International Journal of Reviews in Computing

IJRIC

ISSN: 2076-3328 www.ijric.org E-ISSN: 2076-3336

ONLINE CREDIT CARD FRAUD PREVENTION SYSTEM FOR DEVELOPING COUNTRIES

[1]Rehab Anwer, [2]Shiraz Baig, [3]Dr. Malik Sikandar Hayat Khiyal, [4]Aihab Khan & [5]Memoona Khanum,

[1]Graduate, Department of Software Engineering,, Fatima Jinnah Women University, Rawalpindi, Pakistan

[2]Project Director,ERRA, Muzafarabad, Pakistan

[3]Chairperson, Department of Computer Science and Software Engineering, Fatima Jinnah Women University, Rawalpindi, Pakistan

[4]Assistant Professor, Department of Software Engineering, Fatima Jinnah Women University, Rawalpindi, Pakistan

[5]Lecturer, Department of Computer Science, Fatima Jinnah Women University, Rawalpindi, Pakistan

E-mail: rayhab123@gmail.com, shiraz_baig@yahoo.com, m.sikandarhayat@yahoo.com, aihabkhan@yahoo.com, dr.mahayat@gmail.com

ABSTRACT

Electronic commerce has gained a rapid growth and it has a significant impact on market of all the countries. Credit Card has become a de facto standard for online payments. This increase use of credit card has raised fraudulent practices across the world. There are no secure well defined ways to deal with credit card frauds in developing countries. This research focuses on "card not present" fraud in developing countries. Existing techniques of developed countries have been studied and a new system is proposed which consists of "predefined checks" and data is transmitted by using a pair of symmetric keys. After observing the attributes of fraudulent and non-fraudulent transactions "checks" have been proposed. The proposed system was tested on a data set and it successfully detected both fraudulent and non-fraudulent transactions.

Keywords: *Cardholders, card non present fraud, online payments, ip tracking.*

1. INTRODUCTION

Electronic Payment via credit card has brought profound changes in recent times. This system is widely accepted as it's convenient and simpler to use but credit card fraud has negative effect on its widespread usage.

In developing countries currently there exits less trend of buying things online from electronic shops, there are many reasons for that. One of them is the fraud associated with online payments, because of this the user don't feel comfortable in giving out there information such as credit card numbers and hence avoid purchasing stuff online. A new fraud prevention system is suggested for developing countries .The main purpose of the system is to provide the facility to distinguish fraudulent and legitimate transactions based on "predefined checks in online payments. So that only legitimate transactions are allowed with lowered fraud rates.

1.1 CONTRIBUTIONS

Address verification system (AVS) technique is commonly used to prevent online fraud in "card not present" transactions. This technique is carefully examined and new fraud prevention system is proposed which overcomes the flaws of the AVS technique. Credit card related frauds in online payments have increased rapidly. Many techniques have been designed to find ways to overcome credit card. Still no technique can provide solution for all types of fraud. As far as developing countries are concerned less work has been done to overcome this problem. Losses related with credit cards are rising quickly each year. This research model proposes a framework for "card not present" fraud. This fraud occurs

ISSN: 2076-3328 www.ijric.org E-ISSN: 2076-3336

mostly on internet or on phone, when the user does not physically present his card to the merchant. "Card not present" fraud is much difficult to detect as compared to "card present" fraud.

2. RELATED WORK

Jithendra Dara et al [1] carried out a research to study the ways the banks use to reduce the problems in credit card transactions. The security features used by the banks to protect transactions from fraudsters were also studied in detail. Data was taken from two financial institutions Sweden and India [1].

Micci-Barreca et al [2] proposed an e-payment system to detect fraudulent transactions of Card-Not-Present (CNP) based on data mining techniques. The basic principle was to determine indicators of fraudulent behavior by analyzing a huge amount of data [2].This framework has many parts such as warehouse, profiling module, software programs, a profiler monitor construction module, a storage component and a data mining classifiers modules like artificial neural network (ANN), Its working depends upon the "single detector" which has the capability to detect fraud effectively based on the profiler outputs [2].

Raghuveer Kancherla et al [3] proposed an architecture on which pattern changes at an individual account level are identified. In this architecture a technique called "trend offset analysis" or "TOA" is used .It is basically a supervised learning technique. Further in this model a signature is assigned to each account. The principle was to identify significant deviation in current behavior from the assigned signature, and it was used for outlier detection. The length of time period used to allocate a signature for every account was based on the computational ability of the system of implementation. TOA was compared with the global outlier detection model. This resulted in an incremental decrease in fraud losses [3].

Saleh Alehalfuraih Richard *et al* [4] proposed architecture that focuses on the use of Trusted Email mechanism to prevent credit card fraud. It prevents fraudulent transactions of soft-products. It basically consists of a email solution which identifies and authenticates the online customer. It not only prevents fraudulent transactions but also resolves disputes [4].

3.1 PRELIMINARIES

There are two types of card related frauds. First is online fraud and second is offline fraud. Offline fraud is done by using a stolen physical credit card. In Online fraud only the card details are required. It can be done by internet, phone shopping or cardholder not- present. [5]

3.1 CREDIT CARD FRAUDS

Online Credit Card fraud is one of the main hindrances in promoting Electronic Commerce in developing countries. To resolve this problem it is necessary to first gain in depth knowledge of the different types of online credit card fraud. There are many types of card related frauds. Lost or stolen card is one the most frequent type of fraud. Other kinds of fraud include skimming, Identity theft, counterfeit fraud etc [5]

4. FRAMEWORK OVERVIEW

In this research a model is proposed for fraud prevention for developing countries, it is proposed while keeping in resources of the developing countries. It basically consists of a client server environment. Fraud is a key dilemma in electronic transactions, preventing fraud in real time systems isn't an easy task, the basic approach followed in this system is to prevent fraud at an early stage, and rather than reporting fraud after it has been done.

For this purpose various fraud prevention techniques which have been used in the developed countries have been studied. A new model is proposed which tries to overcome the weaknesses of this system

1. Customer registers with customer's bank
2. Customers enters credit card details (credit card number, security code, expiry date)
3. Customers information is encrypted and sent to merchant
4. Merchant Decrypts the data
5. Merchant encrypts the data and sends it to acquirer bank

ISSN: 2076-3328 www.ijric.org E-ISSN: 2076-3336

6. Acquirer bank decrypts the data Acquirer bank verifies the data from issuer bank
7. Issuer bank executes the "checks"
8. Issuer bank sends the result to acquirer bank
9. Acquirer bank sends message to merchant
10. Merchant sends a success message to customer if all checks are true
11. Merchant sends a failure message to customer if any check is not true
12. Merchant sends an email notification to the customer.

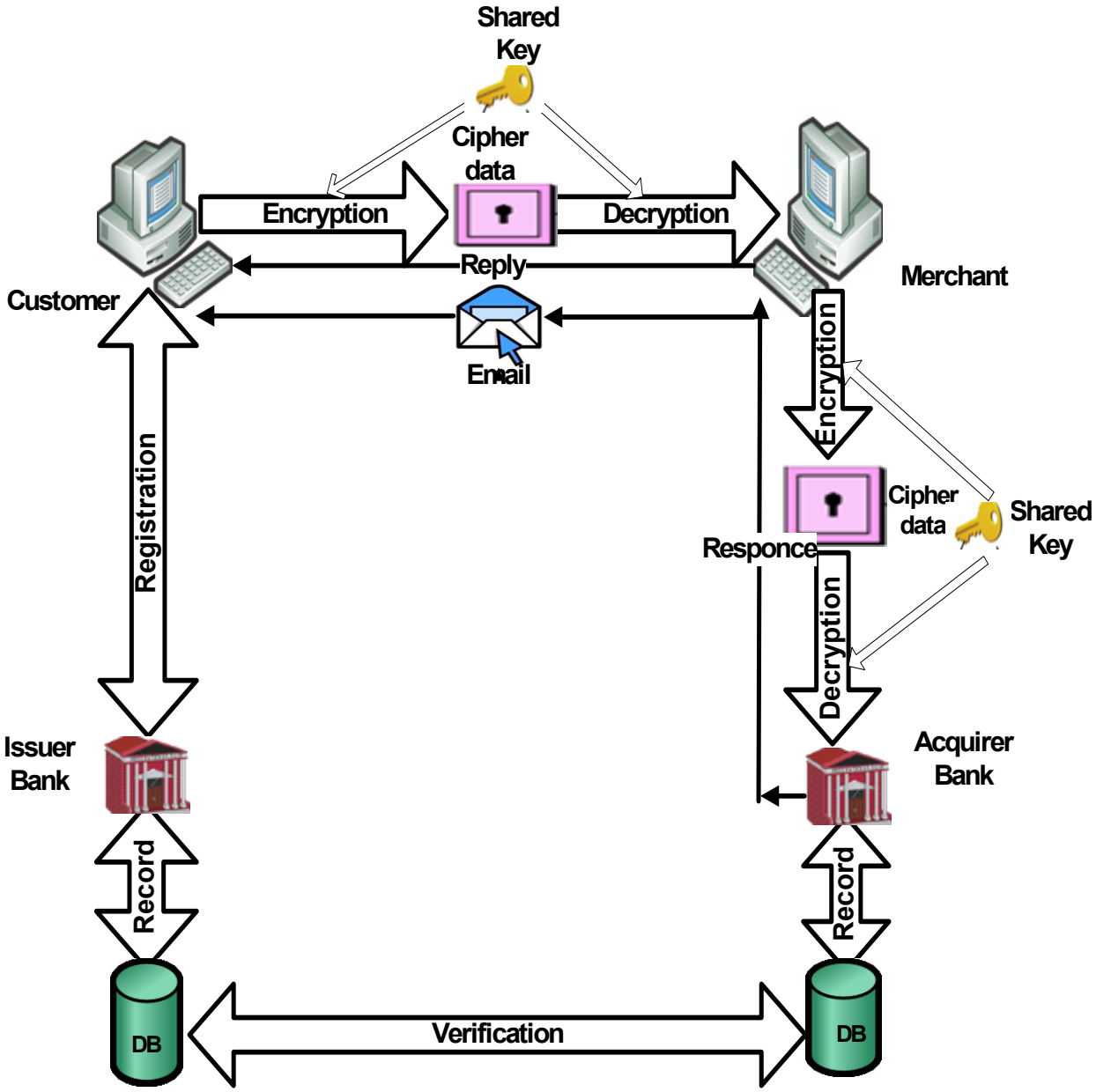

Fig 1:Framework of Proposed System

ISSN: 2076-3328 www.ijric.org E-ISSN: 2076-3336

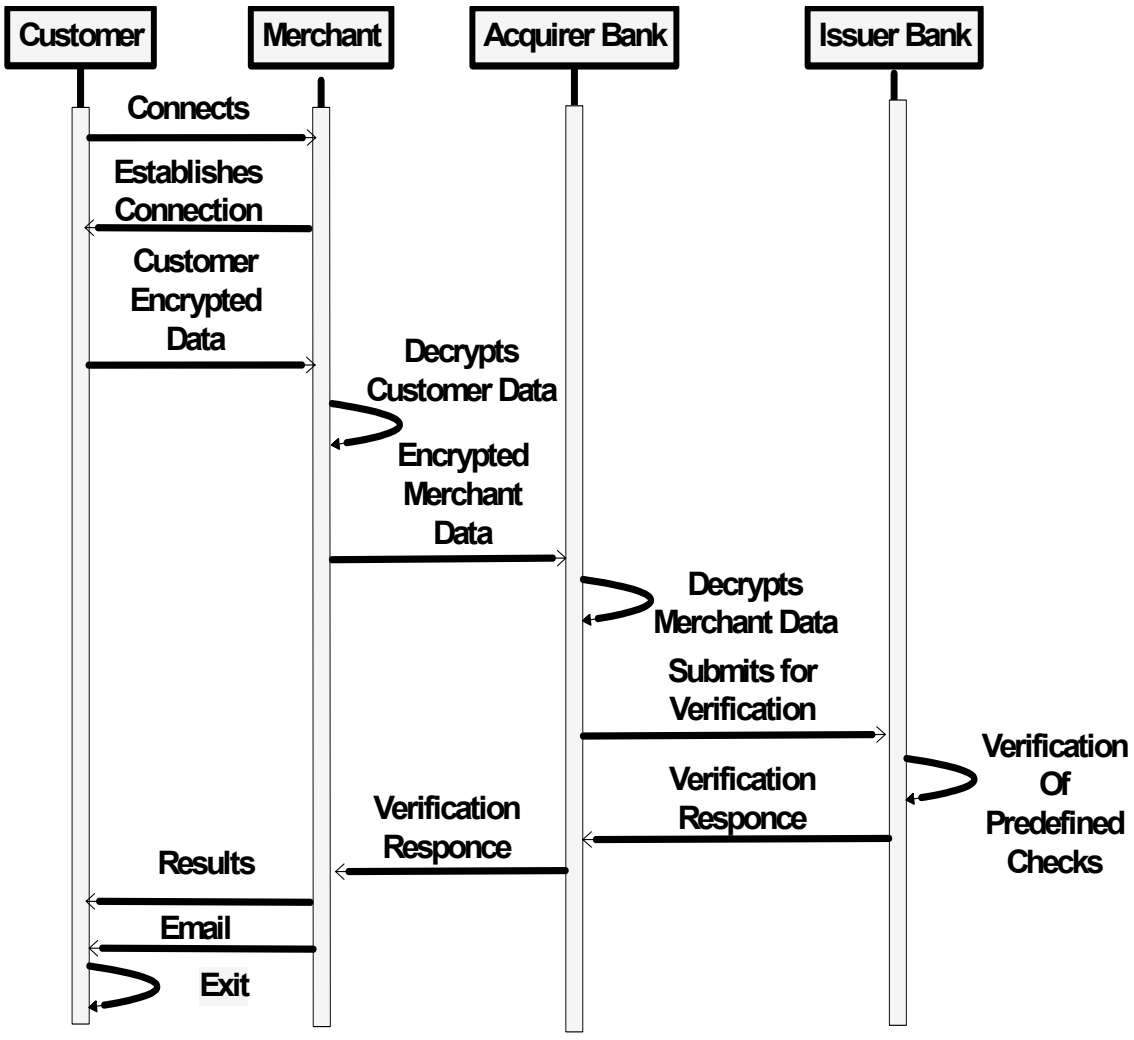

Fig 2: Sequence Diagram of Proposed Model

5. TECHNIQUE

5.1Adress Verification System (AVS)

In AVS the numeric portion of the address is matched. The information collected from the cardholder's billing address is matched with the billing information record of the card issuer. After this a match or mismatch response is generated and returned [6].

5.1.1Advantage

1. It provides some level of protection against the most common account takeover schemes, specifically card generators and credit-card skimmers [2]

ISSN: 2076-3328 www.ijric.org E-ISSN: 2076-3336

5.1.2 Disadvantage

1. Only billing address is matched and validated in AVS.
2. The AVS provides protection in card present transactions in which either the customer has a face-to-face meeting with the merchant or the merchant is actually shipping a package or the like to the address of a customer. However, for online service providers or merchants, address and identity information are generally insufficient to verify[7]
3. AVS is often not available for international cards[7]
4. AVS is not useful for checking the purchase of non-physical goods because the goods are not shipped to the buyer's physical address. [7]

5.1.3 Algorithm

The algorithm proceeds in three steps:

1. System reads credit card numbers
2. The system matches the billing address of the card holder with the already stored address
3. If true, then transaction is allowed
4. Else it is fraudulent

5.2 PROPOSED FRAUD PREVENTION TECHNIQUE

The proposed system consists of many "checks" which are discussed as follows:

Check 1: Lost /stolen (LS)

In this check the credit card number checked that whether it has been reported as a lost credit card or stolen credit card by the cardholder .If the above check is true then transaction won't be allowed, else check 2 will be executed

Check 2: Credit Card Validation (Val)

The credit card number is validated using luhn algorithm, if the result of validation is true then the number will be consider as valid, and check 3 will executed, else transaction won't be allowed

Check 3: Security Code Check (SC)

In this check Security code for each card is checked (card verification value).If it is true, and then check 4 will be executed, else transaction won't be allowed

Check 4: Expiry (Exp)

It checks for valid expiry date. If it is not true, then transaction won't be allowed else check 5 will be executed

Check 5: Multiple IP (MIP)

These checks notes whether same credit card number has been entered from two IP's by comparing time difference between two transactions. If it is true, then transaction won't be allowed else check 6 will be executed

Check 6: Repeated IP (RIP)

This check makes sure that only 1 transaction from the same credit card number and same IP is allowed in 30 minutes. If it is not true, then transaction won't be allowed else it will be executed .The basic idea behind this check is that the customer is in facts not the cardholder and is trying to utilize the card at a large amount as achievable

5.3 ADVANTAGES OF PROPOSED MODEL

1. Lost and stolen card feature makes it easier to stop fraudulent transactions
2. Credit card validation checks detects errors in a sequence of numbers, hence detects valid an invalid numbers easily
3. IP tracking gives details of customer's country
4. Multiple IP(MIP) check makes sure that only one credit card can be used from one IP at a time
5. Repeated IP(RIP) check restricts customer from using a card within small interval of time
6. Security code provides protection from skimmers. Security code ensures that the person submitting the transaction is in possession of the actual card.

ISSN: 2076-3328 www.ijric.org E-ISSN: 2076-3336

7. The proposed system uses symmetric key algorithms which have the advantage of consuming less time

5.4 COMPARATIVE ANALYSIS OF PROPOSED AND EXISTING MODEL

In table 1 comparison of AVS and proposed system is given

Characteristic	Address Verification System	Proposed System
Lost/Stolen Fraud	No Protection	Provides Protection
Credit Card Validation	No	Yes
Skimming Fraud	Provides Protection	Provides Protection
Assumed Identity	No Protection	Provides Protection
Counterfeit Cards Fraud	No Protection	Provides Protection
IP Tracking	No	Yes
Email Notification	No	Yes

Table 1 Comparative Analysis of Proposed and Existing Technique

6.1 TESTING AND RESULTS

To conduct experiments a data set of 500 valid credit card numbers was used for testing purposes [8]. The CVV for each credit card number was obtained through CVV generation software. The obtained data set was used to test all checks related to Credit Card fraud prevention in proposed system.

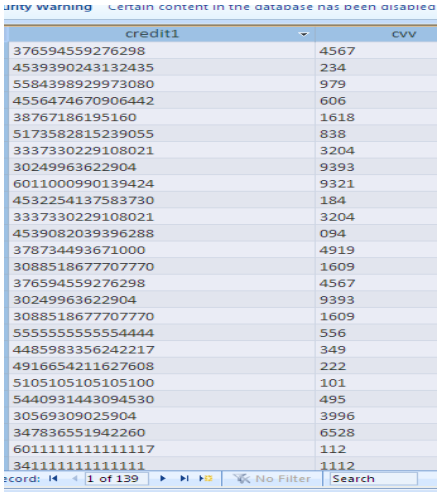

Fig 3: Data Set

6.1.1Generation of Security Code for Testing

The security code for each credit card obtained from was generated with the help of "CVV generator" software. This was done to make sure that the softwares perform well on real life environment.

6.3 Sample Test

Below is shown the result of 3 transactions out of were fraudulent, the details of transactions are given as follows

6.3.1Transaction 1

Customer entered same credit card number and from same IP with in time interval of 30 minutes

6.3.1.1 Expected output

Make sure that repeated IP (RIP) check is detected and transaction is not allowed

6.3.1.2 Proposed System Output

ISSN: 2076-3328 www.ijric.org E-ISSN: 2076-3336

Fig 4: Test No 1

6.3.2 Transaction 2

Customer entered invalid credit card number and invalid expiry

6.3.2.1Expected output

Make sure that invalid Credit Card number and invalid expiry date is detected and transaction is not allowed

6.3.2.2 Proposed System Output

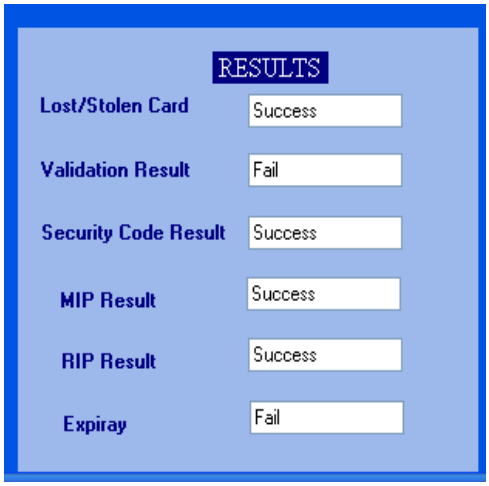

Fig 5: Test No 2

6.3.3 Transaction 3

Customer entered invalid credit card number and invalid security Code

6.3.1Expected output

Make sure that invalid Credit Card number and invalid security code is detected and transaction is not allowed

6.3.1.2Proposed System Output

Fig 6: Test No 3

6.4 GRAPHICAL RESULTS

In figure number 7, graphical representation of the test conducted is shown, for testing purpose the AVS based system was also implemented in order to get accurate results.

X axis =fraud checks

Y axis = Fraud Prevention Systems

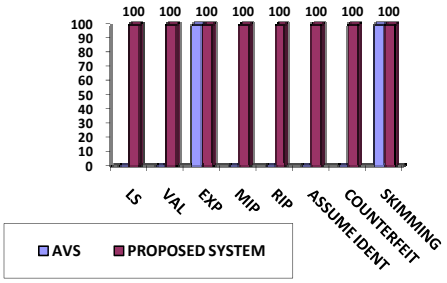

Fig 7: Graphical Result

In Figure 7 the results show that both systems provide protection against the Skimming fraud as AVS uses matches the shipping address and the proposed system matches the security code for each card. Proposed system performs credit card

ISSN: 2076-3328 www.ijric.org E-ISSN: 2076-3336

validation by using luhn algorithm, it also provides prevention against "assumed identity" and "counterfeit" fraud, and finally it also maintains each transaction's IP record, these features are not present in AVS.

7.1 CONCLUSION

Electronic Payment system has brought a lot of changes in recent times. The most commonly used electronic payment method for electronic transactions is credit card. It is popular because of its simplicity of use. This also has raised credit card frauds. As far as developing countries are concerned, they have not yet designed any secure payments with credit card fraud prevention. The proposed system provides the ability to prevent fraudulent and legitimate transactions. The proposed system is user friendly and secure. The proposed system provides the ability only to the legitimate user to execute transaction. The existing technique offered in developed countries is also implemented. It found that Proposed system or is more efficient and secure than existing technique. Proposed system also provides protection against stolen credit card fraud which existing system fails to provide.

7.2 FUTURE ENHANCEMENT

We designed an electronic payment system to prevent fraud in "card not present" transactions. This system is capable of providing most of the essential features required to prevent fraudulent and legitimate transactions. As technology changes, it becomes difficult to track the behavior and pattern of fraudulent transactions. Preventing known and unknown fraud in real-time is not easy but it is feasible. The proposed architecture is basically designed to prevent credit card fraud in online payments, and emphasis is made to provide a fraud prevention system to verify a transaction as fraudulent or legitimate. For implementation purposes it is assumed that issuer and acquirer bank is connected to each other. If this system is to be implemented in developing countries then exchange of best practices and raising consumer awareness among people can be very helpful in reducing the losses causes by "card not present" transactions. Further enhancement can be done by making this system secure with the use of certificates for both merchant and customer and as technology changes new checks can be added to understand the pattern of fraudulent transactions.

8. REFERENCES:

[1]Credit Card Security and E-payment, Enquiry into credit card fraud in E-Payment, Jithendra Dara, Luleå University of Technology, 2006

[2]Unawed by fraud: new techniques and technologies have been enlisted in the fight against online fraud, by Micci-Barreca, Daniele, Security Management, Electronic Commerce, Sept, 2003

[3] S Alfuraih, "Location of Trusted Email for Detection of Credit Card Fraud in Soft-Products E-Commerce", 2004

[4] Saleh I. Alfuraih, Nie n T. Sui and Dennis McLeod, "Using Trusted Email to Detect Credit Card Frauds in Multimedia Products", 2002

[5]Survey of Fraud Detection Techniques Yufeng Kou, Chang-Tien Lu, Sirirat Sirwongwattana, Dept. of Computer Science, Virginia Polytechnic Institute and State University Falls Church, VA 22043, USA and Yo-Ping Huang Dept. of Computer Science and Engineering Tatung University, Taipei, Taiwan 1045

[6]http://www.fraudscreening.com/WhatIsFraud.html, July 2009

[7] http://www.freshpatents.com/Method-of-processing-online-payments-with-fraud-analysis-and-management-system,26 May 2009

[8]http://sqa.fyicenter.com/Online_Test_Tools/Test_Credit_Card_Number_Generator.php,12 July 2009

ISSN: 2076-3328 www.ijric.org E-ISSN: 2076-3336

BIOGRAPHY:

1. **Dr.M.Sikandar H.Khiyal** born at Khushab, Pakistan. He is Chairperson Dept. Computer Sciences and Software Engineering in Fatima Jinnah Women University Pakistan.He Served in Pakistan Atomic Energy Commission for 24 years and involved in different research and development program of the PAEC. He developed software of underground flow and advanced fluid dynamic techniques. He was also involved at teaching in Computer Training Centre, PAEC and International Islamic University. His areas of interests are Numerical Analysis, Analysis of Algorithm, Theory of Automata and Theory of Computation. He has more than eighty research publications published in National and International Journals and Conference proceedings. He has supervised more than sixty research projects at graduate and postgraduate level.

2. **Aihab Khan** works as Assistant Professor in Department of Software Engineering Sciences Fatima Jinnah Women University Pakistan. His research interests are in the field of Data Mining, Data Warehousing as well as Information security.

3. **Shiraz Bag** received his degree of civil engineering in 1975 with silver medal and strategic studies in 1992 and IT in 2005, with gold medal. He has worked on computers since 1976. Mostly worked on networking and communications. Wrote a book on network programming in 2004 winning national award. Have been managing a software house and has remained head of IT of large enterprise for 9 years. Currently, working as a visiting faculty in Islamic International University and Fatima Jinnah Women University, Pakistan.

4. **Rayhab Anwar** did Bachelors of Software Engineering from Fatima Jinnah Women University, Pakistan in 2009

5. **Memoona Khanum** works as lecturer in Department of Computer Science Fatima Jinnah Women University. Her research interests are in the field of Data Mining, Data warehousing, Artificial Intelligence and Algorithms. She received her MS degree from International Islamic University Islamabad