# MASTER CARD FRAUDS IN MOBILE AND WIRELESS COMPUTING EPOCH

*S.A.SathyaPrabha*[1]

**ABSTRACT**

Today belongs to "Mobile computing" i.e., any place any time computing. During this current period, the growing of electronic gadgets - that will associate an integral part of the business and the personal world, brings many challenges to secure the devices from a cyber-crime. These MasterCard frauds and each one of the new trends in cyber-crime that is more important in mobile computing M- COMMERCE and M-Banking. The developments of wireless technology have increased this new mode of operation for the public. This can be true or MasterCard process too. MasterCard (or debit card) fraud may be involves the unlawful the use of a stolen MasterCard information for the purpose of purchasing and to transfer funds from it. This article was mainly focuses on numerous types of MasterCard frauds and aims to help the users, against the fraud to prevent the precautions.

***Keywords:*** Mobile Computing, Wireless Computing, Credit card, Types of Frauds, Techniques, Genetic Algorithm

**Mobile Computing:**

Mobile computing could be a broad term that refers to a bunch of devices that permits individuals to access information and data from wherever they are. Generally noted as "human-computer interaction," mobile computing transports information, voice, and video over a network via a mobile device [2].

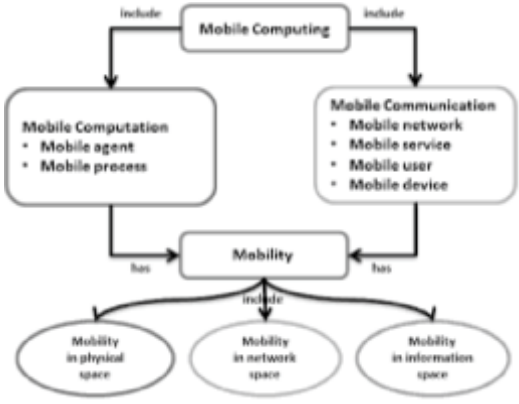


Fig 1: Wireless Computing

**Wireless Computing:**

Wireless USB (WUSB) can be a mode of Universal Serial Bus (USB) technology that uses radio-frequency (RF) links rather than cables to supply the interface between a laptop and peripherals such as the monitors, printers, external drives, head sets, MP3 players, digital cameras, conductor telephones, mobiles etc. [3].

**Types of Current Wireless Systems :**

1. Cellular system
2. Wireless LANs
3. Satellite System
4. Paging System
5. Bluetooth

Asst.Professor, Dept of CS,CA & IT, KAHE

**Elements of Credit Card Fraud :**

Debit/credit card fraud is committed when a person:

1) Fraudulently obtains, takes, signs, uses, sells, buys, or forges somebody else's credit or charge account credit or card information [3];

2) Uses his or her own card with the information that it is revoked or invalid or that the account lacks enough funds to get hold of the things purchased [5]; and

3) Sells merchandise or services to somebody else with information that the account is accessed illegally or is being used without authorization [1][3].

**Types of Credit Card Fraud :**

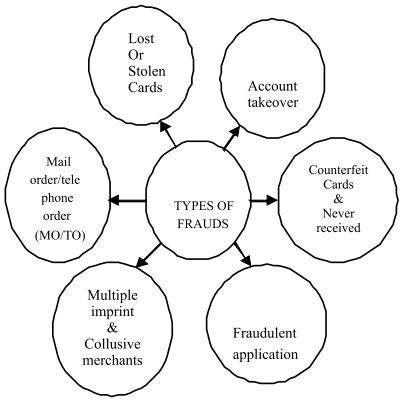


Fig 2: Types of Credit Card Frauds

- lost or taken cards [2].
- "account takeover" - once a cardholder inadvertently offers personal access details [3][5].
- Counterfeiting or "Skimming" is an illegal way of copying the magnetic tape on a legitimate master card through atiny low hand-held device called a "skimmer". Criminals use the data captured by skimmers to clone and build fake payment cards [5]
- Never received.
- Fraudulent application.
- "multiple imprint"- multiplying several times one recorded dealing on ancient MasterCard imprint machines referred to as "knuckle busters".
- Collusive business persons - once merchant workers work with fraudsters to chisel banks [1].
- Mail order/telephone order (MO/TO) fraud.

**Prevent Technology-wise theft :**

1) Use of MasterCard on Public laptop

2) MasterCard Photocopy as Id Proof/Authorization letter

3) Deceitful Calls

4) MasterCard payment through Mobile/ MobileApps

5) Prevention is healthier than Cure

**Credit Card Detection Techniques :**

Presently various algorithms are used to survey master card frauds[5]. A number of the Techniques are used for the purpose:

- Artificial Neural Network (ANN)
- Genetic formula (GA)
- Hidden Markov Model (HMM)
- Support Vector Machines (SVM)
- Bayesian Network
- Fuzzy Neural Network
- Expert Systems
- Decision Tree (DT).

This paper discusses the implementation of Genetic Algorithm and the way it is utilized in MasterCard Fraud Detection Systems.

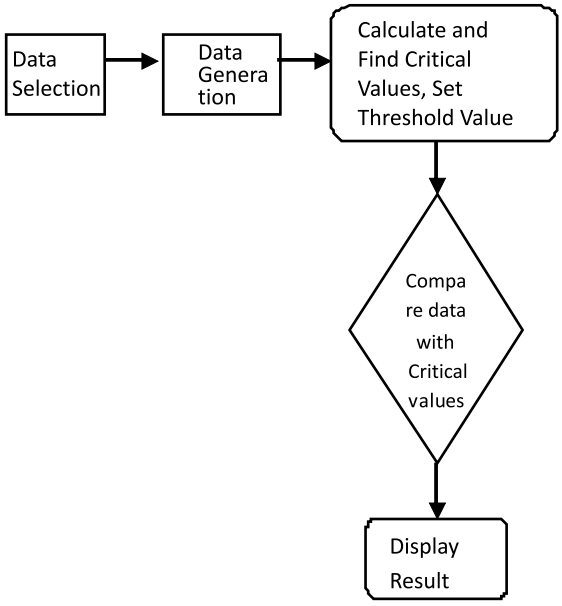


Fig 3: A Simple Method of Genetic Algorithm

Genetic Algorithm can be combined with other techniques to improve security and optimize their parameters [4].

**System Implementation Plan:**

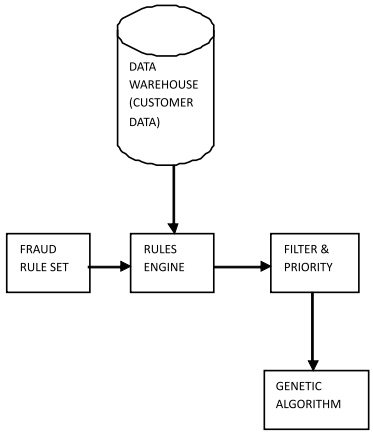


Fig 4: System Architecture

The system design defines the fundamental work of the model. The customer's confidential data was hold within the ware house, which is inserting to the rule engine that accommodates fraud rule set. And therefore the fraud rule set values can feed to the filer & priority, finally that knowledge set can input to the Genetic algorithm.

The initial population is chosen indiscriminately from the sample space that has many populations. The fitness value is calculated in each population and is sorted out. The Crossover is calculated victimization single purpose likelihood. Mutation mutates the new offspring victimization uniform likelihood live.

The new population is generated and undergoes a similar methodology it most kind of generation is reached as in step 3.

**Pseudo code for Genetic rule :**

1. Initialize the population
2. Evaluate initial population
3. Repeat
4. Perform competitive choice
5. Apply genetic operators to come up with new solutions
6. Valuate solutions within the population
7. Until some criteria is met.

**Basic Genetic Algorithm :**

1. [Start] Generate random population of n chromosomes (suitable solutions for the problem)
2. [Fitness] Evaluate the fitness f(x) of each chromosome x in the population
3. [New population] Create a new population by repeating following steps until the new population is complete

1. [Selection] Select two parent chromosomes from a population according to their fitness (the better

fitness, the bigger chance to be selected)

2. [Crossover] With a crossover probability cross over the parents to form a new offspring (children). If no crossover is performed, offspring is an exact copy of parents.
3. [Mutation] With a mutation probability mutate new offspring at each locus (position in chromosome).
4. [Accepting] Place new offspring in a new population
4. [Replace] Use new generated population for a further run of algorithm
5. [Test] If the end condition is satisfied, stop, and return the best solution in current population
6. [Loop] Go to step 2

**Conclusion :**

Among all the techniques the genetic formula works with repetitive information and easy to integrate with totally different systems. This paper provides a general understanding for the MasterCard fraud detection. This article is converse about the MasterCard fraud components and its kinds, and also to stop against the theft in every technology level and user level. And it also focuses on implementing Genetic algorithm in Master card fraud detection. Currently, MasterCard risk observance system is one of the key tasks. There are many ways to detect MasterCard fraud. Genetic Algorithm or the combination of any other card detection algorithm formula is applied in MasterCard fraud detection system; the possibility of fraud transactions is foreseen and prevented from the unauthorized user access. To boot the lot of improvement of the other techniques may result into a lot of strong detection methodology.

**References :**

[1] Linda Delamaire (UK), Hussein Abdou (UK), John Pointon (UK), "Credit card fraud and detection techniques: a review", Banks and Bank Systems, Volume 4, Issue 2, 2009 .

[2] Khyati Chaudhary, Jyoti Yadav, Bhawna Mallick, "A review of Fraud Detection Techniques: Credit Card", International Journal of Computer Applications (0975 - 8887) Volume 45- No.1, May 2012 .

[3] Vladimir Zaslavsky and Anna Strizhak," credit card fraud detection using selforganizing maps", information & security. An International Journal, Vol.18,2006.

[4] L. Mukhanov, "Using bayesian belief networks for credit card fraud detection," in Proc. of the IASTED International conference on Artificial Intelligence and Applications, Insbruck, Austria, Feb. 2008, pp. 221-225.

[5] Abhinav Srivastava, Amlan Kundu, Shamik Sural and Arun K. Majumdar, "CreditCard Fraud Detection Using Hidden Markov Model" IEEE, Transactions On Dependable And Secure Computing, Vol. 5, No 1. , January-March 2008

[6] V. Bhusari, and S. Patil, "Study of Hidden Markov Model in Credit Card Fraudulent Detection", International Journal of Computer Applications (0975 - 8887) Volume 20- No.5, April 2011