

Credit Card Fraud Detection

V. Rajaraman¹, P. Madheswari², B. Sandhiya³, C. Sandhiya⁴

¹Assistant Professor, Dept. Computer Science & Engineering, Adhiyamaan College of Engineering, Hosur, India

^{2,3,4}Student, Dept. Computer Science & Engineering, Adhiyamaan College of Engineering, Hosur, India

Abstract: The use of credit score playing cards for electronic and everyday purchases, as is the fraud related to it, is increasing exponentially. There are many transaction of fraud every day. Transactions of credit score playing cards at the moment are popular, as are the frauds associated with them. The card statistics is now being examine through automated teller machines (ATMs), shop readers, bank, and is also being utilized in on-line net banking. They have a restrained number of cards that is extraordinarily essential. Its protection is primarily based on the plastic card's physical protection in addition to the credit card variety's privacy. Fraud Detection Systems (FDS) are automatic gadget-based totally learning systems utilized by credit card companies to become aware of fraudulent transactions even before enter from give up-users. The goal of such an application is to identify fraudulent transactions earlier than they may be delivered to the database and for this reason save you fraud. They have a unique card range that's of extreme significance. Its safety relies at the physical safety of the plastic card as well as the privacy of the credit card variety. Using the Credit card quantity purchase by on line. Fraud detects user discover the Threshold cost. Without delay and that they have plenty fear to technique them. The predominant aim of the challenge is to provide security for ladies. The cause of the challenge is to offer safety for women.

Keywords: Fraud Detection System (FDS).

1. Introduction

We are living in a global which is hastily adopting virtual payments systems. Credit card and bills corporations are experiencing a completely speedy boom in their transaction volume. Along with this alteration, there's also a fast growth in economic fraud that happens in these price structures. A powerful fraud detection gadget need to be able to discover fraudulent transactions with high accuracy and efficiency. In day after day existence credit score playing cards are used for getting items and services with the help of virtual card for on line transaction or bodily card for offline transaction. In a physical-card based buy, the cardholder provides his card physically to a service provider for making a charge. To perform fraudulent transactions in this kind of purchase, an attacker has to scouse borrow the credit score card. If the cardholder does no longer understand the loss of card, it may result in a considerable economic loss to the credit card agency. While it is vital to save you awful actors from executing fraudulent transactions, it is also very important to make sure actual users aren't avoided from getting access to the bills gadget. A large number of false positives can also translate into terrible customer enjoy and may lead clients to take their

commercial enterprise someplace else. A foremost challenge in applying ML to fraud detection is presence of incredibly imbalanced facts sets. In many available datasets, majority of transactions are genuine with a very small percentage of fraudulent ones. Designing a correct and efficient fraud detection machine this is low on fake positives however detects fraudulent interest successfully is a huge venture for researchers. As credit score card will become the most famous mode of fee for both online as well as normal purchase, cases of fraud related to it are also growing. In this paper, we model the collection of operations in credit score card transaction processing using Threshold and show how it may be used for the detection of frauds. At the equal time, we try to ensure that authentic transactions aren't rejected. We gift distinct experimental effects to show the effectiveness of our technique and compare it with other techniques to be had within the literature.

2. Literature survey

A. *FORCE: Fully off-line relaxed credit for cellular micro bills*

Authors: Vanesa Daza; Roberto Di Pietro; Flavio Lombardi; Matteo Signorini

Abstracts: Payment schemes based on mobile gadgets are anticipated to supersede conventional electronic price techniques within the following few years. However, contemporary solutions are restricted in that protocols require at the least one of the two parties to be online, i.e. Linked both to a depended on 1/3 party or to a shared database. Indeed, in cases in which patron and supplier are persistently or intermittently disconnected from the community, any online charge is not viable. This paper introduces FORCE, a unique mobile micro fee approach where all concerned parties may be fully off-line. Our solution improves over state-of-the-art tactics in phrases of charge flexibility and safety. In fact, FORCE is based solely on nearby information to perform the requested operations. Present paper describes FORCE structure, components and protocols. Further, a thorough evaluation of its purposeful and security residences is furnished displaying its effectiveness and viability.

Algorithm:

- FORCE
- Secret key extraction Algorithm

Disadvantages:

- They are limited to consumer authentication whilst blindly relying on trusting the bank for transactions (as for credit score playing cards).
- The troubles affecting virtual currencies, which includes digital trade, are past the scope of the proposed solution and could now not be analyzed right here.

B. Hacking Point of Sale: Payment Application Secrets Threats and Solutions

Authors: S. Gomzin

Abstracts: Nearly five million point-of-sale (POS) terminals process about 1,500 credit and debit card transactions every second in the United States alone. 1, 2, 3 Most of these systems, regardless of their formal compliance with industry security standards, potentially expose millions of credit card records—including those being processed in memory, transmitted between internal servers, sent for authorization or settlement, and accumulated on hard drives. This sensitive data is often weakly protected or not protected at all. It is just a matter of time before someone comes along and takes it away.

Algorithm:

3DES

Disadvantages:

It's viable to brute-pressure in finite time on current processors, so no-one makes use of it for whatever extreme anymore. Also, some password systems secured with 3DES have been limited to eight characters and would silently truncate otherwise-relaxed passwords.

C. A proxy blind signature scheme and an off-line digital cash scheme

Authors: Jianhua Liu; Yan Hu

Abstracts: Due to the excessive-speed, low-price ubiquity of the net and wireless networks get entry to, the digital commerce has attracted full-size interest from both academia and industry inside the beyond decade. Electronic coins (e-cash) is a famous billing mechanism for electronic transactions considering that it can absolutely defend the anonymity and identity private of customers in numerous electronic transactions. To help retreating and storing money from all levels of the financial institution for the clients inside the actual world, on this paper, we advocate a proxy blind signature scheme and an e-coins scheme based on the new proxy blind signature scheme. The proxy blind signature scheme is proved cozy inside the Random Oracle Model beneath the chosen-target computational Diffie-Hellman assumptions, and the e-coins scheme can offer enforceability of e-cash, anonymity of honest customers and green traceability of double spending.

Algorithm:

Asymmetric Cryptosystem

Demerits:

Decisional Diffie-Hellman problem

Time consuming Problem

D. Continuous and Transparent User Identity Verification for Secure Internet Services

Authors: Andrea Ceccarelli; Leonardo Montecchi; Francesco Brancati; Paolo Lollini; Angelo Marguglio; Andrea Bondavalli

Abstracts: Session control in allotted Internet offerings is traditionally primarily based on username and password, explicit logouts and mechanisms of consumer session expiration the usage of conventional timeouts. Emerging biometric answers allow substituting username and password with biometric statistics at some stage in consultation established order, however in such an approach nevertheless a single verification is deemed sufficient, and the identity of a consumer is taken into consideration immutable for the duration of the whole session. Additionally, the duration of the session timeout can also impact on the usability of the service and consequent purchaser pride.

Algorithm:

CASHMA Authentication

Continuous Authentication Algorithm

Demerits:

Device Cost High.

CASHMA sometime misbehave.

E. A novel micropayment scheme with variable denomination

Authors: Quan-Yu Zhao, Yi-Ning Liu, Gao Liu and Chin-Chen Chang

Recently, the studies of micropayment structures have attracted a number of attention within the literature. Because of its unique characteristic that large quantity of transactions may additionally occur even as every transaction simplest deals with small value, no longer most effective security however also efficiency ought to be carefully considered in these systems, especially when considering that these structures may be carried out in useful resource con-strained cellular gadgets. In this paper, a unique lightweight micropayment scheme with variable denomination is pro-posed. Compared with those existing schemes with xed denomination, our proposed scheme now not best ensures safety goals, but additionally dramatically reduces the computational fee in addition to the storage burden.

Algorithm:

Micropayment Scheme to Return Changes

Demerits:

Diffie Hellman Problem Occurs.

F. A survey on continuous user identity verification using biometric traits for secure internet services

Authors: Harshal A. Kute, D. N. Rewadkar

Abstracts: Security of the internet based offerings is grow to be serious problem now-a-days. Secure person authentication may be very essential and fundamental in most of the structures User authentication systems are historically based totally on pairs of username and password and affirm the identification of the user handiest at login segment. No tests are accomplished all through working classes, which are terminated by using a

specific logout or expire after an idle interest duration of the consumer. Emerging biometric answers provides substituting username and password with biometric statistics for the duration of session established order, however in such a method nonetheless a single shot verification is less sufficient, and the identity of a consumer is taken into consideration everlasting during the entire consultation. A simple answer is to use very quick consultation timeouts and periodically request the consumer to enter his credentials time and again, however this isn't always a definitive answer and closely penalizes the provider usability and in the long run the delight of customers. This paper explores promising alternatives presented by means of applying biometrics in the management of periods. A cozy protocol is described for perpetual authentication via continuous consumer verification. Finally, using biometric authentication allows credentials to be obtained transparently i.e. without explicitly notifying the user or requiring his interplay, that is crucial to guarantee higher carrier usability.

Technique:

Biometric Device

Demerits:

Cost High (biometric device)

G. Multiple verification for continuous secure user authentication

Authors: Poonam Mahale, Niranjana Bhale

Abstracts: In the sector of internet offerings secure internet services is essential trouble. Traditional allotted net offerings are primarily based on session control of username password, logouts and person session expiration based on timeouts. Biometric authentication gives option to replacement password with biometric statistics in session advent with unmarried verification. In proposed paintings, additional degree of protection can be furnished & multiple verification can have deployed for authentication. In this paper we present non-stop authentication of person through more than one authentication. The user identity is constantly demonstrated via applying different authentication in session control. A comfortable records drift with private preservation for the consultation control with the aid of the usage of biometric structures will be presented. This paper described a method used to comfy raw records along with dummy bit insertion in hash code & for much less memory usage. The use of biometric allows identity to be received surely. The end result we have obtained based on actual records from this studies is fine.

Algorithm:

K nearest Neighbour

Demerits:

Time consuming Problem

3. System analysis

A. Existing System

Credit card based transactions have turn out to be a chief prone goal for criminals, hackers and perpetrators. Online use

of credit card requires only the card information to be entered and no longer gift the cardboard bodily. It is impossible to come across such fraudulent transactions amongst lots of normal transactions for credit score card agencies and merchants. Today, fraud detection technology are being carried out to monitor one-twelfth of 1 percentage of all finished transactions, which nevertheless interprets into losses of billions of bucks. Credit card fraud is one among today's fundamental threats to groups. However, its miles essential to first recognize the mechanisms for executing a fraud if you want to combat the fraud correctly. Credit card fraudsters rent a big range of approaches to devote fraud.

Disadvantage:

Tax trial non-existent, like regular coins Money laundering Susceptible of forgery.

B. Proposal System

We will focus on credit card fraud and its prevention mechanisms in this article. A credit score card fraud happens when one person uses the card of any other individual for his very own use without his proprietor's knowledge. When such form of cases takes location by fraudsters, it is used until its entire available restriction is depleted. The gadget for identifying credit score card fraud relies upon on the fraud manner itself. There are several vectors that can be used to dedicate fraud. These can, but, be divided into two major classes. First of all, the frauds due to obtaining bodily card possession illegally. A Main Concept of our task is to shop for a product with the aid of on line the use of credit card. To Buy a Product by means of online, person needs to enter the credit card info. If the person enters the incorrect info for the first time then a SMS might be dispatched to person mobile range the usage of SMS API. If person enters the wrong information for extra than 5 instances, then he will be detected as a fraud user.

Positive Predictive Value or Precision: The positive predictive value (PPV) is defined as:

$$1. \text{PPV} = \frac{TP}{(TP + FP)}$$

PPV is a measure of correct positive results among all positive predictions.

Negative Predictive Value: The negative predictive value is defined as:

$$2. \text{NPV} = \frac{TN}{(TN + FN)}$$

Advantages:

- More Efficient, eventually meaning lower prices
- Lower Transaction costs
- Anybody can use it, unlike credit cards, and does not require special authorization.

4. System requirements

A. Hardware requirements

- System : Pentium IV 2.4 GHz.
- Hard Disk : 40 GB.

- Floppy Drive : 1.44 Mb.
- Monitor : 15 VGA Colour.
- Mouse : Logitech.
- Ram : 512 Mb.

B. Software requirements

- Operating system: Windows XP.
- Coding Language: JAVA
- Data Base: MYSQL

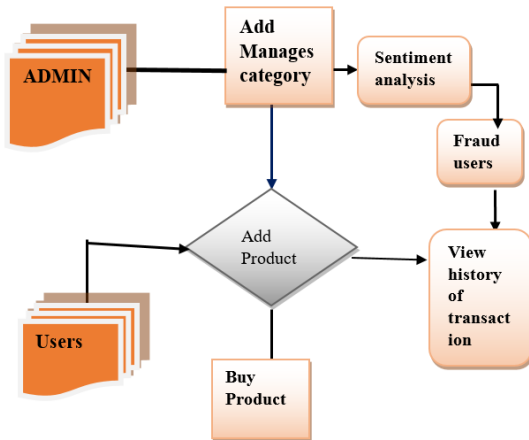


Fig. 1. Architecture diagram

5. System testing

The cause of testing is to find out errors. Testing is the manner of seeking to find out every manageable fault or weak spot in a work product. It provides a way to check the functionality of additives, sub-assemblies, assemblies and/or a finished product. It is the technique of workout software with the intent of making sure that the software device meets its necessities and user expectancies and does not fail in an unacceptable manner. There are diverse forms of check. Each take a look at kind addresses a selected checking out requirement.

A. Types of tests

1) Unit testing

Unit testing entails the design of take a look at cases that validate that the inner software logic is functioning properly, and that application inputs produce legitimate outputs. All choice branches and inner code waft have to be tested. It is the testing of character software devices of the application. It's far achieved after the completion of an individual unit before integration. This is a structural testing, that is predicated on information of its production and is invasive. Unit assessments perform basic exams at factor stage and check a specific commercial enterprise technique, software, and/or system configuration.

Unit assessments make certain that every particular direction of an enterprise process performs as it should be to the documented specs and carries virtually described inputs and predicted consequences.

2) Integration testing

Integration checks are designed to check incorporated software components to determine if they in reality run as one software. Testing is event pushed and is greater involved with the basic final results of displays or fields. Integration checks exhibit that despite the fact that the components had been personally satisfaction, as shown via efficiently unit testing, the mixture of components is correct and consistent. Integration trying out is specially aimed at exposing the issues that stand up from the mixture of components.

3) Functional test

Functional exams offer systematic demonstrations that functions tested are to be had as detailed with the aid of the business and technical necessities, device documentation, and consumer manuals. Organization and practice of practical tests is targeted on requirements, key capabilities, or special take a look at instances. In addition, systematic coverage referring to perceive Business process flows; information fields, predefined approaches, and successive approaches have to be taken into consideration for trying out. Before functional trying out is whole, extra exams are identified and the effective fee of cutting-edge checks is decided.

4) System Test

System checking out guarantees that the complete integrated software device meets necessities.

It assessments a configuration to ensure recognized and predictable consequences. An example of machine testing is the configuration oriented system integration test. System trying out is based on method descriptions and flows, emphasizing pre-driven process links and integration factors.

5) White box testing

White Box Testing is a trying out wherein in which the software tester has understanding of the inner workings, structure and language of the software, or at the least its purpose. It is used to check regions that cannot be reached from a black field level.

6) Black box testing

Black Box Testing is trying out the software without any knowledge of the internal workings, structure or language of the module being examined. Black field checks, as maximum different sorts of checks, have to be written from a definitive supply file, along with specification or requirements record, inclusive of specification or requirements document. It is a trying out wherein the software below test is dealt with, as a black field. You cannot "see" into it. The test affords inputs and responds to outputs without considering how the software works.

7) Unit testing

Unit testing is typically conducted as a part of a mixed code and unit take a look at phase of the software program lifecycle, although it is not unusual for coding and unit testing to be carried out as two wonderful stages.

a) Test strategy and approach

Field testing will be performed manually and functional tests will be written in detail.

b) Test objectives

- All discipline entries must paintings properly.
- Pages ought to be activated from the identified link.
- The access screen, messages and responses ought to no longer be delayed.

c) Features to be tested

- Verify that the entries are of the suitable layout
- No duplicate entries have to be allowed
- All links should take the user to the precise page.

8) Integration Testing

Software integration testing is the incremental integration testing of or extra included software program components on a single platform to supply failures caused by interface defects.

The challenge of the mixing take a look at is to test that components or software packages, e.g. Components in a software program system or – one step up – software packages on the employer level – interact without errors.

Test Results: All the test cases mentioned above passed successfully. No defects encountered.

9) Acceptance Testing

User Acceptance Testing is a vital section of any assignment and requires full-size participation by the stop person. It also ensures that the machine meets the useful requirements.

Test Results: All the test cases mentioned above passed successfully. No defects encountered.



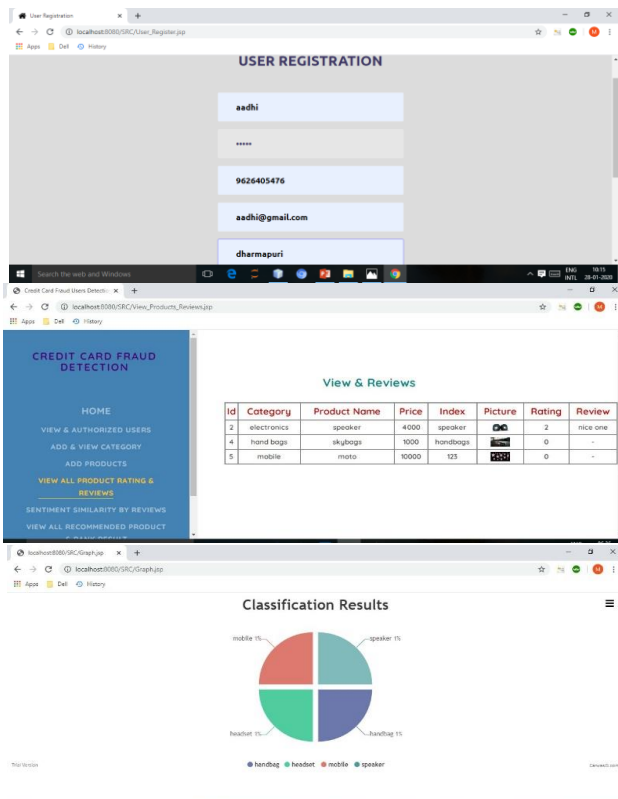
7. Conclusion




Detection of credit card fraud is an uncommon problem of class due to a very high distinction between valid and fraudulent transactions as examples. A range of commonplace algorithms had been evaluated on specific metrics in supervised, ensemble, and unsupervised categories. However, its miles important to first understand the mechanisms for executing a fraud in order to combat the fraud effectively.

References

- [1] Nitu Kumari, S. Kannan and A. Muthukumaravel, “Credit Card Fraud Detection Using Genetic-A Survey” published by Middle East Journal of Scientific Research, IDOSI Publications, 2014.
- [2] Satvik Vats, Surya Kant Dubey, Naveen Kumar Pandey, “A Tool for Effective Detection of Fraud in Credit Card System”, in International Journal of Communication Network Security, Volume 2, Issue 1, 2013.
- [3] Rinky D. Patel and Dheeraj Kumar Singh, “Credit Card Fraud Detection & Prevention of Fraud Using Genetic Algorithm”, in International Journal of Soft Computing and Engineering, Volume 2, Issue 6, January 2013.
- [4] M. Hamdi Ozcelik, Ekrem Duman, Mine Isik, Tugba Cevik, “Improving a credit card fraud detection system using genetic algorithm”, in International conference on Networking and information technology, 2010.
- [5] Wen-Fang YU, Na Wang, “Research on Credit Card Fraud Detection Model Based on Distance Sum”, in IEEE International Joint Conference on Artificial Intelligence, 2009.

6. Output



id	Category	Product Name	Price	Index	Picture	Rating	Review
3	electronics	speaker	4000	speaker		2	nice one
4	hand bags	akubags	3000	handbags		0	-
5	mobile	moto	10000	123		0	-