# E authentication system for E-card generation

Pratima Yadav[1], Anamika Yadav[2], Nikita Jaiswal[3], Km Sweta Sharma[4]

[1] *Student, Computer Science & Engineering, Institute of Technology & Management, Gorakhpur, India*
[2] *Student, Computer Science & Engineering, Institute of Technology & Management, Gorakhpur, India*
[3] *Student, Computer Science & Engineering, Institute of Technology & Management, Gorakhpur, India*
[4] *Student, Computer Science & Engineering, Institute of Technology & Management, Gorakhpur, India*

## ABSTRACT

*Because of the increasing volume of daily electronic transactions, credit cards are the most widely used electronic payment method, making them more vulnerable to fraud. Card fraud has cost credit card companies a lot of money. Credit card fraud detection is currently the most common issue. Credit card companies are looking for the right technologies and systems to detect and reduce credit card fraud. There are several methods for detecting credit card fraud that have been reviewed and highlighted in this paper, as well as their advantages and disadvantages.*

**Keyword: -** *Supervised Machine Learning Techniques, Support Vector Machine, and Naive Bayes.*

## 1. INTRODUCTION

Today, due to the rapid growth of e-commerce, online shopping or online transactions are increasing by the day. Credit cards are accepted as payment. Credit card users are increasing on a daily basis. According to reports, nearly 430 million credit and debit card users exist throughout Europe. As the number of credit/debit card users grows, so does the number of fraudulent users. Credit cards are classified into two types. 1. Physical identification card 2. A virtual credit card. When using a physical card, the user must present the card when making a payment. In this case, a fraudulent user only needs to steal the card in order to gain access to it. The fraudulent user of a virtual card must be aware of the details information. CVV number, Secure code, and credit card number are examples of credit card information. As a result, a secure payment gateway is required to identify the user and confirm whether the user is legal or an attacker. Behavior and Location Analysis is the most effective and appropriate technique for detecting fraud (BLA). For a long time, online transaction fraudsters and detectors have played a complex role. Transaction fraud is more prevalent than ever before, particularly in the Internet age, and it causes significant financial losses. The Nilsson study examined the global scenario surrounding online transaction fraud in depth. Online transaction fraud cost the economy about $21 billion in 2015, $24 billion in 2016, and more than $27 billion in 2017. Year in and year out, The global rate of online transaction fraud is expected to rise to $31.67 billion by 2020. As a result, banks and financial institutions may be required to create an automated online fraud detection system to detect and monitor online transactions. Fraud detection systems are designed to detect and track incoming transactions by separating anomalous activity patterns from large amounts of transactional data. Machine learning has been shown to be extremely effective at detecting these patterns. Alternatively, a large number of transaction records could be used to train a high-performance fraud classifier. Despite the fact that supervised learning has been shown to be extremely effective in detecting fraudulent transactions, transactional fraud analysis technology will continue to advance. Small changes can also save a company a lot of money. There are some flaws in the novel technique of unsupervised and controlled online fraud detection.

## 2. LITERATURE REVIEW

Prajal Save et al. [1] proposed a model based on a decision tree and a hybrid of the Luhn and Hunt algorithms. The Luhn algorithm is used to determine whether or not an incoming transaction is fraudulent. It validates credit card numbers using the credit card number as input. Address Mismatch and Degree of Out lierness are used to assess each incoming transaction's deviation from the cardholder's normal profile. Finally, the general belief is strengthened or weakened using Bayes Theorem, and the calculated probability is recombinated with the initial belief of fraud using an advanced combination heuristic. Vimala Devi Three machine-learning algorithms were presented and implemented by J et al.

[2] to detect counterfeit transactions. Many metrics are used to assess the performance of classifiers or predictors, including the Vector Machine, Random Forest, and Decision Tree. These metrics can be classified as either prevalence-dependent or prevalence-independent. Furthermore, these techniques are used in mechanisms for detecting credit card fraud, and the results of these algorithms have been compared. Pop at and Chaudhary

[3] presented supervised algorithms. Deep learning, Logistic Regression, Nave Bayesian, Support Vector Machine (SVM), Neural Network, Artificial Immune System, K Nearest Neighbor, Data Mining, Decision Tree, Fuzzy logic-based System, and Genetic Algorithm are just a few of the techniques employed. Credit card fraud detection algorithms identify transactions. That are likely to be fraudulent Machine learning algorithm were compared to prediction, clustering, and outlier detection Shiyang Xuan and colleagues.

[4] The Random Forest classifier was used to train the behavioral characteristics of credit card transactions. Random forest based on random trees and random forest-based on CART are used to train the normal and fraudulent behavior features. Performance measures are computed to assess the model's effectiveness. Geetha S. and Dornadula

[5] The transactions were aggregated into respective groups using the Sliding-Window method, i.e. Some window features were extracted to discover cardholder behavioral patterns. There are options for displaying the maximum amount, the minimum amount of a transaction, the average amount in the window, and even the time elapsed. Sangeeta Mittal and colleagues.

[6] Some popular machine learning algorithms in the supervised and unsupervised categories were chosen to evaluate the underlying problems. From classical to modern supervised learning algorithms have been considered. Tree-based algorithms, classical and deep neural networks, hybrid algorithms, and Bayesian approaches are among them. The ability of machine learning algorithms to detect credit card fraud has been evaluated. A number of popular algorithms in the supervised, ensemble, and unsupervised categories were evaluated using various metrics. It is concluded that unsupervised algorithms handle dataset skewness better and thus perform well across all metrics in absolute and comparative terms. Akela and Deepa

[7] Anomaly Detection Algorithm, K-Nearest Neighbor, Random Forest, K-Means, and Decision Tree were among the algorithms used to detect fraud. Presented several techniques and predicted the best algorithm to detect deceptive transactions based on a given scenario. The system used various rules and algorithms to generate the Fraud score for that specific transaction in order to predict the fraud result. Xiao Han Yu et al.

[8] proposed a deep network algorithm for detecting fraud. The paper describes a deep neural network algorithm for detecting credit card fraud. The neural network algorithm approach as well as deep neural network applications have been described.

[9] We intend to change the unique circumstance and exchange of business cards. In our versatile application we need to can supplant a neglected card by "embracing" the telephones. Doing this will move one business card starting with one telephone then onto the next. While this is definitely not an essential capability, it can serve

various requirements in light of the clients' unique situation. In spite of this article is more about Administrations, for example, web, voice and SMS applications in the third world, and how the portable web can make use of a scaffold over what the writer portrays as the computerized split between the third world and the non-industrial nations. Individuals would utilize administrations assuming i.e. designed on their telephone of course and the UI is simple and compare to their assumption. By utilizing this rationale, we want our application to be instinctive, simple to learn and simple to use, while as yet being sufficient to address the clients' all's issues and assumptions. As this is an application that would require a client to make their own profile's, it can't be conveyed designed, yet we ought to endeavor to do It as easy as imaginable to build it, so it tends to be immediately taken into utilization.

## 3. MODELING AND ANALYSIS

### 3.1 PROBLEM DEFINITION

Our present ID card system lacks innovation. Its value can be increased significantly. Present use of ID cards is only for identification purpose. which is very less compared to the potential it contains. Although our College ID card is used in libraries for borrowing, renewing and returning books, but we need to increase this functionality as much as possible. It is also observed that many shopkeepers and students face problems of change unavailability, this idea solves this problem efficiently. It also solves insecurities associated with carrying of cash which may not be found once lost. Installing such a system leads to complications but this idea can be easily implemented with existing college ID and minimal efforts.

### 3.2 PROJECT DISCRIPTION INTRO

A little intro in top will display the features that our website is providing

**Quick Templates access**

The Best templates of our websites will be displayed

**Tips**

All the tips related to making Id card will be displayed.

### Category

In our Category Page there Are many options like vertical & horizontal and in vertical

### Contact Us

This will ask how they can help users to fix any problems they are facing

### 3.3 Proposed architecture

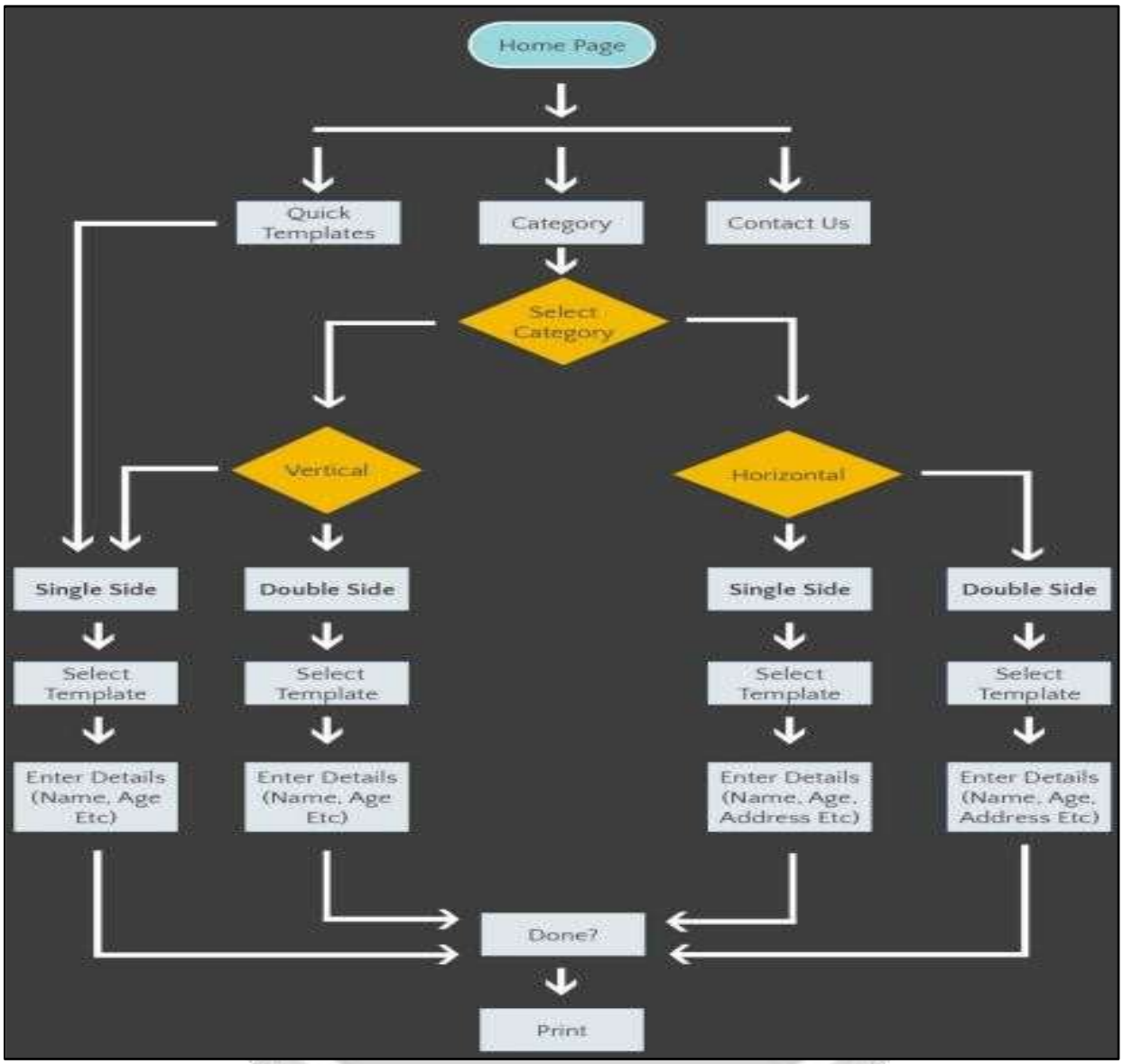


**Figure 1:** The proposed flow of the project

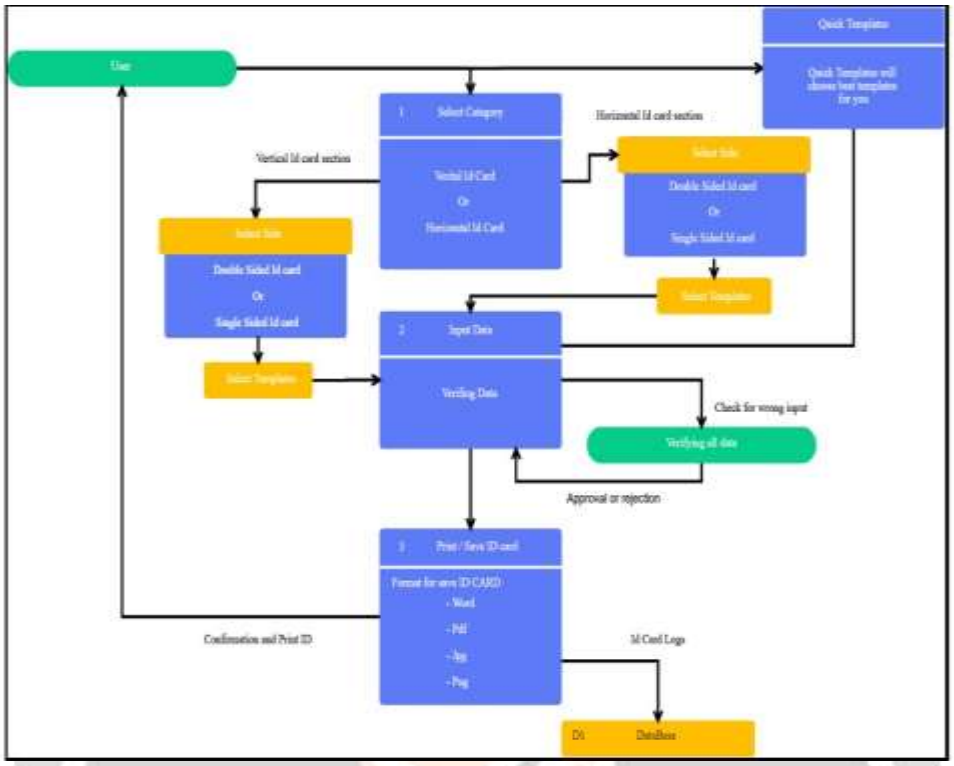


**Figure 2***:* Data Flow Diagram

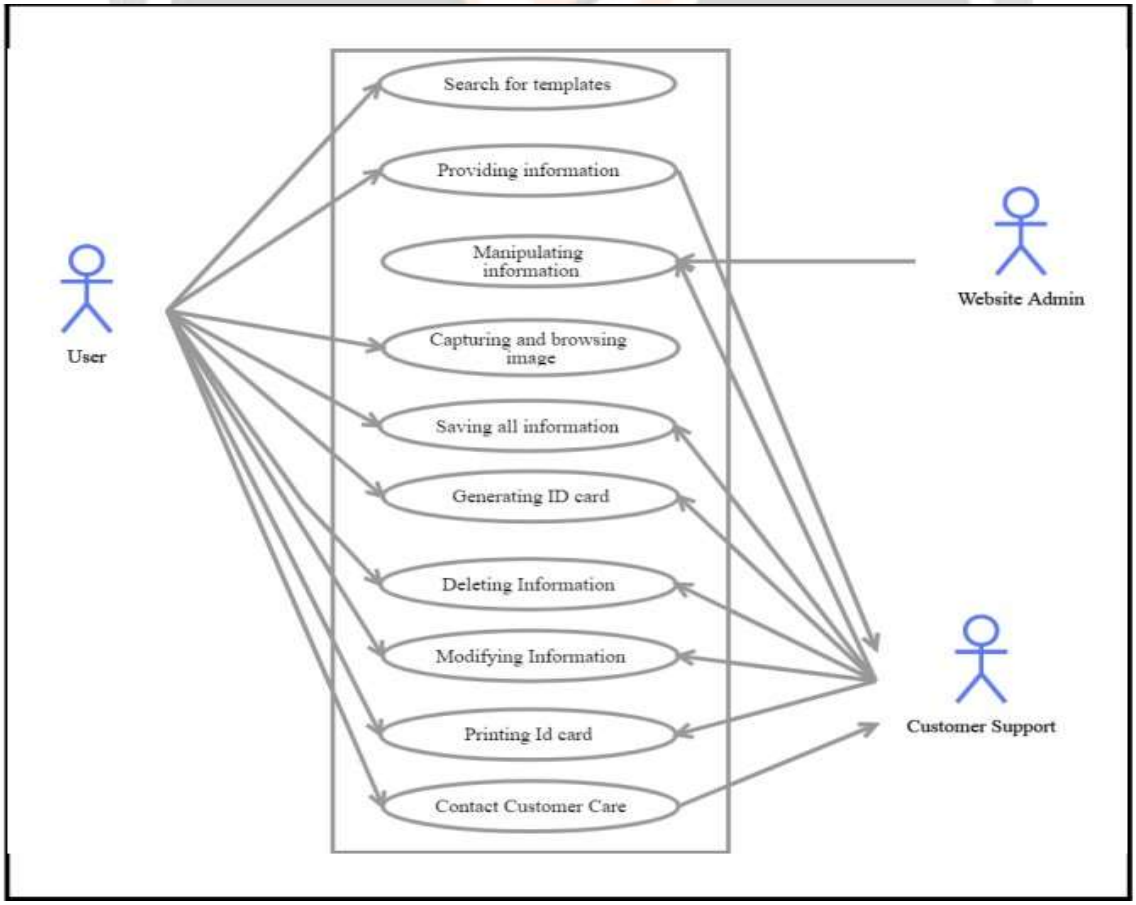

**Figure 3:** Use Case Diagram

**Requirements**

Here we are including the software and hardware used for developing the project and implementing the project

**A. Software requirements**:
-HTML, CSS, JavaScript

-MS Word 97 or later

-Web Browser: Microsoft Internet Explorer, Mozilla, Google Chrome or later

**B. Hardware Requirements:**
-System: Intel I3 Processor

-Hard Disk: 500 GB

-Monitor: Standard LED Monitor

-Input: Keyboard

-Ram: 4GB

## 4. CONCLUSIONS

Credit card fraud has become a major global concern. Fraud causes enormous financial losses around the world. This prompted credit card companies to invest money in developing techniques to detect and reduce fraud. The primary goal of this research is to develop algorithms that can be used by credit card companies to identify fraudulent transactions more accurately, in less time and at a lower cost. Logistic Regression, Decision Trees, Random Forest, Artificial Neural Networks, Logistic Regression, K-Nearest Neighbors, and K-means clustering are among the machine learning algorithms compared. Because no two scenarios are alike, a scenario-based algorithm can be used to determine which scenario is best suited to that scenario. Each of the fraud detection techniques discussed in this survey article has benefits and drawbacks. The researchers employ various performance measures (techniques) and algorithms to predict and identify fraudulent transactions. Studies are refreshed and encouraged to improve the fraud detection basis in order to determine the appropriate weight for cost factors, tested accuracy, and detection accuracy. Such surveys will enable the researchers to develop the most accurate hybrid approach for detecting fraudulent credit card transactions.

## 5. REFERENCES

[1] "JMU Scholarly Commons Detecting Credit Card Fraud: An Analysis of Fraud Detection Techniques," S. H. Projects and W. Lovo,2020. Int. J. Data Min. Tech. Appl., vol. 7, no. 1, pp. 21–24, 2018, doi:10.20894/ijdmta.102.007.001.004; S. G. and J. R. R., "A Study on Credit Card Fraud Detection Using Data Mining Techniques."

[2]. Investopedia's "Credit Card Definition," available at https://www.investopedia.com/terms/c/creditcard.asp (retrieved April 3, 2021).

Credit card fraud: awareness and prevention, Journal of Financial Crime, vol. 15, no. 4, pp. 398–410, 2008, doi:10.1108/13590790810907236.

[3]. *K. J. Barker, J. D'Amato, and* P. Sheridon

.

[4]. S. Geetha and V. N. Dornadula, "Credit Card Fraud Detection using Machine Learning Algorithms," Procedia Computer Science, vol.165, no. 6, 2019, p. 631-641, doi: 10.1016/j.procs.2020.01.057

[5] A. Alhazmi, H., and N. A Survey of Credit Card Fraud Detection Using Machine Learning, Aljehane, 2020 International. Conf. Compute. Inf. Technol. 10-15, 2020; 10.1109/ICCIT-144147971.2020.9213809; ICCIT 2020.Fraud detection based on data mining, arXiv, 2020

[6] A. Agarwal, "Survey of Different Techniques Used for Credit Card Fraud Detection," International J. J. Res. Appl. Sci. Eng. Technology, volume 2020, volume 8, number 7, pages 1642–1646, doi:10.22214/ijraset.2020.30614.
[7] C. A Comparative Study of Credit Card Fraud, vol. 7, no. 19, pp. 998–1011, 2020.
[8] R. Sailusha, G., V., Gnaneswar, and R. Credit Card Fraud Detection Using
[9] B. Ramakoteswara Rao Wickramanayake, Y. Ouyang, C. Ouyang, and D. K. Geeganage. A survey of machine learning for online card payments, Xu, Proc. Int. Conf. Intel Comput.Regulatory Syst. 2020, ICICCS, no. I. I. C. C. S., 2020, pp. 1264–1270, doi: 10.1109/ICICCS48265.2020.9121114. N. Sael, Sadgali, and F. In Benbow's article "Detection and prevention of credit card fraud: State of the Art," published in MCCSIS 2018 - Multi Conf. Compute. Sci. Inf. Syst. Proc. Int. Conf. Using Big Data. Data Minimum Compute. intel. Year 2018 Theory Practice Mod. compute. Connect in 2018. Sama, no. March 2019, pages 129–136

[10] R. A. Goyal and Review on Credit Card Fraud Detection Using Data Mining Classification Techniques & Machine Learning Algorithms, International Journal of Research and Applications, vol. 7, no. 1, 2020, [Online], pp. 972–975. http://www.ijrar.org/papers/IJRAR19K7539.pdf is accessible.