A MODEL FOR DEVELOPING ONLINE VERIFICATION AMONG E-COMMERCE CONSUMERS

[1]SHARFI M. ABBASS, [2]OTHMAN BIN IBRAHIM

[1]Universiti Teknologi Malaysia, Johor, Malaysia & Majmaah University, Majmaah, KSA, Department of Computer science and information system

[2]Universiti Teknologi Malaysia, Johor, Malaysia, Department of Computer science and information system

E-mail: [1]sharfi_islam@yahoo.com , [2]Othmanibrahim@utm.my

ABSTRACT

This paper aims to increase trust in E-Commerce among consumer-to-consumer (C2C) using the assurance key (AK) and supporting it by using face recognition (FR) technology in online verification (OV). This paper considers the development of our proposed model show in (section 2.1). It reviews previous studies of e-commerce regarding consumers' trust, and attempts to identify weaknesses and provide better solutions using a facial recognition technique and data encryption between the client and the server for increased security of data traded between them. It also reports the algorithms used for facial recognition and encryption and the use of appropriate e-commerce among C2C. Finally, it evaluates trust models used in similar studies.

Keywords: *E-Commerce , Consumer-to-Consumer (C2C) , Assurance Key (AK), Face Recognition (FR), Online Verification (OV)*

1. INTRODUCTION

The process of trust is one of the most important issues in e-commerce for those who deal electronically in buying and selling [2].

Previous studies touched on the importance of trust in the other party, and is based on building trust in using systems to verify the other party; for example, eBay uses the verification system of the other party by PayPal, which in turn depends on the credit card registered to have a way of verifying the consumer [3].

In our paper [1], we made a proposal to generate a unique number for each consumer instead of the credit card number used by eBay; this was compared with some credit cards and was distinguished from those cards in terms of safety, which leads to an increase in trust by a large margin. This may be used in the verification, security and trust of systems and can be compared to other biometrics such as fingerprint or eye iris recognition systems or FR [4].

In this paper we aim to use the FR system, because at the moment has become all of the devices used to connect to the Internet could be used in e-commerce, and are supported by digital cameras; for example laptops and mobile phones.

Therefore, we will use the FR system as a means to verify the identity of C2C in this paper, in addition to AK, which was generated using the new algorithm in our paper [1].

1.1 Background of FR:

FR is one of the most relevant applications for analysing images. An automated system works by simulating the ability to recognise faces. The automated system works to overcome the constraints faced by humans because the automated system possesses a very large memory and high processing capacity [5].

1.2 Definition of FR:

A facial recognition system (FRS) is a computer application for automatically identifying or verifying a person from a digital image or a video frame from a video source. One of the ways to do this is by comparing selected facial features from the image to a facial database [4].

Some facial recognition algorithms identify faces by extracting landmarks, or features, from an image of the subject's face. For example, an algorithm may analyse the relative position, size, and/or shape of the eyes, nose, cheekbones, and jaw. These features are then used to search for other images with matching features [6].

1.3 Algorithms of FR:

Many approaches have been taken, which has led to different algorithms. Some of the most relevant are principal component analysis (PCA), linear discriminate analysis (LDA), independent component analysis (ICA) and their derivatives, which are mentioned below.

1.3.1 PCA:

This is a mathematical procedure that uses an orthogonal transformation to convert a set of observations of possibly correlated variables into a set of values of linearly uncorrelated variables called principal components [7].

PCA was invented in 1901 by Karl Pearson [8] and is now used as a tool in the analysis of predictive models, and can be used as a correlation matrix or singular data matrix and z-scores [9]. Therefore, the results are related to component scores that are called factor scores [10]. PCA is the simplest analysis tool that explains the variance in data and can provide a lower–dimensional picture.

Factor analysis typically incorporates more domain-specific assumptions about the underlying structure and solves eigenvectors of a slightly different matrix.

1.3.2 LDA:

This analysis is one of the methods used in the census through pattern recognition and machine learning to find linear properties to characterise or define the difference between the two categories or two things. Thus it can be used as a linear classification in a more comprehensive use of dimensional reduction before classification.

This analysis is linked to significant disparity analysis (ANOVA) and regression analysis, which also aims to find one variable by gathering linear measurements or other attributes [11][12] .

The analysis of LDA tries to find differences between the denominations by modelling data, unlike PCA analysis, which does not attempt to find these differences [13]. In contrast, analysis of the factors seeks to focus on the differences more than the similarities.

Differential analysis also differs from factor analysis by focusing on the distinction between the independent and reliability variables, focusing on finding proceeds Quantity Per variables [14] [15].

1.4 Some of the Problems Concerning FR are:

i. Variations in illumination.
ii. Head rotation.
iii. Facial expression.
iv. Aging.

Studies currently seek to address these problems, for example [16], which addressed some of these problems and is discussed in the Literature Review.

1.5 Face Detection:

There are several algorithms used for the detection of faces, which are different to each other; some are less accurate, some are computationally very expensive and others are better than others. This depends on some of the challenges faced by the face detection, namely:

i. The location of the camera or movement of the camera (angle of photography).
ii. There are additional elements such as beards, glasses and hats.
iii. Facial expressions that vary greatly
iv. Terms imaging: impact of different types of cameras used in photography and the circumstances surrounding the shot on the quality of the image.

1.6 Encryption Data:

To protect data transmitted between networks and access from the client to the server or vice versa, data must be encrypted. Several studies have discussed encryption and decryption programs for data, including text data encryption and photos. They showed [17] that encryption is an effective mechanism and means used to protect valuable electronic information, and it needs to be dynamic in order to meet the new threats and methods used by Crypt analysts.

There are several ways to encrypt such as DES, 3DES, AES, and RC4. RC4 is one of the most popular methods for encryption [18], and has the following advantages [19]:

i. Symmetric stream cipher.
ii. Variable key length.
iii. Very quick in software.
iv. Used for secured communications as in the encryption of traffic to and from secure websites using the SSL protocol.

Study [20] showed that the full RC4 is still secure against known attacks. This study has been approved on the RC4 algorithm and its derivatives by different authors, such as [21].

proposed algorithm in study [17] depend on the results of studies [20] and [21]. According to the studies [20] and [21], study [17] proposed new algorithms and verified the performance of each one individually, to become easily viable depending on the circumstances. The proposed algorithms in this study are fixed initialisation vector (IV) and variable initialisation vector.

This study differs from traditional methods of safety in that it uses encryption techniques that are less complex. The evaluation process and means of safety help in determining the appropriate framework and to identify weaknesses and address them.

The outline of the proposed methodology of S-RC4 is presented here depicting the method of encryption and decryption separately.

[17] is one of the studies that sought to enhance security, and the proposed algorithm aims to stimulate progress in this direction. However, achieving 100% security still remains elusive.

The paper is organised as follows: Section 2 introduces the literature review that contains previous studies of FR, online verification models and our main proposed model; section 3 presents the proposed model and the hypothesis rules; section 4 presents the methodology; section 5 evaluates our proposed model; section 6 introduces suggestions for future research and section 7 gives conclusions.

2. LITERATURE REVIEW

The literature review is split into three main parts: part one focuses on some studies of FR, where we will review some modern studies to solve FR problems; Part two focuses on OV models, and in this part we will discuss some of the models and focus on the eBay model; and Part three focuses on our proposed model, where we will discuss the main proposal to solve weaknesses in similar previous models.

2.1 Summary of our Previous Paper [1]

This paper [1], reviews studies in E-Commerce, which focus on trust building in the other party. It also reviews websites operating in the same area, the most common of which is eBay; it relies on trust in the other party in the payment method of PayPal, which accepts credit cards.

The paper [1], proposes a model for addressing some of the weaknesses in the eBay model such as verifying that the data entered is correct and the credibility of the product details entered.

The paper [1], attempts to provide a more trusted method that ensures the identity of the other party by building a database of trusted third parties (TTP) [1], based on a new algorithm for generating and validating assurance keys (AK's) to all consumers in the world. The AK is saved as the name and image of the consumers in the database to verify them when they make a sale or purchase.

2.1.2 Assurance key (AK) parts

The AK consists of 20 digits, falling into five parts as shown in (fig.1) where part one functions as a continent code while part two represents a country code. The third part (i.e. AK-1) and fifth part (AK-2) are random numbers, each one of them contains 6-digits for each consumer according to the specified range of numbers for a country. Finally, the fourth part (i.e. AK-V) is used for validation of the AK to decide if it is in the system or not.

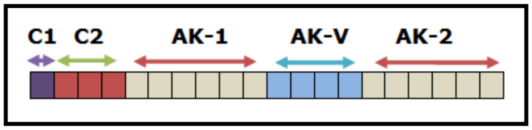


Fig.1 Assurance key parts

(Sharfi M. Abbass, et..al, 2012)

2.1.3 Registration part for new consumers

If the consumer is new then they start by completing the registration form that includes nationality, the national number, mobile number, date of birth, address, and their image to be uploaded from a file or webcam. The national number and mobile number are encrypted so that data can be sent to the TTP.

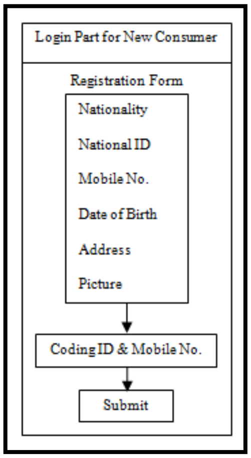


Fig.2 Login Part for New Consumers

(Sharfi M. Abbass, et..al, 2012)

2.1.4 Trusted third parties (TTP) model

TTP TTP receives the data from the registration part decrypts the national number and mobile number, and validates the data by reference to a

Governmental body. If data are not matching, a message will be sent to the consumer's mobile number, informing that the data is invalid so that they provide the valid data. However, if the data are valid, they will be saved on a database peculiar to registration form named App-Fr-DB file, and then given an AK, which is taken from AK-DB files that have been generated from proposed Algorithm in paper[1]. TTP saves its data in App-Fr-DB file where the image is saved in image-DB file by its AK number. A message will be sent to the consumer 's mobile phone with AK number to be used in verification of the consumer when making a sale or purchase.

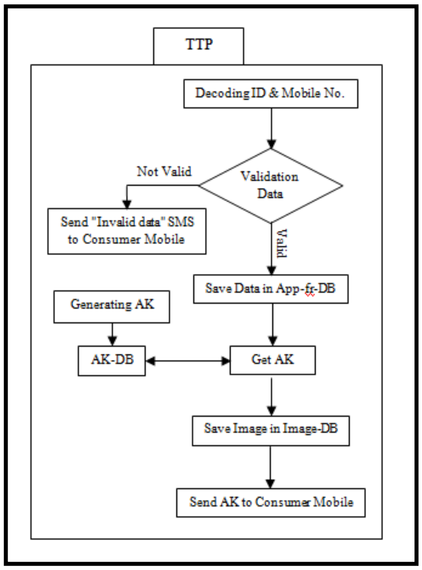


Fig.3 Trusted Third Party Model

(Sharfi M. Abbass, et..al, 2012)

2.1.5 Conclusion

The research attempts to propose a trust model between consumers in the light of the existing models. Particularly, it starts from the examination of the strengths and weaknesses of eBay model and proceeded to formulate the proposed model accordingly. In that connection, this study generated a new digital system (AK system) that has out-performed eBay in a variety of ways.

2.2 Previous Modern Studies of FR

Study [22] proved that the complete linear discriminant analysis (CLDA) was effective for recognising faces; this analysis can be performed by making use of information-distinct training samples.

The primary application of this technology may not be suitable for the incremental learning problem. Therefore, paper [22] introduces a new application of linear calculation which is more efficient than the basic model. It discusses the quantitative style that precisely identifies the discriminant vectors when using new samples in the training process.

Experiments conducted on the ORL, AR and PIE face databases regarding identifying faces showed the effectiveness of the model proposed in this study and the differences between this and the basic model.

Study [16] is based on the analysis of parameters to identify facial expressions, which can be utilised for several reasons, including human-computer interactions, security, law enforcement, psychiatry, and education.

This study discussed the fundamental problems of analysing facial expressions from the perspective of differences and aspects of spacing and convergence between them. The study used a statistical style to recognise the best ways to analyse facial expressions; I used the standard database for knowledge and the application of facial expressions on the following basis: First, when the face shows neutral expressions (natural) and second, when there is advanced information about the face.

The findings of this study are able to answer some basic questions, and the study also identified features and spaces that can differentiate between expressions.

Study [23] discussed an innovative approach of facial expressions based on fundamental analysis (the basic idea), PCA and the use of a technology to clearly differentiate between observations and logical conclusions. First, the difference between the data is demonstrated using PCA for high-processed treatments and the low-processed pictures (photo). Accordingly, the high-processed picture required less image processing. Then, two images were analysed by treatment and the high processing data is detected. This study also raised two models to improve and enhance the results of this process through repeated experiments.

2.3 Previous Study of Online Verification (OV) Models

2.3.1 Model 1: Steven E. K. Model

This touched on some of the previous studies [24], including the existence of a third party working to develop electronic seals, but did not solve the problem by a large margin. Study [24] proposes a model of trust between the business and consumer to ensure access to secure e-commerce and the development of the model shown in (Fig.4) It is important to prevent the hesitancy of consumers in e-commerce, and results show that Web assurance services create trust and lead to a marked increase in the volume of e-commerce. The study [24] concluded that the technology of e-commerce has grown. One barrier to success, however, has been the lack of consumer trust in websites developed by companies. As there have been relatively few papers in the area of Web assurance services, this study serves to make several contributions to the literature, by developing a mechanism to ensure trust among C2C and businessmen.

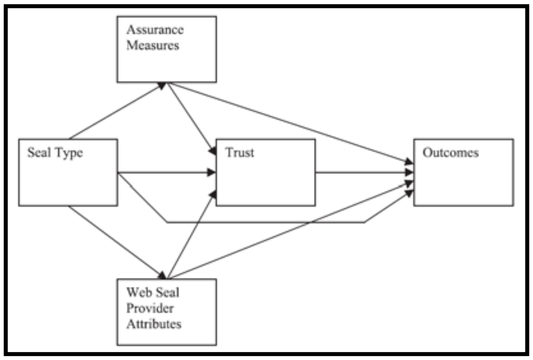


Fig.4 Model of Trust Including Assurance Measures and Provider Attributes (Steven E. K. 2003).

The methods used in study [24], were based on McKnight [25] and Mayer [26]. This study conducted an experiment on the Internet website developed for a fictitious company, which was similar to retail sites selling clothes; it used the fictitious company for a guarantee.

The Steven study [24] concluded that the growth of technology has been seen in e-commerce. The former suggested the existence of a third party working to develop electronic seals, but this did not solve the problem.

2.3.2 Model 2: eBay model

According to the results of our paper [1], we found that eBay is one of the best sites that operate C2C transactions in terms of trust. Therefore, we will review the following mechanism used in online verification by eBay to provide trust.

2.3.2.1 How eBay OV works [27]

i. A seller lists an item on eBay, almost anything from antiques to cars, books to sporting goods. The seller chooses to accept only bids for the item (an auction-type listing) or to offer the "Buy It Now" option, which allows buyers to purchase the item immediately at a fixed price.

ii. In an online auction, the bidding opens at a price that the seller specifies and the product remains on eBay for a certain number of days. Buyers then place bids on the item. When the listing ends, the buyer with the highest bid wins.

iii. In a "Buy It Now" listing, the first buyer willing to pay the seller's price gets the item.

2.3.2.2 eBay Website Access

From the eBay Website [28], operations can be identified. They can be summarised in three main axes: seller, buyer and PayPal. These are explained further along these lines:

2.3.2.2.1 Axis One: Seller

To sell items on eBay, the seller must pass the following stages:

i. Create a seller account: Account creation requires provision of basic information, e.g. name, address, mobile number, verification of identity by the data entered and the method of automatic payment.

ii. Set up your Q&A: Buyers often have questions before, during, and after a sale. When they do, they click the "Ask a Question" link in the listing. When buyers contact the seller directly, it is important for them to respond quickly and thoroughly. This keeps the buyer interested in the listing, saves time, and it is more likely that the seller will get positive Feedback when the transaction is complete. There is also the option of providing buyers Q&A made up of answers generated automatically from your listing, answers you create yourself, and stock answers about eBay policies.

iii. Research your item and the rules of selling: do some research, especially to determine the price and choose the form of the existing category; this will help in the development of best price for your item. It is preferable to clarify the preferred options for shipping costs before the sale. Also, you know the rules, policies and restrictions on eBay regarding being banned and restricted.

iv. Create your listing: When creating your list, you have a variety of options; if you sell an existing product on eBay, you can add product details in the list of the site. There are several rules that exist within the site depending on your product.

v. Manage your listing: this is a process where you can check your product in eBay. The website has a manual to inform sellers about how to amend the list.

vi. Wrap up with your buyer: This is the final stage where the product is sent to the buyer after communicating with him/her and payment is completed. The product is sent through an effective and secure channel.

2.3.2.2.2 Axis Two: Buyer

Buying on eBay is going through several stages:

i. Registration: Registration takes place online on the website. It requires basic data, such as name, email, user name and password.

ii. Finding something to buy: unlike other websites, which are specialised in items such as cars, electronic devices, etc., all products are available on eBay. Products can be accessed in one of two ways. First, they can be found through browsing. This method is used if you are sure that the product has a section in eBay, such as mobile or clothing, etc.; in this case, you can enter the page devoted to it. Second, items can be accessed through searching. This method is used if you are not sure of the existence of the product you are looking for, or do not know a specific page. In this case, the search is the name of the product or a few key words about the product.

iii. Understand the buying format: the eBay site has a lot of ways to purchase items immediately because the purchase price is specified, or it is available to buy through classified ads.

iv. Choosing a payment method is what distinguishes eBay. It uses the PayPal financial transactions (purchase, sale); for detail see more about PayPal (Axis Three). There are also other ways of payment, such as: Bill Me Later and Credit cards and debit cards.

v. Track your purchases: After registration you get access to your own page; through your page you can track your purchases, and can also watch other items that you want to buy.

2.3.2.2.3 Axis Three: PayPal [29]

Overview: PayPal is a faster, safer way to pay and get paid online. The service allows people to send money without sharing financial information, with the flexibility of paying using their account balances, bank accounts, credit cards or promotional finance. With 103 million active accounts in 190 markets and 25 currencies around the world, PayPal enables global ecommerce. PayPal is an eBay (Nasdaq: EBAY) company and is made up of three leading online payment services: the PayPal global payment service, the Payflow Gateway and Bill Me Later. More information about the company can be found at PayPal [29]. PayPal headquarters are in San Jose, Calif. and the international headquarters are located in Singapore.

Why Choose PayPal?

i. Pay securely for your online purchases, and shop securely on eBay and thousands of online stores. When you pay with PayPal, your financial information is not exposed.

ii. Send money quickly and easily. Pay for purchases and send money from 190 countries and regions. All that is needed is the recipient's email address. Recipients do not need a PayPal account – they can sign up when they receive your payment.

iii. Accepted worldwide. PayPal is accepted by thousands of businesses worldwide and is the preferred payment method on eBay.

iv. Easy to sign up, easy to use. Signing up for a PayPal account is easy - it takes just a few minutes. Once you have signed up, you can send your payment in minutes.

The above mentioned points can be summarised in the following model:

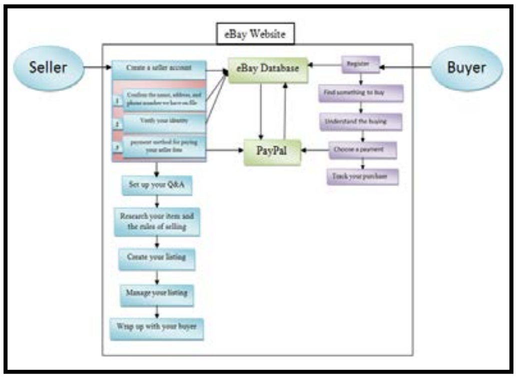


Fig.5 The eBay Website Access Model

2.3.2.2.4 Weaknesses in the eBay model:

i. Seller starts recording data online, thus, it is possible to enter incorrect data, such as an alias, unknown e-mail, or mobile number that is not registered in the name of a specific corresponding client. Thus, the buyer's identity could not always be proved.

ii. There is no clear mechanism to reduce pseudo show or to identify product specifications (the seriousness of purchase).

iii. Verification takes place through registration of a PayPal credit card.

iv. Registered person on PayPal Online cannot be verified. Any person can take someone else's data by data theft or can get registered in PayPal and practice his trade activities.

Since eBay is the best C2C site, this study will try to develop a model to increase trust, and to address the weaknesses in eBay.

2.4 Our Proposed Model:

Our proposed model is considered an upgraded version of the previous model proposed in our prior paper [1].

In our paper [1], we solved some of the weaknesses in the eBay model (fig.5) that were mentioned in section 2.3.2.2.4. However, in this paper we will develop our model by adding OV using FR technology.

In this section we will describe the research methods used to achieve the objectives of the study, through drawing and explaining the model chart, which depends on the OV of the consumer by AK and FR algorithms.

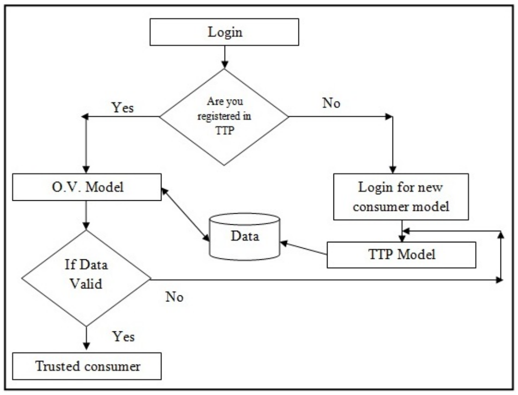


Fig.6 Main Proposed Model

In our proposed model, we start by asking the consumer if they registered data in TTP with AK and picture that is stored by the third party to begin practicing his e-commerce transaction from the purchase or sale.

If one has not registered TTP data yet, they can begin to enter data as a new consumer, show in section (2.1.3). Then the consumer moves on to the next stage, which is Go to TTP, and supplements registration statements. This saves information and gives them an AK to practice their e-services.

If the user is registered in TTP, they can enter the stage of verification via the Internet and through the use of their own AK. In this case, they enters their picture as described in the OV model (Fig.7).

3. RESEARCH MODEL AND HYPOTHESES:

According to our main proposed model (Fig.6), in this part we will describe the OV model.

3.1 Verification Model

According to our proposed model [1], we will describe a mechanism that can be used in TTP and OV, which works to boost trust in e-commerce between C2C in the TTP model. This is through the use of multiple measures to increase trust in the proposed model, which uses more than one measure to verify the customer. In our paper [1], we had already generated AKs for all consumers to use for multiple measures from consumers. In this paper, we work to add new methods to the model in paper [1], to increase trust; this method is the FR technique.

3.2 The model works on the Internet as follows:

It begins by asking the consumer who wishes to conduct an e-commerce transaction if they are registered in the TTP. If the answer is no, they will be required to register in TTP to be given an AK. If, on the other hand, the answer is yes, they will be asked to enter their AK to be encrypted and verified.

If the AK does not match, the customer will be given specific opportunities to re-try; if they fail to enter a number of AKs properly and exhaust all of the opportunities, they will be required to enter their mobile number and the national number registered in the NID [1] for comparison with the AF-DB. When they are matched, a message will be sent to their mobile phone. If the mobile number or the national number is incorrect, they will be asked to go back to the TTP.

If the AK is identical to the database, the AK-DB will ask the user to enter his image through the webcam to determine the face in the picture; only then can the person be trusted and allowed to perform an e-commerce transaction through the site.

If the picture does not match, they will be given specific opportunities to re-try; if they fail to insert pictures that are acceptable to the system and exhaust all opportunities, they will be required to enter their mobile number and the national number registered in the NID to compare them with the AF-DB. If they match, they will be granted additional opportunities to re-enter the picture to be verified; if either the mobile number or the national number is incorrect, they will be required to go back to the TTP.

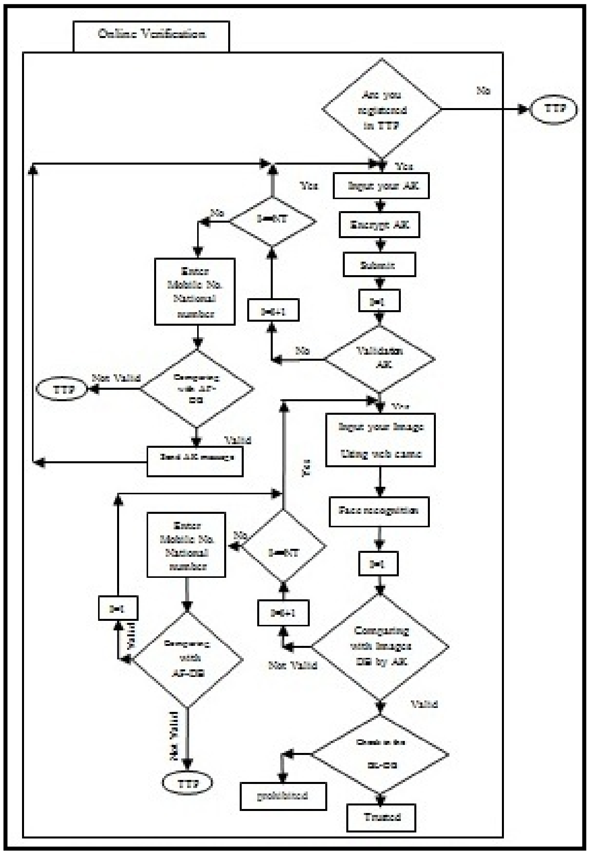


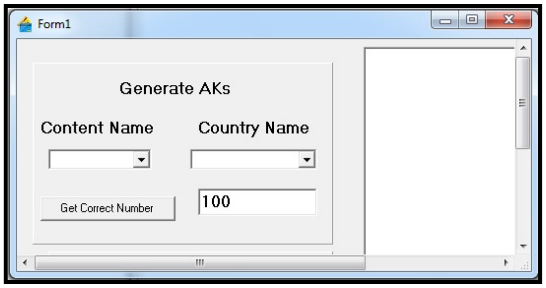
Fig.7 Online Verification Model

3.3 Hypotheses:

It is supposed that this model addresses the weaknesses mentioned for the eBay model, some of which were solved in our paper [1]. Our proposed model in this paper aims to verify C2C online by AK and FR, and we have stated in our paper [1] that the proposed model to generate AK according to the specified mechanism achieved better results than that used in the credit card used in the eBay model by PayPal. In our proposed model in this paper we use online verification by AK and add verification by FR, which in turn increases trust and achieves better results than seen in our paper [1]. In section 4, we will explain how to verify by AK and FR.

4. METHODOLOGY:

Our methodology falls into two main parts: part one focuses on AK implementation, where we will review the steps of generating and validating AKs, while part two focuses on FR implementation, so we will review the steps of capturing photos by digital camera and comparing them with the ORL database.



100

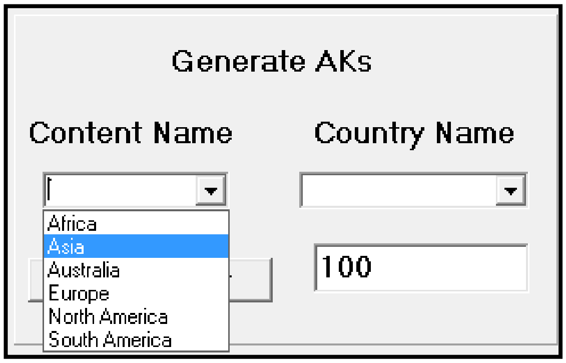
AK implementation

Fig.8 Generate AKs Main Menu

Fig.8 shows the main menu for generating AKs, which contains the name of the continent among six continents (each continent is symbolised by one digit, as shown in Table 1 in our paper [1]). When choosing one continent, the countries are then shown in the name box and each state is symbolised by three digits, as shown in Table 1.

Table 1: Countries of Asia, (Range of people in Asia Continent from 50,000,000,001 to 300,000,000,000)

Content Code	Country Name	Country Code	Range of people
2	Abkhazia	061	150,000,000,001 to 152,000,000,000
2	Afghanistan	062	152,000,000,001 to 154,000,000,000
		. . .	
2	Malaysia	093	224,000,000,001 to 226,000,000,000
		. . .	
2	Yemen	119	276,000,000,001 to 278,000,000,000



Generate AKs

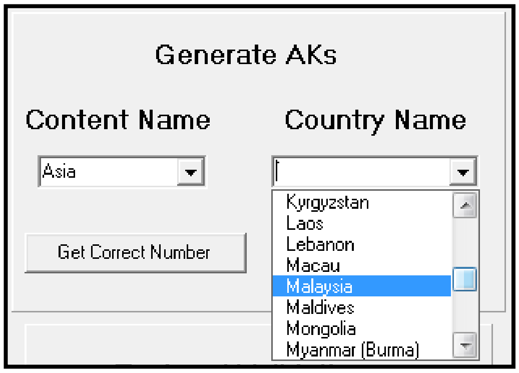
Content Name

Country Name

Africa
Asia
Australia
Europe
North America
South America

100

Fig.9 Select Content Name



Generate AKs

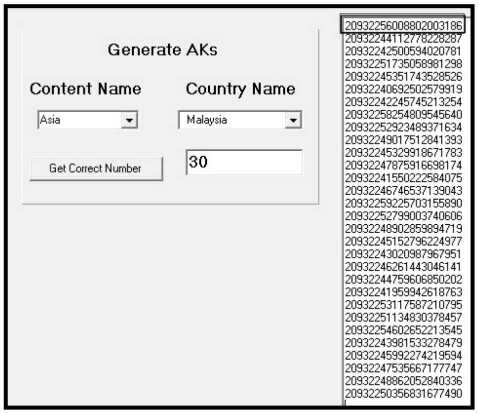
Content Name: Asia

Country Name

Kyrgyzstan
Laos
Lebanon
Macau
Malaysia
Maldives
Mongolia
Myanmar (Burma)

Fig.10 Select Country Name

After selecting the continent and the state to generate numbers, we indicate the number of AKs to be generated. Here, we generate AKs composed of 20 digits, as shown in Fig.12 These are required to be Random Number 12-digits (shown in Fig.12), which are symbolised by AK-1 and AK-2 to form the scope of the numbers specified for this state as shown in the tables (tables of Asian countries to another continent countries tables). For example, we generated 30 random numbers for Malaysia, which is an Asian state, to explain in detail the AKs and verifications in accordance with the attached data tables.



Generate AKs

Content Name: Asia

Country Name: Malaysia

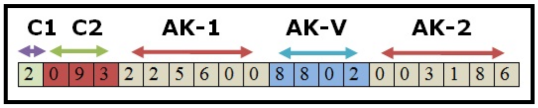
30

```
20932256008802003186
20932244112778228287
20932242500594020781
20932251735058981298
20932245351743528526
20932240692502579919
20932242245745213254
20932258254809545640
20932252923489371634
20932249017512841393
20932245329918671783
20932247875916698174
20932241550222584075
20932246746537139043
20932259225703155890
20932252799003740606
20932248902859894719
20932245152796224977
20932243020987967951
20932246261443046141
20932244759606850202
20932241959942618763
20932253117587210795
20932251134830378457
20932254602652213545
20932243981533278479
20932245992274219594
20932247535667177747
20932248862052840336
20932250356831677490
```

Fig.11 Generate 30 AKs for Malaysia

To verify that the AKs were generated in accordance with the conditions specified, we will test one random number shown in fig. 11 Above; let us test the first number which is:

2 093 225600 8802 003186



2	0	9	3	2	2	5	6	0	0	8	8	0	2	0	0	3	1	8	6

Fig.12 Details of AK

To test the validity of the number we should fulfil the conditions in all of its parts. The conditions are:

i. The C1 is between 1 and 6 as symbol for the continent; here, C1 is the number 2, if this condition is verified.

ii. The C2 is between 61 and 119, as shown in Table 1; here C2 is 93, if the condition is verified.

iii. The AK-1 and AK-2 in the range specified for this state are 224,000,000,001 to 226,000,000,000, as in Table1; here, AK-1 and AK-2 are 225,600,003,186 if the condition is verified.

iv. The total number of AK-V must be divisible by 3, and the total numbers (8 +8 +0 +2) = 18, 18/3 = 6, if the condition is verified.

FR implementation

The main menu for FR implementation contains photo entering by browsing or entering the photo by a Webcam, as shown in the following figure:

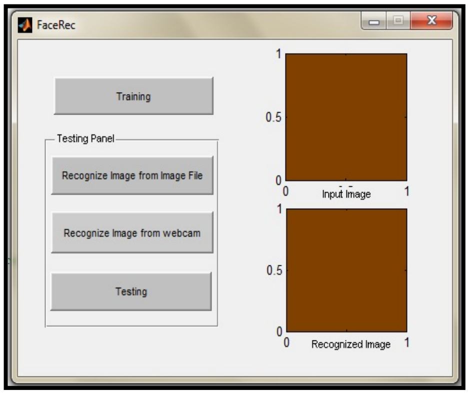
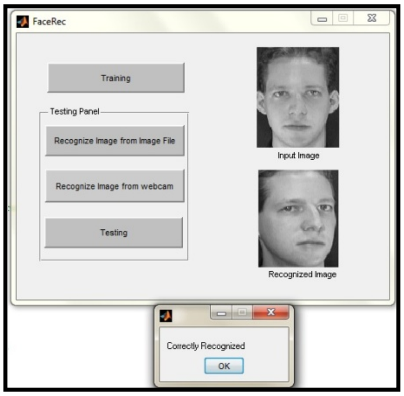


Fig.13 Main Menu For FR Implementation

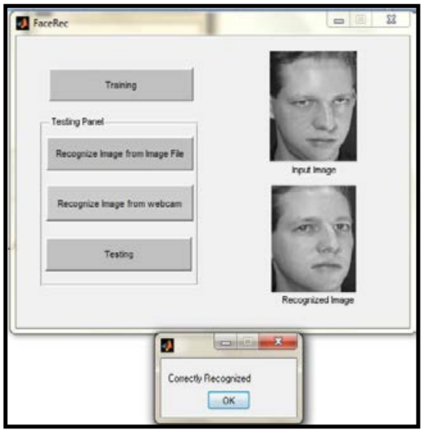
The first way: insert a photo from a file (from ORL database); this is then compared with the existing database, as in the following figure:



Correctly Recognized

Fig.14 Insert A Photo From A File And Compare It With The ORL Database

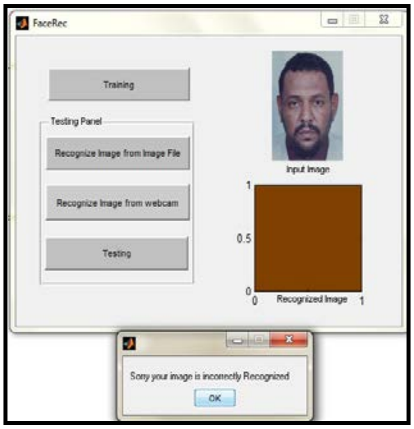
We show massage of a "Correctly Recognised" because the input photo corresponds to a person with a photo in the ORL database. If you enter another photo of the same person, the same message "Correctly Recognised" is shown.



Correctly Recognized

Fig.15 Insert Another Photo From A File And Compared It With The ORL Database

However, if we enter a different photo which does not exist in the ORL database the message is as follows:



Sorry your image is incorrectly Recognized

Fig.16 Insert Photo That Does Not Exist In The ORL Database

The second way: enter a photo using a digital camera; we will enter a photo that does not exist in the ORL database, then we will input this person's data to the ORL database and then re-enter the same photo.

Stage One: Entering a photo that does not exist in the ORL database.

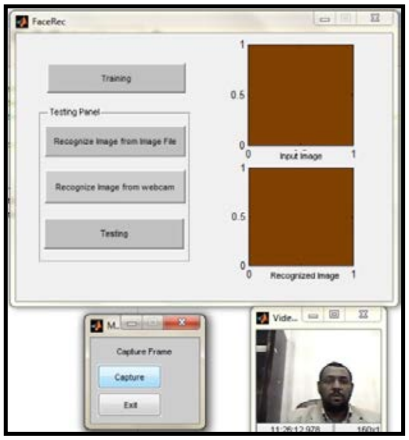
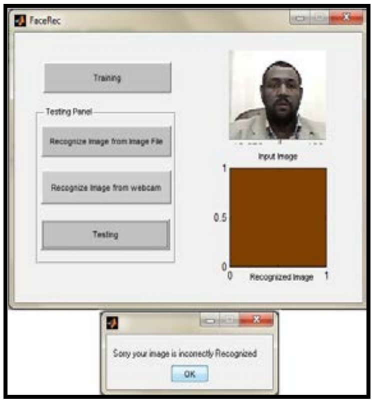


Fig.17 Photo Does Not Exist In The ORL Database



Sorry your image is incorrectly Recognized

Fig.18 The Result When A Photo Does Not Exist In The ORL Database

In this case, the message "Sorry your image is incorrectly recognised" is shown because the input photo does not find a match due to the photo not existing in the ORL database.

Stage two: add the photo of the same person in the ORL database and re-compare the photo after saving the photo in the ORL database

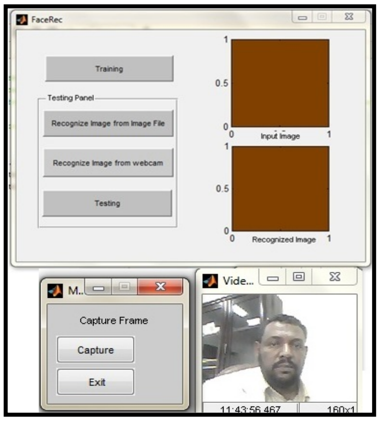
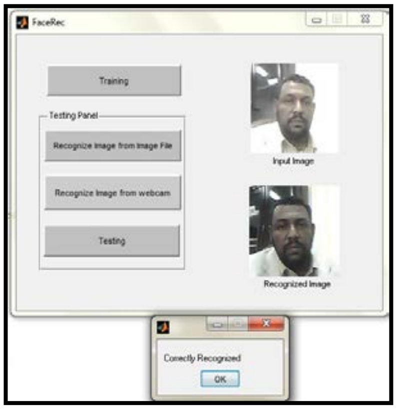


Fig.19 Save New Photo In ORL Database

Now, we re-compared the photo with the new photo added to the ORL database.



Correctly Recognized

Fig.20 Results of comparison after adding

new photo to the ORL database

We show the message "Correctly Recognised" because the input photo corresponds to a person with a photo in the ORL database.

5. EVALUATE OUR PROPOSED MODEL:

The process of trust for vendors and transactions are considered very important issues in e-commerce [2].

This has been used in the evaluation of e-commerce models using or enabling Business Process Reengineering (BPR) [30].

In recent years, most of research has been based on trust regarding the evaluation of a reputable trust model [31].

In this study we worked on making a model to develop trust among C2C compared with the trust model used by the eBay site and an evaluated model [32], according to the following points:

The evaluation roles for eBay architecture as follows: (Quality Requirement):

Scalability: System should support variations in load without human intervention. As more and more people join the internet, more and more users attempt to access the website and request information simultaneously; they must be serviced without fail.

Availability/Reliability:

The system should provide 24/7 availability with almost no downtime period.

Security: The system should authenticate users and protect against unauthorised access to data. Such access could have disastrous effects for an online marketplace.

Usability: Different users should be able to access different content in different categories and multiple users must be able to bid on items at the same time.

Performance: Users should be provided with fast response times. This is especially necessary when a bid is coming to a close and the user wants to ensure that he/she gets the chance to see the last bid.

Our model is characterised by the eBay model, including the following:

First: study [33] evaluated the trust models that were used in the studies [34-36], which evaluated the trust based on Bayesian risks, and on the basis of recommendations that focus on distribution system trust; also trust was calculated according to the data of the transactions.

It turned out that these studies evaluated trust within the same P2P network, but did not address how to assess trust if access to other P2P networks occurred.

Therefore, study [33] aimed to solve this problem by developing a model to assess the trust in the event of access to various P2P networks. This was based on calculations and data through the development of a specific part of the trust, which is Trusted Platform Module (TPM), supported by electronic signature technology providers.

In our OV model, we used AK and facial recognition technology for the consumer and the seller, which prevented impersonation.

Second: Study [2] worked on the development of management mechanism trusts from which is calculated the value of trust; : this study found that some e-commerce sites such as eBay rely on ratings that previous trading has seen. This value can only reflect the state of public trust or global Seller's; it is not restricted to new transactions, so the buyer can easily fall victim to swindlers in new transactions, where the seller can acquire a good reputation by selling at a lower price.

After gearing customer trust , some buyers start changing high prices ; thus , trust has to a permanent basics for past and future transaction. This study also provides a new method to assess trust, where it is compared with the previous trading transactions, and in this case the value of new trading transactions is determined ; the study found that this method can determine and prevent any fraud or fraudulent transactions.

This study lacks a way to verify that the seller is the same account holder, i.e. you must make sure that all transactions are for a single vendor; people should not be able to enter a pseudonym to exploit others and their business reputation. Our model proposed to prevent this because when you display an item or service it must be verified by AK using the photo that is maintained by the TTP; no consumer can have more than one AK, as shown in our paper [1].

In our proposed model there would be punishment for vendors who act fraudulently; data would be sent to a blacklist (BL) and the vendor would be prevented from practicing sales through the Internet, as shown in (Fig.7).

6. FUTURE WORK:

The establishment of government agencies in all countries in the world is required, where there is mutual agreement between the powers of these agencies to identify people. Thus all data on persons would be available through the Internet and the exporting government would be a third-party guarantor.

A global mechanism jointly established by governmental agencies so that data will be available all over the world with mechanisms to allow people to log in without accessing the personal data of other consumers.

You can use this data to provide trust between B2C or in e-government transactions as data for the world's population; this would be a standardised mechanism, through which to identify people and the countries to which they belong.

7. CONCLUSION:

This paper has reviewed the methods used in the verification of C2C in e-commerce. It has reported the weaknesses in the methods used in the eBay model as one of the best sites in e-commerce among C2C, and has put forward a proposal to increase trust by using FR technology with the use of AK, as well as to increase the trust in the other party by verifying the consumer through his/her personal image and AK stored on the TTP. Our proposed model should be considered as a solution to the weaknesses of the eBay model mentioned previously.

8. ACKNOWLEDGMENTS

We are so grateful to Dr. El-Sadig Yahya Abdalla and Mr. Ahmed Yassin Ahmed for their great efforts concerning revision and proofreading of our paper.

REFRENCES:

[1] Sharfi M. Abbass, Othman Bin Ibrahim and M. S. Farag. Article: Building a Trust Model for Generating and Validating Assurance Keys Between Consumers in E-Commerce. International Journal of Computer Applications 57(1):17-25, November 2012. Published by Foundation of Computer Science, New York, USA.

[2] Haibin Zhang, Yan Wang, Xiuzhen Zhang " Transaction Similarity-Based Contextual Trust Evaluation in E-Commerce and E-Service Environments", 2011 IEEE International Conference on Web Services (ICWS), , pp 500-507

[3] http://pages.ebay.com/help/account/questions/aboutebay.html

[4] "Facial Recognition Applications". Animetrics. http://www.animetrics-.com/technology/frapplications.html. Retrieved 2008-06-04.

[5] Proyecto Fin de Carrera, " Face Recognition Algorithms " , Master's thesis in Computer Science, Universidad Euskal Herriko 2010.

[6] Bonsor, K.. "How Facial Recognition Systems Work". http://computer.howstuffworks.com/facial-recognition.htm. Retrieved 2008-06-02.

[7] http://en.wikipedia.org/wiki/Principal_Component_Analysis

[8] Pearson, K. (1901). "On Lines and Planes of Closest Fit to Systems of Points in Space" (PDF). Philosophical Magazine 2 (6): 559–572.

[9] Abdi. H., & Williams, L.J. (2010). "Principal component analysis.". Wiley Interdisciplinary Reviews: Computational Statistics, 2: 433–459.

[10] Shaw P.J.A. (2003) Multivariate statistics for the Environmental Sciences, Hodder-Arnold. ISBN 0-340-80763-6.[page needed]

[11] Fisher, R. A. (1936). "The Use of Multiple Measurements in Taxonomic Problems". Annals of Eugenics 7 (2): 179–188. DOI:10.1111/j.1469-1809.1936.tb02137.x. hdl:2440/15227.

[12] McLachlan, G. J. (2004). Discriminant Analysis and Statistical Pattern Recognition. Wiley Interscience. ISBN 0-471-69115-1. MR 1190469.

[13] Martinez, A. M.; Kak, A. C. (2004). "PCA versus LDA". IEEE Transactions on Pattern Analysis and Machine Intelligence 23 (2): 228–233. DOI:10.1109/34.908974.

[14] Abdi, H. (2007) "Discriminant correspondence analysis." In: N.J. Salkind (Ed.): Encyclopedia of Measurement and Statistic. Thousand Oaks (CA): Sage. pp. 270–275.

[15] Perriere, G.; & Thioulouse, J. (2003). "Use of Correspondence Discriminant Analysis to predict the subcellular location of bacterial proteins", Computer Methods and Programs in Biomedicine, 70, 99–105.

[16] N. Alugupally, A. Samal, D. Marx, and S. Bhatia, " Analysis of Landmarks in Recognition of Face Expressions " , Pattern Recognition and Image Analysis, 2011, Vol. 21, No. 4, pp. 681–693.

[17] Arun Kumar Singh, , Shefalika Ghosh Samaddar, Swagat Ranjan Sahoo, Glitto Mathew , " Increasing Robustness of RC4 Family for Automated Selection of Cipher suites ", Procedia Engineering Volume 30, 2012, Pages 45–52, © 2012 Published by Elsevier Ltd

[18] Subhamoy Maitra and Goutam Paul, "Analysis of RC4 and Proposal of Additional Layers for Better Security Margin", INDOCRYPT **,2008** LNCS 5365, pp. 27–39, 2008. Springer-Verlag Berlin Heidelberg 2008**.**

[19] Allam Mousa, Ahmad Hamad. , "Evaluation of the RC4 Algorithm for Data Encryption", International Journal of Computer Science & Applications, Vol. 3, June 2006.

[20] S. Mister , S. E. Tavares,S. Tavares and H. Meijer (Eds.), SAC'98, LNCS 1556, pp. 131{143, 1999. Springer-Verlag Berlin Heidelberg 1999 **,**Cryptanalysis of RC4-like Ciphers**.**

[21] Prasithsangaree, P.; Krishnamurthy, P., "Analysis of Energy Consumption of RC4 and AES Algorithms in Wireless LANs", Global Telecommunications Conference, 2003. GLOBECOM '03. IEEE.

[22] Gui-Fu Lu , Jian Zou , Yong Wang, " Incremental complete LDA for face recognition " Pattern Recognition 45 (2012) 2510–2521.

[23] Xiang Xu, Wanquan Liu, Svetha Venkatesh, " An innovative face image enhancement based on principle component analysis " Int. J. Mach. Learn. & Cyber. DOI 10.1007/s13042-011-0060-x.

[24] Steven E. K. , Robert J. N. A Web assurance services model of trust for B2C e- commerce.

D 2003 Published by Elsevier Inc. 4 (2003) 95–114.

[25] McKnight DH, Cummings LL, Chervany NL. Initial trust formation in new organizational relationships. Acad Manage Rev 1998;23(3):473–90.

[26] Mayer RC, Davis JH, Schooman FD. An integrative model of organizational trust. Acad Manage Rev 1995 ; 20(3):709–34.

[27] http://pages.ebay.com/help/account/questions/about-ebay.html

[28] http://www.ebay.com/

[29] http://www.paypal.com

[30] I.P. Tatsiopoulos, N.A. Panayiotou, S.T. Ponis, " A modelling and evaluation methodology for E-Commerce enabled BPR ", Computers in Industry 49 (2002) 107–121**.**

[31] S. Balfe, A.D. Lakhani, K.G.Paterson, “Trusted Computing: Providing Security for Peer to Peer Networks”, In Proc. Fifth International Conference on Peer to Peer Computing, IEEE Computer Society, 117-124, 2005.

[32] Mohammad Usman Ahmed, www.cs.mcgill.ca/~mahmed26/eBay_Architecture_Stud
y.pdf.

[33] Zhenling Wang, " A Trust Evaluation Algorithm in P2P Network based on Trust Model ", International Journal of Digital Content Technology and its Applications. Volume 5, Number 8, August 2011.

[34] Y. Wang, J.Vassileva, “Bayesian Network-based Trust Model in Peer to Peer Networks”, in Proc. of the Workshop on “Deception, Fraud and Trust in Agent Societies” at the Autonomous Agents and Multi Agent Systems. LNCS 2872, Berlin: Springer-Verlag, 2003.

[35] W. J. Adams, N.J. Davis, “Toward a Decentralized Trust-based Access Control System for Dynamic Collaboration”, in Proc. of the IEEE Workshop on Information Assurance and Security United States Military Academy. West Point: IEEE Press, 317-324, 2005.

[36] S. D. Kamvar, “The Eigen Trust Algorithm for Reputation Management in P2P Networks”, in Proc. of the 12th International Conference on World Wide Web(WWW2003), 640-651 ,2003.