Comprehensive study on methods of fraud prevention in credit card e-payment system

Dr. Saleh Al-Furiah
alfuraih@ccis.edu.sa

Lamia AL-Braheem
Lamia_ea@yahoo.com

ABSTRACT
Due to the increasing demand on electronic payment, fraud methods also increasing which resulted in losing millions of Riyals worldwide each year. Several ways have been applied to fight against fraud, therefore, fraud prevention is becoming a vital subject to be studied and improved. In this paper we will provide a comprehensive study on methods of fraud prevention techniques in credit card E-payment system.

Keywords
Fraud prevention, Fraud detection, credit card, MTIO.

1. INTRODUCTION
Nowadays Internet is providing online purchases and facilitates payment by making it very flexible. One of the most popular ways of payment is credit card which is a method where it gives you the opportunity to buy goods and pay later [14]. Although the electronic payment systems having a lot of advantages like fast buying any product from a far country in the world, but it has many risks with the information security. The credit card fraud is becomes the nightmare for the all parties involved. Also, the credit card fraud losses are increasing daily [26].

Fraudsters are trying all possible ways to discover any weak point to be utilized. From this point we can see the necessity of identifying and improve fraud prevention techniques that decrease the fraudsters' activates. Although there are many methods for fraud prevention but in the same time the card fraud methods are improving [26].

This paper is organized as follows: Section 2 provides a background about the credit card e-payment system. Section 3 presents the literature review about credit card fraud. Section 4 displays the fraud detection techniques. Section 5 displays the fraud prevention techniques. Also it includes the comparison and evaluation between the fraud prevention techniques. Finally, section 6 contains the conclusion of the paper.

2. BACKGROUND
There are four parties involved in the process of credit card e-payment system: **customers**, **merchant**, **issuer bank** "customer's bank" which refers to the bank that issued the payment instrument (e.g. credit card). As they also watch and maintain the credit card account of the customer. Usually the issuer bank is associated with the **card associations** such as Visa, MasterCard, American Express and Discover. The **acquirer bank** is the merchant bank [20].

The scenario of the credit card e-payment can be summarized as following: first of all, when the customer wants to make online purchasing, he selects the goods or services and then he provide his credit card information by filling the required form. After he submit the form to the merchant, the merchant send the request to the acquirer bank to make sure that the customer has enough money on his credit card. This is the start of a process called Authorization. Then the acquirer bank sends a request for authorization through the card association to the issuer bank. The issuer bank checks the customer's credit card account. If this account holds enough money cover the amount needed, the required money will be reserved only. After that, the issuer bank sends appropriate response through the card association to the acquirer bank where it will return to the merchant and this is the end of the authorization process. If the response is positive, the merchants will send the ordered goods or services to the customer. At this stage the settlement process start where the merchant will request the actual amount of the goods or services. Then, the acquirer bank sends a settlement request to the issuer bank through the card association. As result of this settlement, the money will be deposited in the merchant's account. Also the issuer bank will charge the amount of money to the customer's credit card. Furthermore, after a period of time (e.g. monthly) the issuer bank will send a notification to the customer to inform him about the accumulated charges [20, 22].

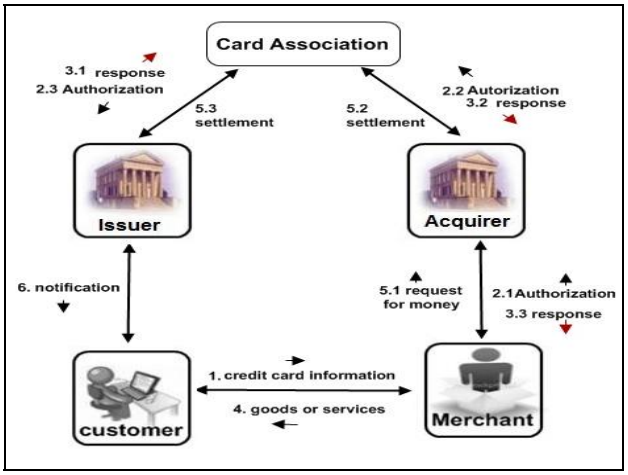

Figure 1: Credit Card e-payment system [23].

3. CREDIT CARD FRAUD

3.1 Credit Card Fraud definition

The credit card fraud can be described as using someone's credit card but without the knowledge of the owner or issuer of the credit card. Moreover, the person (Stolen) who's using a credit card has no relation with the owner or issuer of the credit card and has no intention of either inform the cardholder or make repayment for the goods been purchased [14]. There are two different kind of fraud that we can identify: offline fraud and online fraud. The offline fraud can be identified as the traditional way by using a stolen credit card at a store to purchase any item. On the other hand, the online fraud (cardholder-not-presents) takes place thru Mail, Telephone and Internet Order (MTIO) [30].

3.2 Type of Credit Card Fraud

There are various ways of credit card fraud and it can be categorized as a stolen card which represents almost 25% of the total credit card fraud. Counterfeit card fraud or skimming has been a fast-growing criminal activity in recent years where a device is used to scan a card and obtain the code hidden in the magnetic stripe so that it can be replicated and used fraudulently. This way constitutes almost 24% of the total credit card fraud. Also, to commit this type of fraud it is necessary to obtain the details of the card without the cardholder's knowledge Third way is Mail, Telephone, Internet Order (MTIO), as per the researchers it represents 21% and they consider it the fastest increasing fraud. Fourth, lost cards which are the card reported missing by the cardholder of record, or a card that was never received and is presumed to have been lost in the mail. This way constitutes only 15 %. The remaining 15% is distributed to the rest of credit card fraud [3].

3.3 Fight against Fraud

The current existing techniques to fight fraud can be classified into two types: fraud prevention and fraud detection. Fraud prevention can be defined as "measures to stop fraud occurring in the first place". On other hand, fraud detection "involves identifying fraud as quickly as possible once it has been perpetrated [7].

3.4 Impact of Credit Card Fraud

The dangerous of the fraudulent activity on card usually will affect all or some parties involved. As we observed that customers are the least effected party. This is due to the limitation of the customer liability for credit card transactions by the legislation applying in most countries [6].

Most of the legislation applied charges to the merchants for any losses due to fraud, especially in the card-not-present. Whenever the customer object any transaction thru the credit cards, the card issuer will send a chargeback to the merchant (thru the acquirer) reversing the credit for the transaction. If the merchant couldn't provide any prove (e.g. evident of delivery) to the acquirer it will be impossible to reverse the chargeback. Moreover, the merchant will undertake all expenses i.e. cost of goods, shipping cost, merchant bank fees and cost of charge back [6].

Under the rules of MasterCard and Visa the Issuer/Acquirer sometimes will bear what they called the indirect cost such as the administrative and manpower costs that the bank has to incur. It's also necessary by the issuer and acquirer to adopt and develop sophisticated systems to prevent any fraudulent transactions [6].

4. CREDIT CARD FRAUD DETECTION TECHNIQUES

The development of new fraud detection techniques is difficult because the limitation in exchange the ideas in this field. When details provided about the detection techniques, the fraudsters can use this information to avoid detection. Also, the data set required for any detection techniques are not available to public [8].

The fraud detection techniques may be implemented by number of methods such as data mining, statistics and artificial intelligent [21]. Also the fraud detection techniques have two categories: supervised and unsupervised techniques. In supervised techniques, we need to build a model using samples of both fraudulent and non-fraudulent transactions and trained the model to differentiate between them. So, if there is a new transaction this model should able to assign it to one of the two classes. Moreover, the supervised techniques can only used to detect frauds type that previously occurred [8].

On other hand, the unsupervised techniques don't need the previous knowledge of fraudulent and non-fraudulent transactions in historical database. These techniques can be used to find clusters, groups with the same properties, or find outliers which are the "basic form of non-standard observation that can be used for fraud detection". Also, it can detect previous unknown fraud [21].

4.1 Supervised Technique

There are many researchers used neural networks for supervised credit card fraud detection include (Ghosh and Reilly 1994) [17], (Aleskerov, Ferisleben and Rao 1997) [2], (Dorronsoro, et al. 1997) [15], (Brause, Langsdor and Hepp 1999) [9] and (Guo and Li 2008) [19].

Shen et al. [25] compare the efficiency of three different classification models to credit card fraud detection problems. These models based on the data mining techniques including neural networks, logistic regression and decision tree. The results of their study confirm that the neural network and the logistic regression approaches do better than the decision tree.

4.2 Unsupervised Technique

Bolton and Hand [7] proposed two approaches to unsupervised credit card fraud detection through behavioral outlier detection techniques. These approaches are Peer point analysis and Break point analysis. The PGA aim to detect any individual account that begins to behave in different way from other accounts in the same peer group. The PGA work as following: After making some statistical analysis on the data, the PGA identifies peer groups for each individual account (target). The accounts in the peer group are the most similar accounts to the target account. Then, in each subsequent time point the behavior of target account will be compared with the summary of its group analysis. Those target accounts deviate from their peer groups will be flagged as outliers for further investigations.

Peer Group Analysis can detect a new type of fraud. However, it is unrealistic approach to credit card fraud detection because it is

very slow and the comparisons must perform immediately at the time of actual transaction. The problem with fraud detection is not just to detect the fraudulent transaction but it should detect them as quickly as possible. Also, when the peer group contains outliers the PGA will not detect the fraudulent account as an outlier [29].

Break Point Analysis is another method for unsupervised fraud detection. Bolton and Hand [7] define the break point as the time where anomalous behavior is detected. The BPA works on the account level only by comparing the sequences of transactions (their amount or frequency) to detect a change in the behavior of the account at a period of time. So, the unexpected increase in the amount of the transactions or its frequently can be considered as fraudulent behavior. It is not powerful like a peer group analysis because it is not using the information of other accounts. Furthermore, any change in the behavior does not necessarily mean it is fraud [29].

5. CREDIT CARD FRAUD PREVENTION TECHNIQUES

5.1 The Address Verification Service

The Address Verification Service (AVS) is a security technique used to prevent the online credit card fraud. This technique used by the merchant to check if the customer's billing address is matching with customer's file in the credit card issuer bank [11]. AVS technique takes the first five digits from the submitted street address and Zip code to be checked and matched with the customer's file in the issuer bank [27] .(see Figure 2)

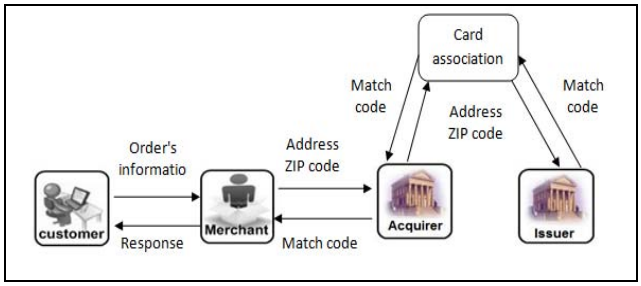

Figure 2 : Address Verification Service (AVS)

5.2 Card Verification Value 2 (CVV2)

CVV2 is stand for Card Verification Value 2. This value consists of three or four digit number printed on the front or back of the credit cards [24]. CVV2 is a security feature used to prevent fraud especially when the fraudster obtains the credit card number in the internet. And since he doesn't have a physical card, he will not be able know the card verification value (CVV2) [28].

5.3 Manual Review

Manual Review is a technique used by merchants to prevent the online credit card fraud by reviewing every order manually to decide which orders are fraudulent [6]. It is appropriate for small merchants with low numbers of orders but not for those merchants who have a huge number of sales. It is better to review only the orders which have high likelihood to be fraudulent [24].

5.4 Positive List and Negative List

Using of lists is considered to be the basic technique in any fraud prevention strategies. It is used by the merchants to identify returning customers if they are trusted customers or fraudsters. Usually, this list would contain these customers' information i.e. address, zip code, phone number, email and credit card number [22].

There are two types of lists: positive list and negative list. Positive list can be used to identify trusted customers. It contains the information about the customers who have a previous successful transaction. Negative list is used to reject customers' orders that have a previous fraudulent transaction. As a good example of a negative list is the Safe file provided by MasterCard. When a customer makes an order, the merchants must review the negative list to check before any approving request to authorization. By this way, the merchant will assure to reject only the order of the customer in the negative list [13, 6].

5.5 Customer Authentication

The customer authentication is a technique used to authenticate the authorized customers who want to make a purchase. Visa provides customer authentication services and it called **"Verified by Visa".** Also, MasterCard provides this service with name **"MasterCard SecureCode"** [22]. The the scenario of this technique works as the following: First, the customer must register with the issuer bank and take the PIN or password number. On the other hand, the merchant should registered though his issuer with the customer authentication services (i.e., Visa or MasterCard) to get the merchant plug-in software. Then, when the customer wants to make any online purchase, he will need to select the goods or services and provide his credit card information by filling the required form. After that, he will submit the form to the merchant, who will send the request to card association (i.e., Visa or MasterCard) by using the plug-in software. This request is to check if the customer is participating in the customer authentication service. If the customer is participating in this service, the card association will send a pop-up window to the customer. Then, the customer will need to enter the PIN or password number. Next, the issuer bank will validate the PIN or password and send the result to the merchant [18, 10, 22].

With Regards to the security issue in this technique, the communication between the issuer bank and the customer is secured. So, whenever the customer wants to make sure that the receiving pop-up window is from the card association and not a fake, there will be a secret message in that window which is only the customer know it. This message was given to him during his registration [22].

5.6 Trusted Email

AlFuriah et al. [3] proposed Trusted Email technique that was used to prevent fraudulent transaction on soft-product. The idea of the Trusted Email is considering the email address as the billing address in the physical shipment. The Authors provides a new version of the Address verification service (AVS) system which is called full address verification system (FAVS). It works like AVS but it verifies also the email address. The email address must be stored in the customer's file at the Issuer bank.(See Figure 4)

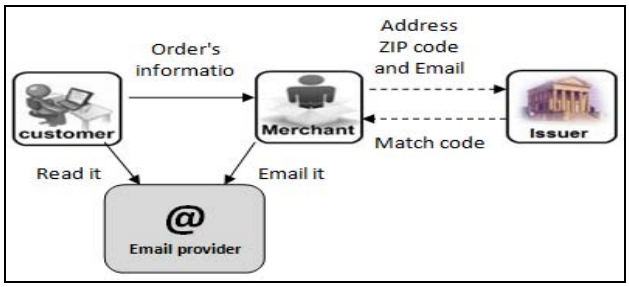

Figure 4: **New version of AVS [3]**.

The new version of AVS will work very well if someone commits a fraud. However, if the fraud committed by the credit card holder himself, the credit card issuer will face difficulties to prove the dispute is not correct. This is because the credit card issuer cannot request from the email provider (e.g. Hotmail or Yahoo) to check if the merchant send an email to the customer. So, the authors provided a trusted email server (TES) to overcome this problem. The trusted email server will required the customers, merchants and credit card issuer to have an account on the server. The customer must register his email with his credit card issuer. Then when a customer goes to the merchant's web site and performs an online purchasing, the merchant will request the Full Address Verification technique (FAVS). If the merchant receive a positive response, he will send the order to the customer by email. On the other hand, if the verification response is negative the merchant will inform the customer and give him another chance to enter the correct email.

When the fraud committed by the credit card holder, and he requests a charge back. The credit card issuer will be able to request the trusted email server to check if the merchant sent an email to the customer that was contained the soft-product or not. After verifying the above mentioned process the customer's dispute will be rejected or accepted [3]. (See Figure 5)

5.7 Biometrics

Biometrics is used to verify a personal identity through physiological or behavioral characteristics (e.g. Fingerprint, Hand geometry, Face, Iris and voice). It gives a very effective technique for authentication but the problem that it is very expensive to implement [22].

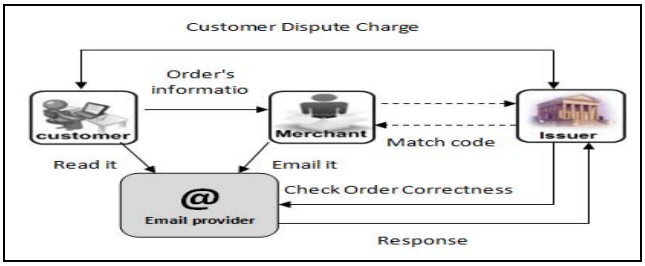

Figure 5: Trusted Email [3].

5.7.1 Securing Online shopping using Biometric Personal Authentication and Steganography

A.Ihmaidi et al. [1] proposed a system which will be using two techniques: fingerprint verification and steganography algorithm. In order to implement this technique the credit card issuer will request each customer to record his fingerprint. Then the issuer bank will gather all the information i.e. (cardholder name, Card number, expiration date…etc) and encrypt it. Then the fingerprint feature extraction and the encrypted information will convert to binary stream and embedded in the EISC image using steganography algorithm. Then the issuer will generate storage device that contain EISC and special software. Then the customer will be given this device to be used in each online purchasing.

When the customer needs to buy anything thru the Internet, the merchant will request either the required information in the traditional way or he will request to upload EISC image. Then the customer will open the software in the storage device then it will request the customer to use his fingerprint for verification. After that it will request him to add the amount of the order then the software will generate the EICS image. Each generated EISC image has a validation tag which means that it will be only used once. The validation tag contains a binary stream of the transaction amount and the transaction serial number. When the customer uploads the EISC image to the merchant site, it will be sent directly to the issuer. In order to verify this information the issuer will need to use special software to validate the sent EISC Image [1].

5.8 The Evaluation and Comparisons of Fraud Prevention Techniques

In the section 2 tabular format analysis will be presented the first one will be about Evaluation of fraud prevention techniques where multiple features are evaluated using the following scale **High (H), Medium (M), Low (L), NI (Not indicated), NE (Not exist)** (See Table 1 in APPENDIX) and the second one gives a summary of Advantages and disadvantages of fraud prevention techniques (see Table 2 in APPENDIX).

6. Conclusion

In this paper the e-payment credit card system was discussed. It presents the credit card fraud from different aspect including Credit card fraud definition, type of credit card fraud, fight against fraud and impact of credit card fraud. In addition, it presents the credit card detection techniques which are categorize into supervised techniques and unsupervised techniques. Moreover, it provides a survey for the existing credit card fraud prevention techniques. Also, it provides a comparison and evaluation between the prevention techniques.

Based on our comparison and evolution of the fraud prevention techniques, we found that the Trusted Email server is the best solution to prevent the credit card online fraud. So, as a future work we will try to build a prototype for the Trusted Email Server.

7. REFERENCES

[1] A.Ihmaidi, Hussam Ud-DIN, Ahmad Al-Jaber, and Amjad Hudaib. "Securing Online Shopping using Biometric Personal Authentication and Steganography." *Conference on Information and Communication Technologies.* IEEE, 2006. 233-238.

[2] Aleskerov, E, B. Ferisleben, and B. Rao. "CARDWATCH: A Neural Network Based Database Mining System for Credit Card Fraud Detection." *Computational Intelligence for Financial Engineering.* IEEE, 1997. 220-226.

[3] Alfuraih, Saleh I., Nient T. SUI Alsawi, and Dennis Mcleod. "Using Trusted Email to Prevent Credit Card Frauds in Multimedia Products." *World Wide Web: Internet and Web Information Systems, 5*, 2002: 245–256.

[4] ALFURAIH, SALEH, and RICHARD SNOW. "Location of Trusted Email for Prevention of Credit Card Fraud in Soft-Products E-Commerce." *the 4th WSEAS International Conference on Applied Informatics and Communications* . Wisconsin, USA : World Scientific and Engineering Academy and Society (WSEAS) , 2004. 1-6.

[5] AlFuraih, Saleh, Nient AlSawi, and Dennis Mcleod. "Trusted Email: A Proposed Approach to Prevent Credit Card Fraud in Softproducts E-Commerce." *Proceedings of the 6th International Conference on Enterprise Information Systems.* Porto, Portugal: April 14-17, 2004. 106-113.

[6] Bhatla, Tej Paul, Vikram Prabhu, and Amit Dua. *Understanding Credit Card Frauds.* Tata Consultancy Services, 2003.

[7] Bolton, Richard J., and David Hand. "Unsupervised Profiling Methods for Fraud Detection." *Conference on credit scoring and credit control.* Edinburgh, UK, 2001.

[8] Bolton, Richard J., and David j. Hand. "Statistical Fraud Detection: A Review."*Statistical Science , 17*, 2002: 235-255.

[9] Brause, R., T. Langsdor, and M. Hepp. "Neural Data Mining for Credit Card Fraud Detection." *Proceedings 11th IEEE International Conference on Tools with Artificial Intelligence* , Chicago, Illinois, USA*:* IEEE, 1999.103.

[10] Charlton, Kate, and Natalie Taylor. *Online Credit Card Fraud against small business.* Research and Public Policy Series, Australian Institute of Criminology, 2004.

[11] CyberSource. *Security Best Practices.* White paper, Lightbridge, Inc., 2006.

[12] CyperSource. *Fifth Annual UK Online Fraud Report* . CyperSource, 2009.

[13] CyperSource. *The Insiders Guide to Managing Card Not Present Fraud: Strategies to Maximise Sales and Minimise Fraud.* White paper, CyberSource, 2005.

[14] Dara, Jinthendra, and Laxmon Gundemoni. *Credit card security and e-payment.* Thises, Lulea university of technology, 2006.

[15] Dorronsoro, J. R., F. Ginel, C. Sanchez, and C. S. Cruz. "Neural Fraud Detection in Credit Card Operations." *IEEE Transactions on Neural Networks 8* (IEEE), 1997: 827-834.

[16] Ferdousi, Zakia, and Akira Maeda. "Unsupervised Fraud Detection in Time Series data." *Proceedings. 22nd International Conference on Data Engineering Workshops.* Georgia, USA : IEEE, 2006.

[17] Ghosh, Sushmito, and Douglas Reilly. "Credit Card Fraud Detection with a Neural-Network." *Proceedings of the 27th Annual Hawaii International Conference on System Science.* Maui, Hawaii : IEEE, 1994.

[18] GPayments. *Verified by Visa Overivew.* White Paper, Warriwood, Australia: GPayments, 2002.

[19] Guo, Tao, and Gui-Yang Li. "NEURAL DATA MINING FOR CREDIT CARD FRAUD DETECTION." *Proceedings of the Seventh International Conference on Machine Learning and Cybernetics.* Kunming: IEEE, 2008. 12-15.

[20] Hassler, Vesna. *Security Fundamentals for E-Commerce.* Boston: Artech House, 2001.

[21] Kou, Yufeng, Chang-Tien Lu, Sirirat Sirwongwattana, and Yo-Ping Huang. "Survey of fraud detection techniques." *International Conference on Networking, Sensing and Control.* Taipei , Taiwan: IEEE, 2004. 749 - 754.

[22] Montague, David. *Fraud Prevention Techniques for Credit Card Fraud.* Victoria,BC,Canada: TARFFORD, 2004.

[23] O'Mahony, Donal, Michael Peirce, and Hitesh Tewari. *Electronic Payment Systems for E-Commerce.* 2nd Edition. Boston: ARTECH HOUS, 2001.

[24] Paintal, Guntee. *Fraud Mnangement in the Online Retail Environment.* White paper, Infosys Technologies Limited, 2008.

[25] Shen, Aihua, Rencheng Tong, and Yaochen Deng. "Application of Classification Models ON Credit Card Frau Detection." *International Conference on Service Systems and Service Management.* Chengdu: IEEE, 2007. 1-4.

[26] Sinic, Dejan. "REDUCING FRAUD IN ELECTRONIC PAYMENT SYSTEMS." *The 7th Balkan Conference on Operational Research "BACOR 05".* Constanta , Romania, 2005.

[27] Visa. *Merchant Guide to the Visa Address Verification Service.* Visa U.S.A. Inc, 2008.

[28] Visa. *VISA CARD VERIFICATION VALUE 2 (CVV2) MERCHANT GUIDE.* U.S.A inc, 2002.

[29] Weston, Daivid J., David J. Hand, Naill M. Adams, Christopher Whitrow, and Piotr Juszczak. "Plastic card fraud detection using peer group analysis." *Advances in Data Analysis and Classification,2*, *Springer Berlin*, 2008: 45-62.

[30] Yufeng, Kou, Lu Chang-Tien, S Sirwongwattana, and Huang Yo-Ping. "Survey of fraud detection techniques." *International Conference on Networking, Sensing and Control.* Taipei, Taiwan : IEEE, 2004. 749 - 754.

APPENDIX

Table 1: Evaluation of fraud prevention techniques

		Techniques evaluation						
Features		**AVS**	**CVV2**	**Manual review**	**negative & positive lists**	**Customer Authentication**	**Trusted Email**	**Biometrics**
General	**Easy to use**	**H**	**H**	**M**	**H**	**H**	**H**	**M**
	Easy to implement	**H**	**H**	**M**	**H**	**H**	**H**	**L**
	Fast	**H**	**H**	**L**	**M**	**H**	**H**	**M**
	cost	**L**	**L**	**M**	**M**	**M**	**L**	**H**
Conceptual	**Cover charge back**	**M**	**M**	**NI**	**NE**	**H**	**H**	**H**
	Require any change to the system	**L**	**L**	**L**	**M**	**M**	**L**	**H**
	prevent the fraud	**M**	**M**	**L**	**L**	**H**	**H**	**H**
	Real time process	**H**	**H**	**NE**	**H or NE**	**H**	**H**	**H**
	Mostly used in 2008 (based on the Fifth Annual UK Online Fraud Report ,2009)	**H**	**H**	**H**	**Built-in-hose : (M) Shared service (L)**	**Verified by visa (H) MasterCard SecureCode (H)**	**NI**	**L**
	Merchant planed to implement the technique in 2009. (based on the Fifth Annual UK Online Fraud Report ,2009)	**M**	**M**	**M**	**Built-in-house (M) Shared service (M)**	**Verified by visa (H) MasterCard SecureCode :(H)**	**NI**	**H**
High (H) , Medium (M) , Low (L) , NI (Not indicated) , NE (Not exist)								

Table 2: Advantages and disadvantages of fraud prevention techniques.

Techniques	Advantages	Disadvantages
AVS	• It is easy, fast and one of the most risk management techniques the merchant can take [27]. • Reduce the risk of fraud [27]. • AVS will help the merchant to cover the charge back [27]. • There is no extra cost when using the AVS because the merchants can request this check as a part of an authorization request [22].	• Sometimes the customer's billing address is different from the one on the customer's file at issuer bank. As an example, the customer may order as a gift and send it to someone else [22]. • It is not a perfect indicator to the fraudulent behavior [22]. • The merchants need to change their system to deal with return AVS code [22] • . AVS is ineffective for the soft-product [4].
CVV2	• It reduces the Cardholder-not-present fraud [27]. • It prevents the counterfeit cards [22]. • There are no extra costs [22]. • It reduces the fraudulent charge back [28].	• CVV2 is not useful in the lost or stolen cards. • The fraudster can hacked into the online system then get the CVV2 [3] .
Manual Review	• It is more efficient when it using as an additional technique [13].	• It is not effective fraud prevention technique [22]. • Quality of work depends on the experience of the review employees [22]. • It is very expensive and consumes a lot of time [22].
Negative and Positive list	• The using of the lists is considered the basic technique in any fraud prevention strategies [22]. • The using of lists is very easy [22]. • Negative list is a good for prevent repeat fraud [22]. • Positive list reduce the time which taken to check a valid order [6].	• This list cannot use prevent identity theft fraud [13]. • The lists need a frequently updating [6].
Customer authentication	• It is a first tool provides a protection to the merchant from fraud-related charge back [22]. • The card association provides this technique to increase the customer confidence to perform an online purchasing [22]. • The total cost is approximately low [22]. • The customer authentication technique is an excellent tool to prevent the fraud [13]. • The charge back liability in this technique will be against the customer.	• Only the Visa or Master card customer can use this service. So, the merchant need to use additional fraud prevention techniques [22]. • The customers do not like this technique [13].
Trusted Email	• It is effective technique to protect the merchants from the fraud and minimize the charge back disputes [3, 5]. • Easy to implement and easy to use [3, 5]. • It is better than any other techniques using billing address or other code for verification [3, 5]. • Low cost [3, 5]. • It requires minimum changes for all parities in the e-payment system [3, 5]. • Not contains the drawbacks of other solution [3, 5].	Not indicated.
Biometrics	• Very effective technique to authentication a customer's identity [22].	• Difficult to implement. • Very expensive. • Require a lot of changes.