**Index**

|  |  |  |
| --- | --- | --- |
| **Sr.no** | **Content** | **Page no.** |
| 1. | Brief introduction | **1** |
|  | Aim of microproject | **1** |
|  | Resources required | **1** |
|  | Action plan | **2** |
| 2. | Brief description | **3** |
|  | Aim of microproject | **3** |
|  | Course outcomes | **3** |
|  | Actual procedure followed | **4** |
|  | Actual resources used | **9** |
|  | Learning outcomes | **9** |
|  | References | **9** |

**Annexure: I**

**Credit Card Fraud as an Identity Threat**

* **Brief introduction :-**

Fraud is one of the major ethical issues in the credit card industry. The main aims are, firstly, to identify the different types of credit card fraud, and, secondly, to review alternative techniques that have been used in fraud detection. The sub-aim is to present, compare and analyze recently published findings in credit card fraud detection. An E-commerce and financial service company that offered products and services that can be paid for using mobile money or a bank card (e.g., Visa and MasterCard) to make their platform a safer place for online transactions for their customers. Along with the increase in the number of customers who faced issues with their money suddenly disappearing or being transferred to another unknown account, our client thought of implementing a modern fraud prevention method for their platform.

* **Aim of project :-**

1. Any credit card fraud detection system is to identify suspicious events and report them to an analyst while letting normal transactions be automatically processed.
2. Fraud detection is a set of activities that are taken to prevent money or property from being obtained through false pretenses.

* **Resources required :-**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sr.no** | **Name of resources** | **Specification** | **Qty** | **Remark** |
|  | Computer system | Computer i3  Ram 2GB | 1 | Ok |
|  | Website | Google | 1 | Ok |
|  | Emerging Trends in Computer Technology | Book | 1 | Ok |

Page no:1

* **Action plan :-**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sr.no** | **Detail of activity** | **Planned start date** | **Planned finished date** | **Name of students** |
| 1. | Raw data | 05-04-2021  2:30 to 3:15 | 09-04-2021  12:30 to 1:15 |  |
| 2. | Design | 14-04-2021  11:00 to 11:45 | 22-04-2021  11:00 to11:45 | Awad Deepak |
| 3. | Prepare coding | 29-04-2021  11:00 to 11:45 | 05-05-2021  1:00 to 3:00 | Mohite Krushna |
| 4. | Testing of project | 13-05-2020  1:00 to 3:00 | 16-05-2021  2:30 to 3:15 | Karke Irnath |
| 5. | Display output | 20-05-2021  11:00 to 11:45 | 28-05-2021  12:30 to 11:45 | Sourabh Bhalerao |
| 6. | Prepare report | 04-06-2021  12:30 to 11:45 | 08-06-2021  11:00 to 11:45 |  |

* **Name of team member :-**

1. Awad Deepak Fulchand.
2. Karke Irnath Siddheshwar.
3. Bhalerao Sourabh Baliram.
4. Mohite Krushna Vishwanath

Page no:2

**Annexure: II**

**Credit Card Fraud as an Identity Threat**

* **Brief description :-**

Fraud is one of the major ethical issues in the credit card industry. The main aims are, firstly, to identify the different types of credit card fraud, and, secondly, to review alternative techniques that have been used in fraud detection. The sub-aim is to present, compare and analyze recently published findings in credit card fraud detection. An E-commerce and financial service company that offered products and services that can be paid for using mobile money or a bank card (e.g., Visa and MasterCard) to make their platform a safer place for online transactions for their customers. Along with the increase in the number of customers who faced issues with their money suddenly disappearing or being transferred to another unknown account, our client thought of implementing a modern fraud prevention method for their platform.

* **Aim of project :-**

1. Any credit card fraud detection system is to identify suspicious events and report them to an analyst while letting normal transactions be automatically processed.
2. Fraud detection is a set of activities that are taken to prevent money or property from being obtained through false pretenses.

* **Course outcomes :-**

1. Describe Artificial Intelligence, Machine Learning and deep learning.
2. Detect Network, Operating System and applications vulnerabilities.
3. Interpret IoT concepts.

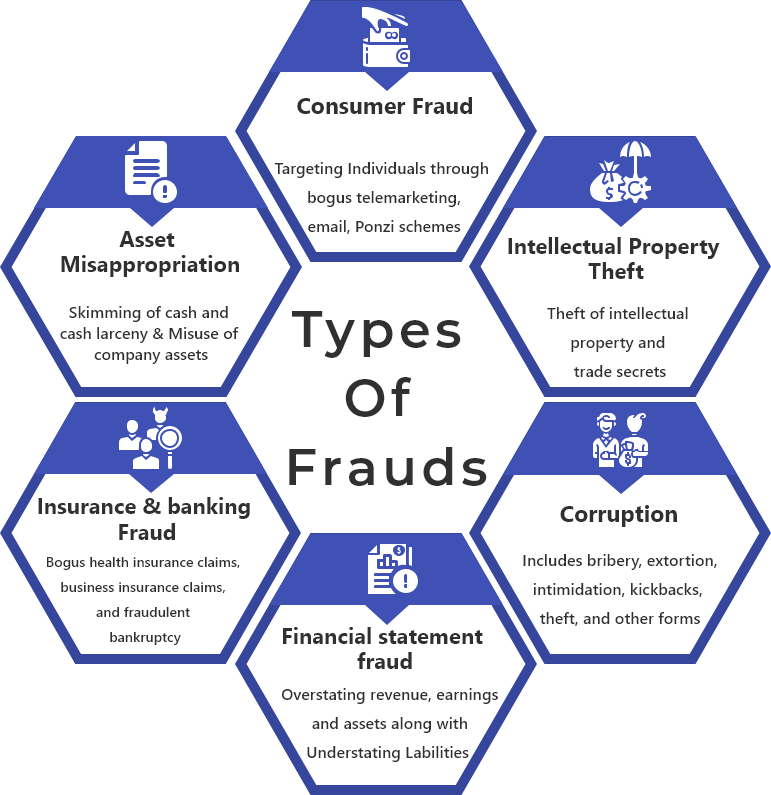
Page no:3

* **Actual procedure followed :-**

Fraud is one of the major ethical issues in the credit card industry. The main aims are, firstly, to identify the different types of credit card fraud, and, secondly, to review alternative techniques that have been used in fraud detection. The sub-aim is to present, compare and analyze recently published findings in credit card fraud detection. This article defines common terms in credit card fraud and highlights key statistics and figures in this field. Depending on the type of fraud faced by banks or credit card companies, various measures can be adopted and implemented. The proposals made in this paper are likely to have beneficial attributes in terms of cost savings and time efficiency. The significance of the application of the techniques reviewed here is in the minimization of credit card fraud. Yet there are still ethical issues when genuine credit card customers are misclassified as fraudulent.

Credit cards are one of the most famous targets of fraud but not the only one; fraud can occur with any type of credit products, such as personal loans, home loans, and retail. Furthermore, the face of fraud has changed dramatically during the last few decades as technologies have changed and developed. A critical task to help businesses, and financial institutions including banks is to take steps to prevent fraud and to deal with it efficiently and effectively.

* **Types of Frauds :-**



Page no:4

* **Bankruptcy fraud :-**

Bankruptcy [fraud](https://www.law.cornell.edu/wex/fraud) is a [white-collar crime](https://www.law.cornell.edu/wex/white-collar_crime) that commonly takes four general forms:

1. A [debtor](https://www.law.cornell.edu/wex/debtor) conceals [assets](https://www.law.cornell.edu/wex/asset) to avoid having to forfeit them.
2. An individual intentionally [files](https://www.law.cornell.edu/wex/file) false or incomplete forms. Including false information on a [bankruptcy](https://www.law.cornell.edu/wex/bankruptcy) form may also constitute [perjury](https://www.law.cornell.edu/wex/perjury).
3. An individuals [files](https://www.law.cornell.edu/wex/file) multiple times using either false information or real information in several [jurisdictions](https://www.law.cornell.edu/wex/jurisdiction).
4. An individual [bribes](https://www.law.cornell.edu/wex/bribery) a [court](https://www.law.cornell.edu/wex/court)-appointed [trustee](https://www.law.cornell.edu/wex/trustee).

Commonly, the [criminal](https://www.law.cornell.edu/wex/criminal) commits one of these forms of [fraud](https://www.law.cornell.edu/wex/fraud) with another [crime](https://www.law.cornell.edu/wex/crime), such as identity theft, [mortgage](https://www.law.cornell.edu/wex/mortgage) fraud, [money laundering](https://www.law.cornell.edu/wex/money_laundering), and [public corruption](https://www.law.cornell.edu/wex/public_corruption).

* **Application fraud :-**

Application fraud is when someone applies for a credit card with false information. To detect application fraud, the solution is to implement a fraud system that allows identifying suspicious applications. To detect application fraud, two different situations have to be distinguished: when applications come from a same individual with the same details, the so-called duplicates, and when applications come from different individuals with similar details, the so called identity fraudsters.

In most banks, to be eligible for a credit card, applicants need to complete an application form. This application form is mandatory except for social fields. The information required includes identification information, location information, contact information, confidential information and additional information. Recurrent information available would be for identification purposes, such as the full name and the date of birth. The applicant would inform the bank about his/her location details: the address, the postal code, the city and the country. The bank would also ask for contact details, such as e-mail address, land-line and mobile phone numbers. Confidential information will be the password. In addition, the gender will be given. All those characteristics may be used while searching for duplicates. To identify the so-called duplicates, cross-matching techniques are in common use. Rather than using statistical techniques, another method easy to implement is cross-matching. For instance, simple queries that give fast results are to cross-identify information with location details.

Page no:5

* **Behavioral fraud :-**

Behavioral fraud occurs when details of legitimate cards have been obtained fraudulently and sales are made on a ‘cardholder present’ basis. These sales include telephone sales and e-commerce transactions, where only the card details are required (Bolton & Hand, 2002). Behavioral fraud can be detected by implementing a fraud scorecard predicting which customers are likely to default. Traditional credit scorecards are used to detect customers who are likely to default, and the reasons for this may include fraud (Bolton & Hand, 2002). Regarding the process, using scoring for fraud prevention is similar to any other use, including profit, default, and collection. The score reflects experience of past cases, and the result is a binary outcome: a genuine customer or a fraudster.

* **Detection techniques :-**

1. **Decision tree :-**

The idea of a similarity tree using decision tree logic has been developed. A similarity tree is defined recursively: nodes are labelled with attribute names, edges are labelled with values of attributes that satisfy some condition and ‘leaves’ that contain an intensity factor which is defined as the ratio of the number of transactions that satisfy these condition(s) over the total number of legitimate transaction in the behavior. The advantage of the method that is suggested is that it is easy to implement, to understand and to display. However, a disadvantage of this system is the requirements to check each transaction one by one. Nevertheless, similarity trees have given proven results.

1. **Genetic algorithms and other algorithms**:-

Algorithms are often recommended as predictive methods as a means of detecting fraud. One algorithm that has been suggested by Bentley et al. (2000) is based on genetic programming in order to establish logic rules capable of classifying credit card transactions into suspicious and non-suspicious classes. Basically, this method follows the scoring process. In the experiment described in their study, the database was made of 4,000 transactions with 62 fields. As for the similarity tree, training and testing samples were employed. Different types of rules were tested with the different fields. The best rule is the one with the highest predictability. Their method has proven results for real home insurance data and could be one efficient method against credit card fraud. Chan et al. (1999) also developed an algorithm to predict suspect behavior. The originality of their research is that the model is evaluated and rated by a cost model, whereas other studies use evaluation based on their prediction rate/the true positive rate and the error rate/the false negative rate. Wheeler & Banks and Bank Systems, Volume 4, Issue 2 2009 64 Aitken (2000) developed the idea of combining algorithms to maximize the power of prediction. In their article, they present different algorithms: diagnostic algorithms, diagnostic resolution strategies, probabilistic curve algorithms, best match algorithms, negative selection algorithms, and density selection algorithms. They conclude from their investigation that neighborhood-based and probabilistic algorithms have been shown to be appropriate techniques for classification, and may be further enhanced using additional diagnostic algorithms for decision-making in borderlines cases, and for calculating confidence and relative risk measures.

Page no:6

1. **Clustering techniques :-**

Bolton & Hand (2002) suggest two clustering techniques for behavioral fraud. The peer group analysis is a system that allows identifying accounts that are behaving differently from others at one moment in time whereas they were behaving the same previously. Those accounts are then flagged as suspicious. Fraud analysts have then to investigate those cases. The hypothesis of the peer group analysis is that if accounts behave the same for a certain period of time and then one account is behaving significantly differently, this account has to be notified. Breakpoint analysis uses a different approach. The hypothesis is that if a change of card usage is notified on an individual basis, the account has to be investigated. In other words, based on the transactions of a single card, the break-point analysis can identify suspicious behavior. Signals of suspicious behavior are a sudden transaction for a high amount, and a high frequency of usage.

1. **Neural networks :-**

Neural networks are also often recommended for fraud detection. Dorronsoro et al. (1997) developed a technically accessible online fraud detection system, based on a neural classifier. Bayesian networks are also one technique to detect fraud, and have been applied to detect fraud in the telecommunications industry (Ezawa & Norton, 1996) and also in the credit card industry (Maes et al., 2002). Results from this technique are optimistic. However, the time constraint is one main disadvantage of such a technique, especially compared with neural networks (Maes et al., 2002). Furthermore, expert systems have also been used in credit card fraud using a rule-based expert system (Leonard, 1995).

For new issuing banks, a proposal would be to rely on credit bureaux score in order to control fraud and avoid expected losses. Even though those scorecards are primarily used to predict defaulting customers, one could use them to detect fraud, since fraud and default are strongly correlated. Generic scoring systems are typically based on a sample from the past experiences of several lenders. Generic systems are sold to creditors who believe they will find them useful.

* **Conclusion :-**

Clearly, credit card fraud is an act of criminal dishonesty. This article has reviewed recent findings in the credit card field. This paper has identified the different types of fraud, such as bankruptcy fraud, counterfeit fraud, theft fraud, application fraud and behavioral fraud, and discussed measures to detect them. Such measures have included pair-wise matching, decision trees, clustering techniques, neural networks, and genetic algorithms.

Page no:7

* **Resources required :-**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sr.no** | **Name of resources** | **Specification** | **Qty** | **Remark** |
|  | Computer system | Computer i3  Ram 2GB | 1 | Ok |
|  | Website | Google | 1 | Ok |
|  | Emerging Trends in Computer Technology | Book | 1 | Ok |

* **Learning Outcomes:-**
  1. I will learn the concept of emerging trends in information technology.
  2. I will study about the concept of machine, artificial learning.
  3. I will study the concept credit card frauds techniques.

1. I will study the concept of Interpret IoT concepts.

* **References:-**

1. [www.google.com](http://www.google.com)
2. [www.TutorialsPoint.com](http://www.TutorialsPoint.com)
3. [www.frauds](http://www.frauds).com

Page no:8