlers open a new online store to conduct the same tricks.

4) Some websites use special contracts, which do not mention any guarantees for the quality of goods, to conduct transactions with consumers. When consumers buy a product that has quality problems, they can neither return the product nor have the product repaired.

4. Using "trojan horse" or "hacker" technology to steal user information. In the emails sent by the perpetrators or on some websites, there are hidden "trojan horse" programs. The users' computers easily get infected by opening these emails or accessing the evil websites. When the users have any on-line transaction on the infected computer, the "trojan horse" program will record the keys that were pressed and obtain the users' bank accounts and passwords.

5. Cracking users' "weak passwords" to steal money. Some users set up relatively simple passwords called "weak passwords" for their bank accounts for the sake of convenience. Perpetrators search those users' bank accounts using search engines and utilize many cracking tools to crack these "weak passwords". Consequently, the perpetrators login to the users' internet bank accounts and purloin their money.

6. Mobile phone text message scam. Perpetrators use a computer that stores millions of mobile phone numbers to

send many fraudulent messages to trick users. The messages contain the information such as "hit the jackpot", "rebate", or "investment advice" in order to tempt users to remit the money, transfer the money, or conduct other operations that make them lose their wealth.

The methods for conducting internet frauds are getting more spurious and there is no regular pattern to discover them. Therefore, it is very difficult for individuals to judge whether or not they encounter a fraud. To address this issue, we build a framework that uses the wisdom of crowds to enable knowledge sharing. With the shared knowledge, we believe that individuals are able to identify internet frauds more easily and more quickly.

3. METHODOLOGY

The key idea of our method is to provide a simple interface helping users share internet frauds they know and identify the internet frauds by querying the system. The Semantic Web and Web 2.0 techniques are used to to build the framework. Figure 2 depicts the framework of our method. There are mainly eight modules composing the framework:

- Internet fraud report module;
- Key element extraction module;
- Linked data generation module;
- Linked data repository;
- Query interface;
- Query interpretation module;
- SPARQL module;
- And answer generation module.

As shown in Figure 2, the eight modules cooperate to provide a full service for users to share and use the information of internet frauds. First, users report the internet frauds with a controlled natural language [19], which is a subset of natural languages; Based on the grammar of the controlled natural language, the key element extraction module utilizes regular expressions to extract the information from the reports. The key elements include the subjects that conducted the internet fraud, the actions indicating how the internet frauds are conducted, the places and the time on which the internet frauds happened. Note that it is not necessary that the reports contain all the elements. If some elements are missing, we use null values to indicate that. Then, the linked data generation module uses the extracted key elements to compose the triples, i.e., subject, predicate, and object. All the constructed triples are stored in a RDF (resource description framework) file. RDF provides interoperability between applications that exchange machine-understandable information on the Web [22]. The RDF file is collected into a linked data repository. The linked data repository indexes the RDF data and supports the semantic query for the RDF data.

Next, users are able to query the internet frauds through the query interface. The query interface also uses a controlled natural language to reduce the ambiguity of the query. The query interpretation module processes the query into the SPARQL language, which is a query language for RDF [24]. Then the SPARQL module uses the SPARQL query to access the linked data repository. The query result is processed by the answer generation module to propose users an understandable answer.

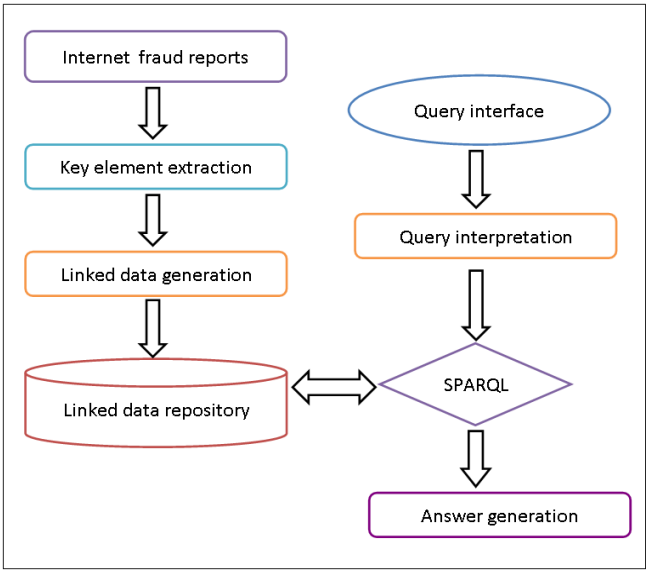

Figure 2: Framework of the proposed method

3.1 Internet fraud report

To enable users report the internet frauds easily, we build a microblogging interface like Twitter [26]. The interface is simple for users to report internet frauds using not only computers, but also mobile phones. However, in order to enable reliable automatic semantic analysis of the internet fraud reports, we restrict the grammar of the reports. Considering the way to represent most of the internet frauds, we restrict the format of the reports as follows:

- "Subject" with "Value" do "Action" at "Place" on "Time" .

Although the format is not the syntax of natural language, it is quite intuitive for understanding. The report is represented as the *subject* (email, website, or people etc.) having the *value* (URL, email address, or person name etc.) conduct the *action* to commit an internet fraud at some *place* on some *time*. We use a simple example to illustrate our method: a user wants to report a false website for the bank of China, which has URL http://www.bank-off-china.com/ and has been established from 2003 to the present. Then, the user can input the report as follows:

- "Website with http://www.bank-off-china.com/ do false website for the bank of China at null on 2003-now".

If there is no information about some field in the report, the user can use a null value to fill the corresponding field. For example, since there is no *place* information in the report, the user can use a null value to fill the *place* field.

Note that although it is more easy for users to input the internet fraud reports using natural language, the processing of natural language increases the complexity and uncertainty of the system. The complexity increases because we need to additionally employ a number of preprocessing modules,

such as tokenization, Part-Of-Speech tagging, and stemming etc., to conduct the natural language processing. The uncertainty increases because the expression of natural language is so varied that it is very hard for computers to catch the semantics exactly. Since the reports are restricted to the internet fraud domain, it is not difficult for users to make the reports using controlled natural language. We also consulted 20 users randomly to ask them whether or not they would like to report the internet frauds using controlled natural language, 17 of them agreed to use the controlled natural language to input the internet fraud reports. The survey verifies that users accept constructing the internet fraud reports using controlled natural language. Therefore, we use a controlled natural language as the input language to achieve a tradeoff between understandability and complexity.

3.2 Key element extraction and linked data generation

To compose the linked data that represents the semantics of the internet fraud reports, we firstly need to extract the key elements from the reports. The key elements include the subjects that conducted the internet fraud, the actions indicating how the internet frauds are conducted, the places and the time on which the internet frauds happened. In this study, we use a regular expression to make the information extraction pattern as follows:

- (Subject)∗'with' (Value)∗'do' (Action)∗'at' (Place) ∗'on' (Time)∗.

We use the pattern on the above example and get the five key elements: "Website", "http://www.bank-off-china.com/", "false website for the bank of China", "null", "2003-now", respectively. Note that if some elements are missing, we use null values to indicate that.

To generate the RDF data as linked data for internet fraud reports, we first define the name space and property. We primarily define the "subject", "value", "action", "place", and "time" as the properties of the RDF data. Then we use Jena [18] to develop the program to automatically generate the RDF data with the extracted elements. Jena provides an API to extract data from and write to RDF graphs. For the example we used, the RDF data is generated as follows:

```
<?xml version="1.0"?>
<rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/
22-rdf-syntax-ns#"
 xmlns:fraud="http://www.tsinghua.edu.cn/2010/
 report/fraud#">

 <fraud:Website rdf:ID="FlaseSite1">
    <fraud:subject>
    website
    </fraud:subject>
    <fraud:value>
    http://www.bank-off-china.com/
    </fraud:value>
    <fraud:action>
    false website for the bank of China
    </fraud:action>
    <fraud:place> </fraud:place>
    <fraud:time> 2003-now </fraud:time>
 </fraud:Website>
</rdf:RDF>
```

Note that if some elements have null values, the corresponding field in the RDF will be empty. With the RDF data, we are able to develop many algorithms to mine the semantic relations between the reports and discover the internet fraud patterns.

Finally, we use Sesame [23] as the linked data storage to save the generated RDF data. Sesame is an open source Java framework for storing, querying and reasoning with RDF and RDF Schema. Since the RDF data is indexed by Sesame, we can use SPARQL to query the RDF data. Compared to the traditional relational databases, Sesame allows us to make SPARQL to query the RDF data more semantically as well as discover the semantic relations between objects more easily.

3.3 Query interpretation and answer generation

In the query interface, we also use a controlled natural language as the query language for reliable semantic processing. Considering the query that the user may use, we restrict four formats of queries as follows:

- What is the value of "subject" doing "action" at "place" on "time"?
- When does "subject" do "action" at "place"?
- Where does "subject do "action" on "time"?
- What "action" is done by "subject" at "place" on "time" ?

The "suject" refers to the agent (email, website, or people etc.) that conducts internet frauds. The query is composed based on the "subject". In this study, four patterns are proposed to query the information of the "subject". The four patterns are used to query the "value", the "place", the "time", and the "action" respectively, which are related to the "subject" about which the user concerns.

For example, a user may want to know which website is a false website for the bank of China. He/she can compose the query as follows:

- What is the value of website doing false website for the bank of China?

Note that if some information is missing, the user do not need to specify the information in the query. The system can still process the query by skipping the corresponding fields.

To interpret the query, first, we develop four regular expressions as follows:

- 'What is the value of' (Subject)∗'doing' (Action)∗'at' (Place)∗'on' (Time)∗?
- 'When does' (Subject)∗'do' (Action)∗'at' (Place)∗?
- 'Where does' (Subject)∗'do' (Action)∗'on' (Time)∗?
- 'What' (Action)∗'is done by' (Subject)∗'at' (Place)∗'on' (Time)∗?

With the four regular expression, the system can extract the elements to compose the SPARQL query automatically. For example, the above query is processed by the first pattern. Then, the "subject" is website, the "action" is "false

website for the bank of China", the "place" and "time" are null values. Based on these elements, the system generates the SPARQL query as follows:

```
PREFIX fraud:<http://www.tsinghua.edu.cn/2010
/report/fraud>
SELECT ?value
WHERE
 { ?x fraud:subject "website"
   ?x fraud:value ?value
   ?x fraud:action "false website
   for the bank of China"
  }.
```

The SPARQL module uses SPARQL to query the RDF database in the linked data repository, Sesame. As a result, the URL "http://www.bank-off-china.com/" is returned as the value of the "website".

Note that the "action" expressions may have similar meanings in various forms input by users. We develop a module to extract the keywords in the "action" expressions in order to enable the system to identify similar "action" expressions. Since the "action" expressions generally are composed of one sentence, we simply use the CRFTagger [21] to conduct POS (Part-Of-Speech) tagging on the sentence and extract the nouns as keywords. CRFTagger is a java-based conditional random fields POS Tagger for English. In this way, the system is able to retrieve more results based on fuzzy matching. Although the precision declines, the recall of the system is improved. We leverage the precision and the recall to achieve a tradeoff.

To improve the understandability of the system, we develop the answer generation module to construct the sentence in a restricted grammar. Since the answers are closely related to the queries, we make the corresponding pattern to compose answers as follows:

- The "Subject" with value "Value" doing "Action" at "Place" on "Time".

For the example we used, the answer is generated as follows:

- The website with value http://www.bank-off-china.com/ doing false website for the bank of China.

We can see that although the answer is not natural language, it is intuitive and easy for understanding. In addition, since we do not employ any complicated module to process the query and the answer, the whole process of query interpretation and answer generation is quite fast, which ensures the scalability of our method.

4. A CASE STUDY

In this section, we conduct a case study to illustrate the effectiveness of our system. Let's consider a scenario as follows:

SCENARIO 1. *Since it is cheaper and more convenient for users to buy the flight tickets through travel websites nowadays, a user wants to book a ticket from Shanghai to Beijing through the web. However, he/she find that it is too many travel websites and some of these websites provide the unbelievable low prices of the tickets. The user wants to buy a cheap ticket but he/she worry about being cheating. Therefore, the user needs to detect the vicious websites in order to avoid being cheated.*

In this scenario, the user want to detect the vicious websites to help him/her make a decision for buying a ticket. Since there are too many travel websites, it is very time-consuming and labor-intensive to check all the travel website and identify whether or not the websites are vicious. Therefore, the user wants to use our system to query all the vicious travel websites and exclude them from the list.

First, the user can construct the query as follows:

- What is the value of website doing false website for traveling?

Based on the query, our system automatically use the pattern "'What is the value of' (Subject)∗'doing' (Action)∗'at' (Place)∗'on' (Time)∗?" to extract the key elements. Consequently, the "subject" is website, the "action" is "false website for traveling", and the "place" and the "time" have null values. Next, the SPARQL is composed by the query interpretation module as follows:

```
PREFIX fraud:<http://www.tsinghua.edu.cn/2010
/report/fraud>
SELECT ?value
WHERE
 { ?x fraud:subject "website"
   ?x fraud:value ?value
   ?x fraud:action "false website for traveling"
  }.
```

The SPARQL is used the query the internet report database in Sesame. As a result, a number of URL "http://www.allyou.cn/", "http://www.fei-na.com/", "http://www.51taopiao.com/", and "http://www.leyoutour.com/" etc. are returned. Next, the answer generation module construct the answers based on the returned values as follows:

- The website with value http://www.allyou.cn/ doing false website for traveling.
- The website with value http://www.fei-na.com/ doing false website for traveling.
- The website with value http://www.51taopiao.com/ doing false website for traveling.
- The website with value http://www.leyoutour.com/ doing false website for traveling.

Finally, the user can easily exclude the false traveling websites and choose the suitable website to book an air ticket. The response time is about 0.2 second, which indicates that our system has relative high efficiency. To verify the correctness of the answers, we manually search google [14] and check whether or not these websites are vicious. We surprisingly find that all these websites are reported in different public forums that they have fraudulent behaviors or low quality of service. Therefore, we believe that the answers generated by our system definitely help the user to avoid financial losses and save the precious time. The case study partially indicates the usability of our method.

5. ANALYSIS

To evaluate the effectiveness of the proposed method, we should perform comprehensive experiments. However, we found that there is no standard answer set for internet frauds. The proposed system also does not have many users because its setup time is short. Therefore, we use a case study to partially prove the validity of the system. Based on the case study, we can see the system is able to help users identify internet frauds. In addition, the response time is very short, which indicates the system has relative high scalability. However, the precision and the recall of the answers rely on the quantity and quality of the internet fraud reports. In future work, we plan to develop a mechanism to improve the quantity of the internet fraud reports and check the quality of internet fraud reports.

In order to evaluate our method from the the users' point of views, we make a simple survey that mainly includes several questions as follows:

- Have you ever suffered from internet frauds? (Yes or NO)
- Do you think it is necessary or not to build an internet fraud report platform? (Yes or NO)
- Have you ever tried to detect internet frauds? (Yes or NO)
- Are you willing to report internet frauds? (Yes or NO)
- Can you accept using a controlled natural language to report the internet frauds? (Yes or NO)
- Will you use an application to query information about internet frauds? (Yes or NO)
- Can you accept using a controlled natural language to query the internet frauds? (Yes or NO)
- Can you understand the answers written in the controlled natural language? (Yes or NO)

Although the survey is simple, it can evaluate the usability of our system because the system is built based on the wisdom of crowds. In addition, the simple survey does not require much time to finish so that more users would be able to take the survey. We use this survey to ask 50 users randomly, including students, teachers, and engineers etc.

The result of the survey is that: 45 users had suffered from internet frauds; 50 users thought it necessary to build an internet fraud report platform; 38 users had tried to detect internet frauds; 34 users were willing to report the internet frauds; 33 users could accept using a controlled natural language to report the internet frauds; 46 users wanted to use an application to query the information about internet frauds; 42 users could accept using a controlled natural language to query the internet frauds; 45 users could understand the answers written in the controlled natural language.

This survey is a preliminary evaluation of our method from the users' perspectives. The survey can not prove the efficacy of our method logically because of the small sample number, but it does show that: 1. most netizens suffer from internet frauds; 2. the necessity for building an internet fraud report platform is very high; 3. more than half of users are willing to report internet frauds in a controlled natural language; 4. a system is useful to provide a service of querying information about internet frauds; 5. most users are willing to query internet frauds in a controlled natural language; 6. the answers written in the controlled natural language are understandable.

One limitation of our method is that the usability depends on the quantity and quality of the users' reports. When more and more users start using our system, the power of the system increases exponentially. When the linked data reaches a certain scale, many data mining techniques can be used to discover internet fraud patterns. The quality of the users' reports is also important. If some reports are false, the answers including these reports will become an "internet fraud" for the users who conducted the corresponding queries. Therefore, if the quantity or the quality of the users' reports are low, our system will show poor performance.

6. RELATED WORK

In the social science domain, there is numerous research on how to prevent internet frauds. Burns et al. [5] provided information from law enforcement agencies on their general level of preparedness to address internet frauds. In this paper, four aspects of law enforcement were addressed: (1) preparedness to enforce internet fraud crimes; (2) perceptions of internet fraud; (3) cooperative policing efforts; and (4) internet fraud information dissemination practices. Rusch et al. [25] gave an overview of internet fraud and suggested that enterprises should treat information security as a business issue for preventing internet frauds. Chua et al. [6] employed the 'parasite' metaphor as a way of building theory about internet auction fraud. The paper then introduced three theories from the parasitism literature and demonstrate the insights these theories can produce. The first theory, the competitive exclusion principle, highlights how separate auction markets evolve their own species or types of fraud. The second theory details various parasite infection mechanisms to show that on-line fraud is composed of two processes; the actual deception and escape. Finally, virulence theory provides one way to predict how much harm a particular kind of fraud will cause to an individual victim. Furnell [12] listed the examples of threats facing end-users and proposed the key issues that end-users ought to know beyond the mere existence of the threats. Baker et al. [4] examined the questions of crime, fraud and deceit on the internet and discusses whether such activities constitute a new type of abusive social behavior, or whether they are classic forms of capitalistic excess appearing in a new medium. Jenamani et al. [16] conducted theoretical studies as well as simulation experiments to find out the effect of cheating in three important types of auctions: English auction, first-price sealed-bid, and second-price sealed-bid auction. Gavish et al. [13] employed a variety of methods to undertake an exploratory investigation of internet aution fraud. Dinev [9] discussed how spoof frauds cause significant business, personal, and social damage and proposed two major fronts in the fight against spoofing: increased public awareness and research into new technologies that help consumers identify spoof sites. However, while these methods are proposed to help users analyze the internet frauds, they do not focused on developing a system to help users more easily identify the internet frauds.

In the computer science domain, a number of studies on internet frauds have been conducted. To prevent internet auction frauds, Antony et al. [1] identified factors that affect

the behavior of buyers in an online auction market who had to either adopt or not adopt online escrow services (OES). An experimental C2C auction system with embedded decision support features was used to collect data. Results show that market factors, such as fraud rate, product price, and seller's reputations are important in determining buyers' OES adoption. Ba et al. [3] used a game theoretic approach to propose a design of an economic incentive mechanism, the trusted third party (TTP), to serve the online auction communities. The proposed model addressed both the economic and technological aspects of online auction transactions by assigning a digital certificate to each participant. Ba also [2] used a prescriptive approach to analyze how a certain social structurea community responsibility system, supported by present technology, can be set up. In addition, the paper used game theoretic tools to prove that under the community responsibility system for trust building, online transactions that are impersonal can be supported and can preserve at the same time anonymity to a large extent. Kim et al. [17] examined the effects of an educational intervention designed to increase consumer's knowledge, of security and privacy aspect of business-to-consumer (B2C) e-commerce websites and assurance seal services. Zhang et al. [29] discussed payment choices made by trading partners based on risk, convenience and cost dimensions. Then, the paper analyzed how product attributes, traders' characteristics, and payment attributes affect payment choice. Differing from these methods' aim at developing decision support systems, our method is proposed to use the power of collective intelligence to prevent internet frauds. To the best of our knowledge, this study has not been researched in detail.

7. CONCLUSION

The paper investigates internet frauds in China and categorizes the methods that internet frauds utilize. A so-called "internet fishing" method occupies more than 90% internet frauds in China. We analyzed how the internet fishing methods is conducted. Based on the analysis, we proposed a method to use the wisdom of crowds to help users easily and precisely identify the internet frauds. The method employs the Semantic Web and Web 2.0 technologies to build a system that automatically generates linked data based on internet fraud reports. In addition, the system enables users to use a controlled natural language to query the internet frauds. The proposed system is able to use the query to automatically construct the SPARQL query and retrieve information about the related internet frauds. Finally, our system generates the answers in a controlled natural language in an automatic fashion. To evaluate the effectiveness of the proposed method, we performed a case study and gave a simple survey. The case study and the survey indicate that our system is able to help users to detect internet frauds. Therefore, we believe that the proposed method will play an important role giving full play to collective intelligence to prevent internet frauds.

Since the usability of the proposed method relies on the "wisdom of crowds", that is, the quantity and quality of the users' reports, we should not only develop algorithms to improve the effectiveness of the system, but also develop the mechanism that motivates users to use the system in the future. In addition, we will develop a mechanism to identify the quality of the users' reports by considering the reputation of the users. We have planned to collect more large-scale datasets to perform the experiments to evaluate the system comprehensively. Finally, we will consult the users to gauge how our method can best be used to support them to share and identify the internet frauds.

Acknowledgements

This research is supported by the seed fund of Graduate School at Shenzhen, Tsinghua University. We thank Charles Borchert for his helpful English revision. We also thank the anonymous reviewers whose comments and suggestions led us improve significantly the paper.

8. REFERENCES

[1] S. Antony, Z. Lin, and B. Xu. Determinants of escrow service adoption in consumer-to-consumer online auction market: An experimental study. *Decision Support Systems*, 42(3):1889 – 1900, 2006.

[2] S. Ba. Establishing online trust through a community responsibility system. *Decision Support Systems*, 31(3):323 – 336, 2001.

[3] S. Ba, A. B. Whinston, and H. Zhang. Building trust in online auction markets through an economic incentive mechanism. *Decision Support Systems*, 35(3):273 – 286, 2003.

[4] C. R. Baker. Crime, fraud and deceit on the internet: is there hyperreality in cyberspace? *Critical Perspectives on Accounting*, 13(1):1 – 15, 2002.

[5] R. G. Burns, K. H. Whitworth, and C. Y. Thompson. Assessing law enforcement preparedness to address internet fraud. *Journal of Criminal Justice*, 32(5):477 – 493, 2004.

[6] C. E. H. Chua and J. Wareham. Parasitism and internet auction fraud: An exploration. *Information and Organization*, 18(4):303 – 333, 2008.

[7] *Dbpedia*. http://dbpedia.org/.

[8] *Del.icio.us*. http://delicious.com/.

[9] T. Dinev. Why spoofing is serious internet fraud. *Commun. ACM*, 49(10):76–82, 2006.

[10] *Facebook*. http://www.facebook.com/.

[11] *Flickr*. http://www.flickr.com/.

[12] S. Furnell. Internet threats to end-users: Hunting easy prey. *Network Security*, 2005(7):5 – 9, 2005.

[13] B. Gavish and C. L. Tucci. Reducing internet auction fraud. *Commun. ACM*, 51(5):89–97, 2008.

[14] *Google*. http://www.google.com/.

[15] *Internet Frauds in China*. http://www.chinawe.net/html/buxian/rjdt/20090929_171486.htr

[16] M. Jenamani, Y. Zhong, and B. Bhargava. Cheating in online auction - towards explaining the popularity of english auction. *Electronic Commerce Research and Applications*, 6(1):53 – 62, 2007.

[17] D. J. Kim, C. Steinfield, and Y.-J. Lai. Revisiting the role of web assurance seals in business-to-consumer electronic commerce. *Decision Support Systems*, 44(4):1000 – 1015, 2008.

[18] B. McBride. Jena: A semantic web toolkit. *IEEE Internet Computing*, 6(6):55–59, 2002.

[19] U. Muegge. Controlled language: the next big thing in translation? *ClientSide News Magazine*, 7(7):21–24, 2007.

[20] *Myspace*. http://www.myspace.com/.

[21] X.-H. Phan. Crftagger: Crf english pos tagger. *http://crftagger.sourceforge.net/*, 2006.

[22] *Resource Description Framework*. http://www.w3.org/tr/pr-rdf-syntax/.

[23] *Sesame*. http://www.openrdf.org/.

[24] *SPARQL Query Language for RDF*. http://www.w3.org/tr/rdf-sparql-query/.

[25] Computer and internet fraud: A risk identification overview. *Computer Fraud and Security*, 2003(6):6 – 9, 2003.

[26] *Twitter*. http://twitter.com/.

[27] *Wikipedia*. http://en.wikipedia.org/wiki/main_page/.

[28] *Youtube*. http://www.youtube.com/.

[29] H. Zhang and H. Li. Factors affecting payment choices in online auctions: A study of ebay traders. *Decision Support Systems*, 42(2):1076 – 1088, 2006.