IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2320-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 9, Issue 9, September 2020

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.512

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 9, September 2020||

Credit Card Fraud Detection Using Collaborative Filtering Datamining Techniques

Nikhil Handa[1], Nidhi Agrawal[2], Vaibhav Katkar [3], Gaurav Rathod [4], Prasad Ikhar [5], Komal Hole[6]

B.E. Student, Department of Computer Science and Engineering, Prof. Ram Meghe Institute of Technology and Research, Badnera, Maharashtra, India[1]

B.E. Student, Department of Computer Science and Engineering, Prof. Ram Meghe Institute of Technology and Research, Badnera, Maharashtra, India[2]

B.E. Student, Department of Computer Science and Engineering, Prof. Ram Meghe Institute of Technology and Research, Badnera, Maharashtra, India[3]

B.E. Student, Department of Computer Science and Engineering, Prof. Ram Meghe Institute of Technology and Research, Badnera, Maharashtra, India[4]

B.E. Student, Department of Computer Science and Engineering, Prof. Ram Meghe Institute of Technology and Research, Badnera, Maharashtra, India[5]

Assistant Professor, Department of Computer Science and Engineering, Prof. Ram Meghe Institute of Technology and Research, Badnera, Maharashtra, India[6]

ABSTRACT: Due to the rise and rapid growth of E-Commerce, use of credit cards for online purchases has dramatically increased and it caused an explosion in the credit card fraud. As credit card becomes the most popular mode of payment for both online as well as regular purchase, cases of fraud associated with it are also rising. In real life, fraudulent transactions are scattered with genuine transactions and simple pattern matching techniques are not often sufficient to detect those frauds accurately. Implementation of efficient fraud detection systems has thus become imperative for all credit card issuing banks to minimize their losses. Data mining is becoming increasingly common in both the private as well as public sectors. The Credit Card Fraud Detection Problem includes modelling past credit card transactions learning the behaviour of user to find out the fraud. Data mining involves the use of data analysis tools to find out formerly unknown, believable patterns and relationships in large data sets. This is then used to recognize whether a new transaction is fraudulent or not. Our objective here is to detect 100% of the fraudulent transactions while minimizing the incorrect fraud classifications. In this process, we have focused on analysing and pre-processing the data sets. Here we are using AES algorithm for the encryption of data and Luhn algorithm for detecting the card type in order to simplify the data mining process. In this process our main motive is to track the fraudster and prevent the use of the theft credit cards from the further use by blocking the fraudster on an E-commerce website. By using the above techniques, we can minimize a hefty number of credit card frauds on an e-commerce website with the feasibility of finding the current location of the fraudster

KEYWORDS: fraudulent transactions,AES algorithm, Luhn algorithm.

I. INTRODUCTION

In these modern times the mode of payment types are changed into the online transactions. There are many types of payment options for online transaction but due to rise and rapid growth in E-Commerce, use of Credit cards for online transactions has drastically increased. As Credit card is easy and substituted for cash and also one of the convenient methods of payment it has become the most popular mode of payment for both online as well as for regular purchase and this has caused an explosion in the Credit card fraud [2].

Credit card fraud is nothing but usage or removal of other person's funds without any authentication. In real life, fraudulent transactions are scattered with genuine transactions and simple pattern matching techniques are not often sufficient to detect those fraud accurately. Implementation of efficient fraud detection system has thus become imperative for all credit card issuing banks to minimize there losses. Detecting unauthorized credit card transactions is an extremely complex problems features are seldom useful if taken individually.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 9, September 2020||

Data mining is becoming increasingly common in both the private as well as the public sectors. The Credit Card Fraud Detection Problem includes modelling past credit card transactions learning the behaviour of user to find out the fraud.When these different features have to be combined in non-trival ways,the customary solution is to resort to a data mining,a subfield of computer science dealing with the automatic discovery of patterns in data set. Data mining involves the use of data analysis tools to find out formerly unknown, believable patterns and relationships in large data sets. While data mining is able to detect hidden patterns in data it lacks the capacity of synthesizing metrics describing the global structure created by the interactions between the different features. To detect 100% of the fraudulent transactions while minimizing the incorrect fraud classifications.tn this process one have to focuses on analysing and pre-processing the data sets [3]. In order to simplify the process of data mining, the two algorithms have been used and they are AES algorithm and Luhn algorithm.

Advanced Encryption Standard (AES) algorithm is one of the most common and widely used algorithm worldwide.AES algorithm is used for the encryption of the data,it has its own particular structure to encrypt and decrypt sensitive data and is applied in hardware and software worldwide. It is very difficult for hackers to get the real data when encrypting by AES algorithm till date there is no evidence to crake this algorithm.

Luhn Algorithm is a simple checksum formula used to validate a variety of identification numbers such as credit cards,national providers etc.Luhn algorithm is used for detecting the card type in order to simplify the data mining process.[5]

The main motive is to track the blocking the fraudster on an E-commerce website. By using these techniques one can minimize a hefty number of credit card frauds on an e-commerce website with the feasibility of finding the current location of the fraudster.

II. METHODOLOGY

DATA FLOW DIAGRAM:-

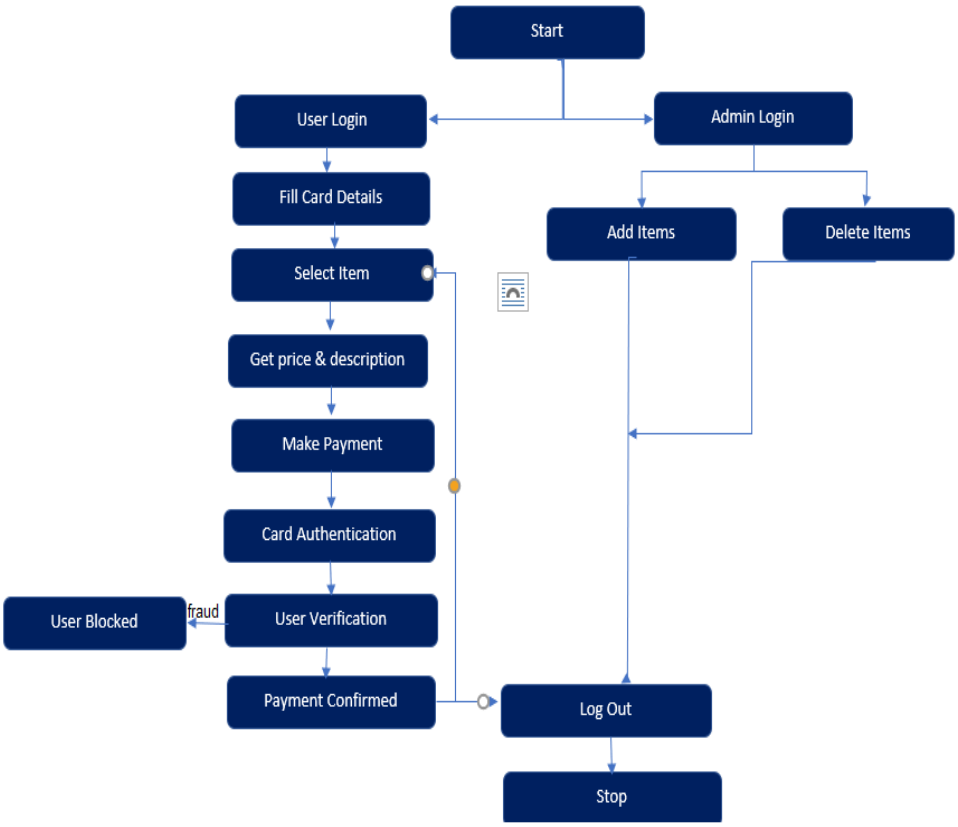

FIG.1 DATA FLOW DIAGRAM FOR CREDIT CARD FRAUD DETECTION.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 9, September 2020||

Description: A data flow diagram is a type of diagram that represents an algorithm, workflow or process, showing the steps as boxes of various kinds, and their order by connecting them with arrows. There are two sections that is user and admin. The user section is for customers or buyers who may visit the e-commerce website, and buy the stuff they need.[5] The admin section includes Upload new items to the e-commerce website or delete item from the website, logout.

AES Algorithm: -
The National Institute of Standards and Technology has started development of AES in 1997 for the need of successor algorithm for the Data Encryption Standard (DES).[6]
How AES encryption works
AES comprises three block ciphers they are AES-128, AES-192 and AES-256. AES-128 uses a 128-bit key length to encrypt/decrypt a block of messages, AES-192 uses a 192-bit key length and AES-256 a 256-bit key length to encrypt/decrypt messages. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128, 192 and 256-bits, respectively.[7]

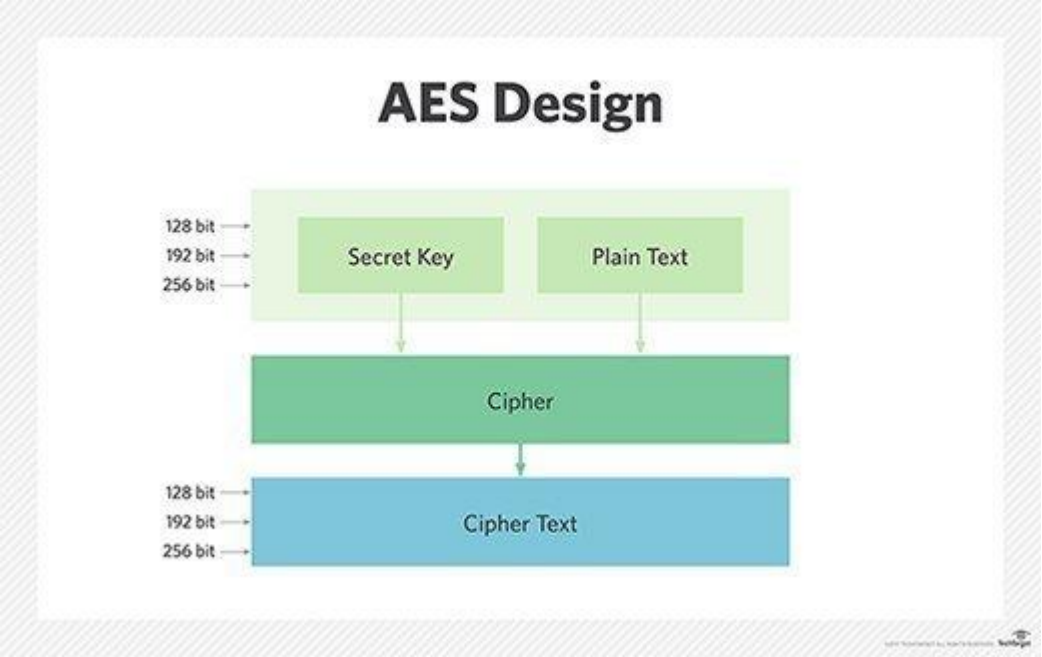

FIG.2 DESCRIBING THE RELATIONSHIPS BETWEEN SECRET KEY, PLAINTEXT, CIPHER, AND CIPHERTEXT.

The AES encryption algorithm defines a number of transformations that are to be performed on data stored in an array. The first step of the cipher is to put the data into an array; after which, the cipher transformations are repeated over a number of encryption rounds. The number of rounds is determined by the key length, with 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys.[8]
The first transformation in the AES encryption cipher is substitution of data using a substitution table; the second transformation shifts data rows, the third mixes columns. The last transformation is a simple exclusive or operation performed on each column using a different part of the encryption key. Longer keys need more rounds to complete.

Luhn Algorithm: -
The LUHN algorithm is used to generate and/or validate and verify the accuracy of credit-card numbers. The LUHN formula was created in the late 1960s by a group of mathematicians. Shortly thereafter, credit card companies adopted it. Because the algorithm is in the public domain, it can be used by anyone.[9]
Most credit cards contain a check digit, which is the digit at the end of the credit card number. The first part of the credit-card number identifies the type of credit card (Visa, MasterCard, American Express, etc.), and the middle digits identify the bank and customer[10].To generate the check digit, the LUHN formula is applied to the number. To validate the credit-card number, the check digit is figured into the formula.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 9, September 2020||

WORKING:-

Step 1: -Starting with the last digit of the credit card number and moving left and then double the value of all the alternating digits.

Step 2: -Starting from the left then after that take all the unaffected digits and add them to the results of all the individual digits from step 1. If the results from any of the numbers from step 1 are double digits, make sure to add the two numbers first (i.e. 18 would yield 1+8). Basically, your equation will look like a regular addition problem that adds every single digit.

Step 3: -The total from step 2 must end in zero for the credit-card number to be valid.

III. IMPLEMENTATION &EXPERIMENTAL RESULTS

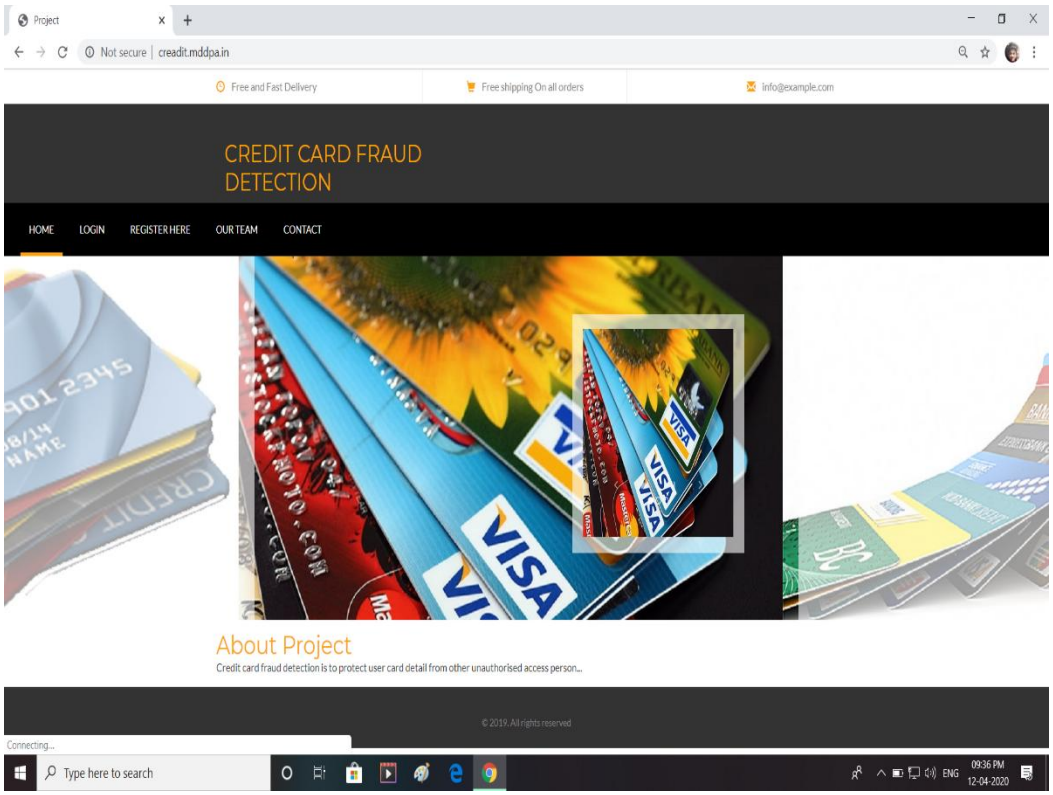

FIG 4.1: - MAIN PAGE OF THE WEBSITE.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 9, September 2020||

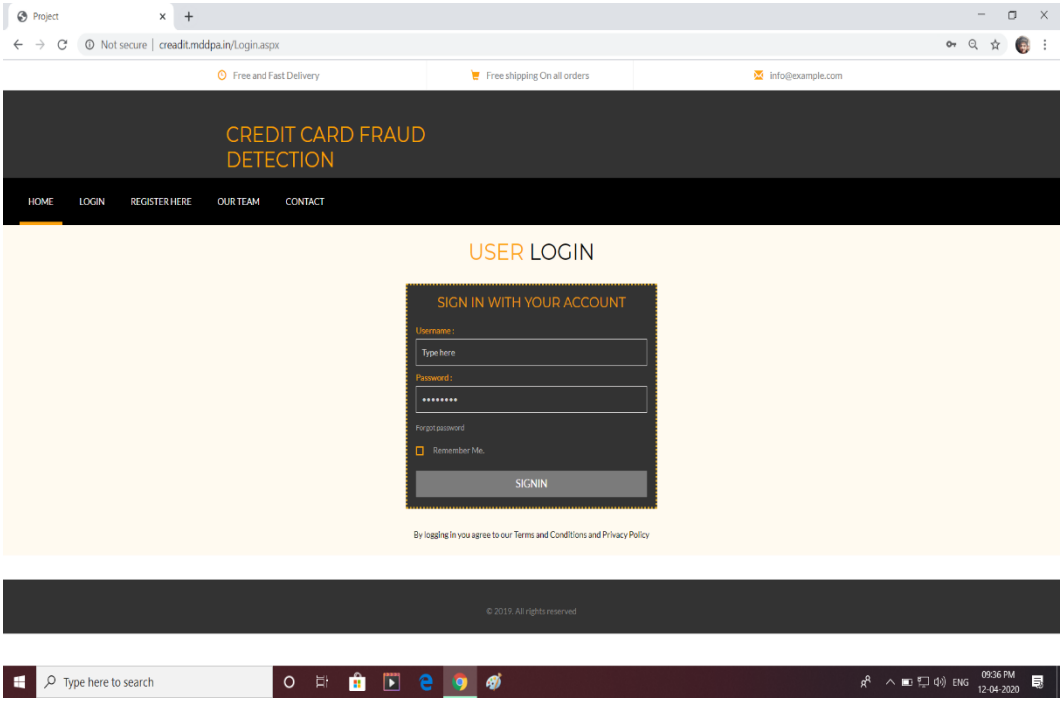

FIG 4.2: - LOGIN PAGE

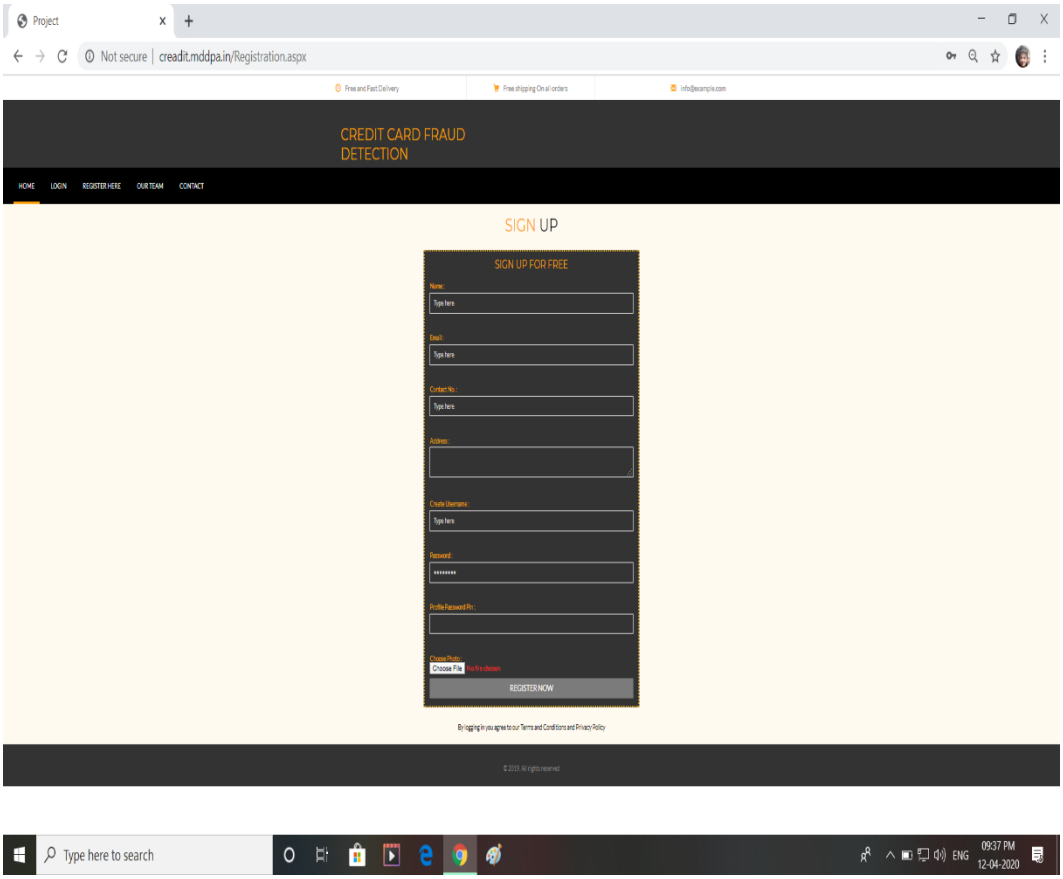

FIG 4.3: - REGISTRATION PAGE.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 9, September 2020||

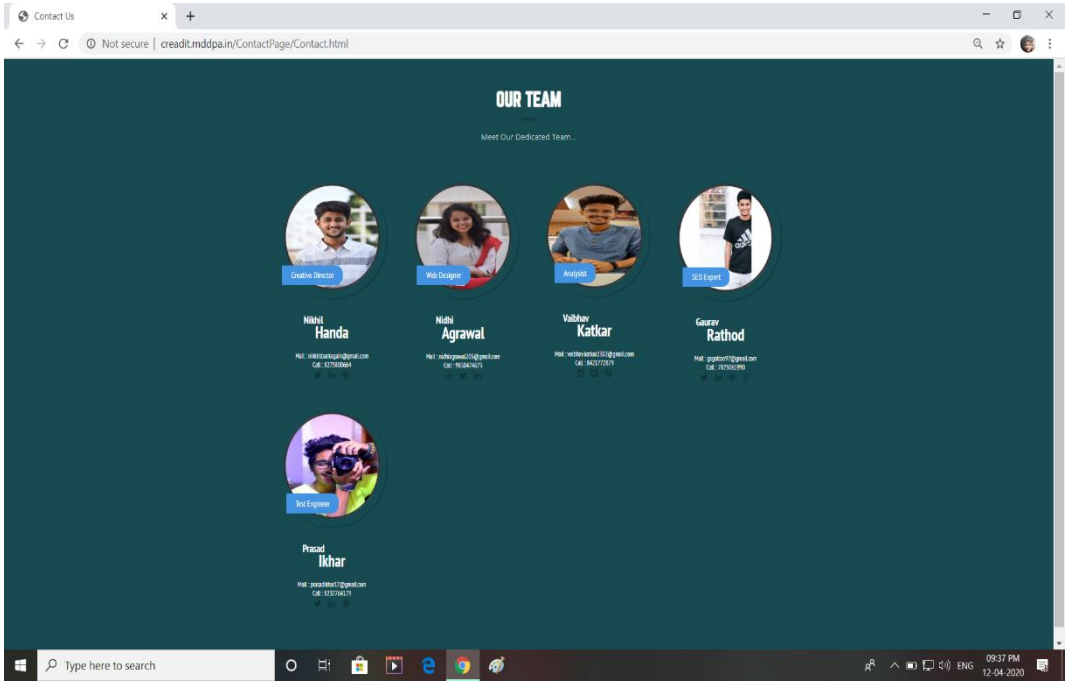

FIG 4.4: - ADMIN CONTACTS

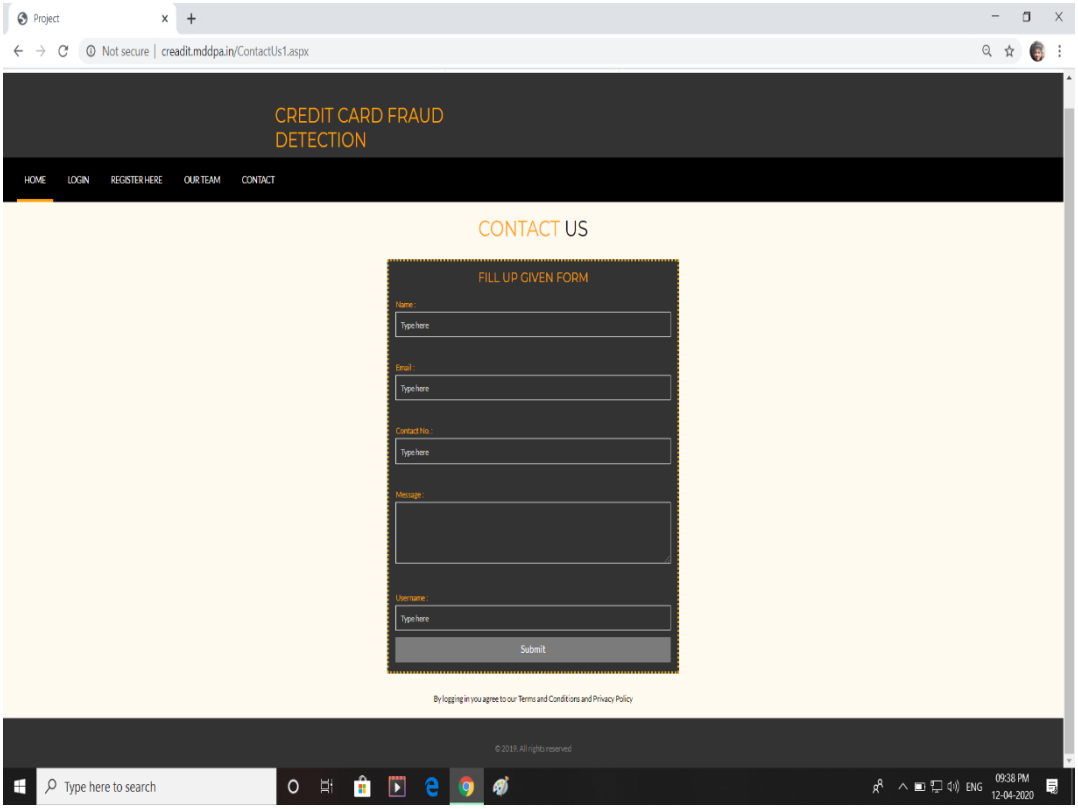

FIG 4.5: - CONTACT US FORM.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 9, September 2020||

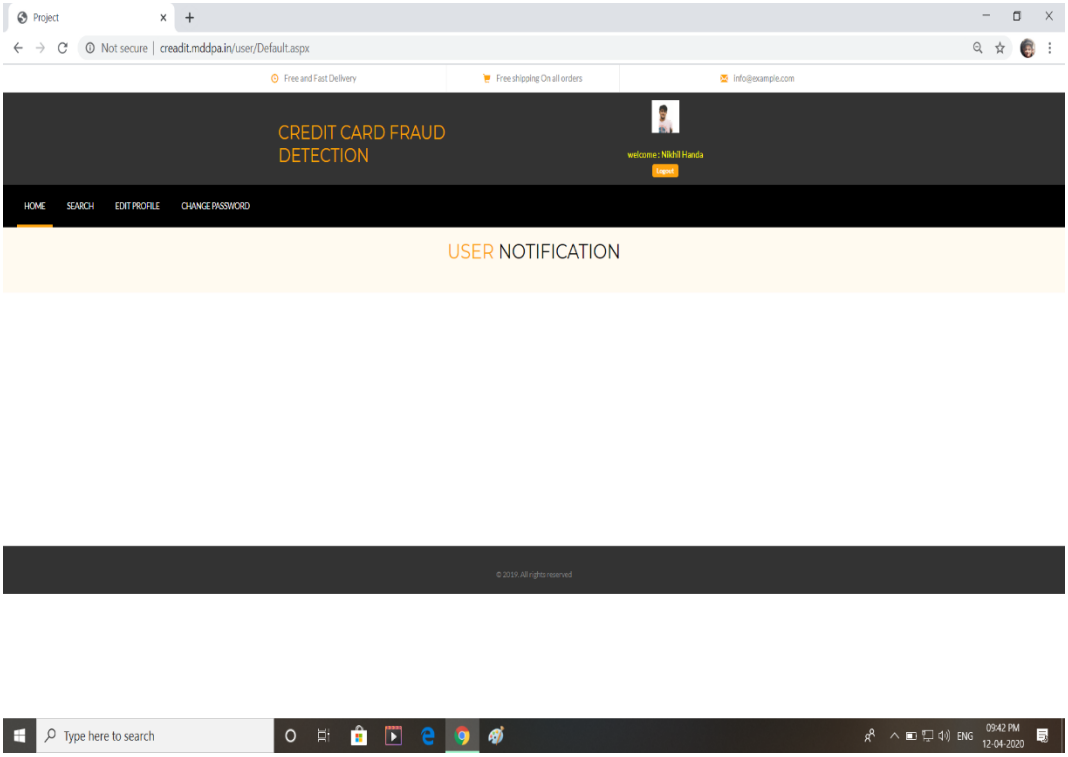

FIG 4.6: - AFTER LOGIN HOME PAGE.

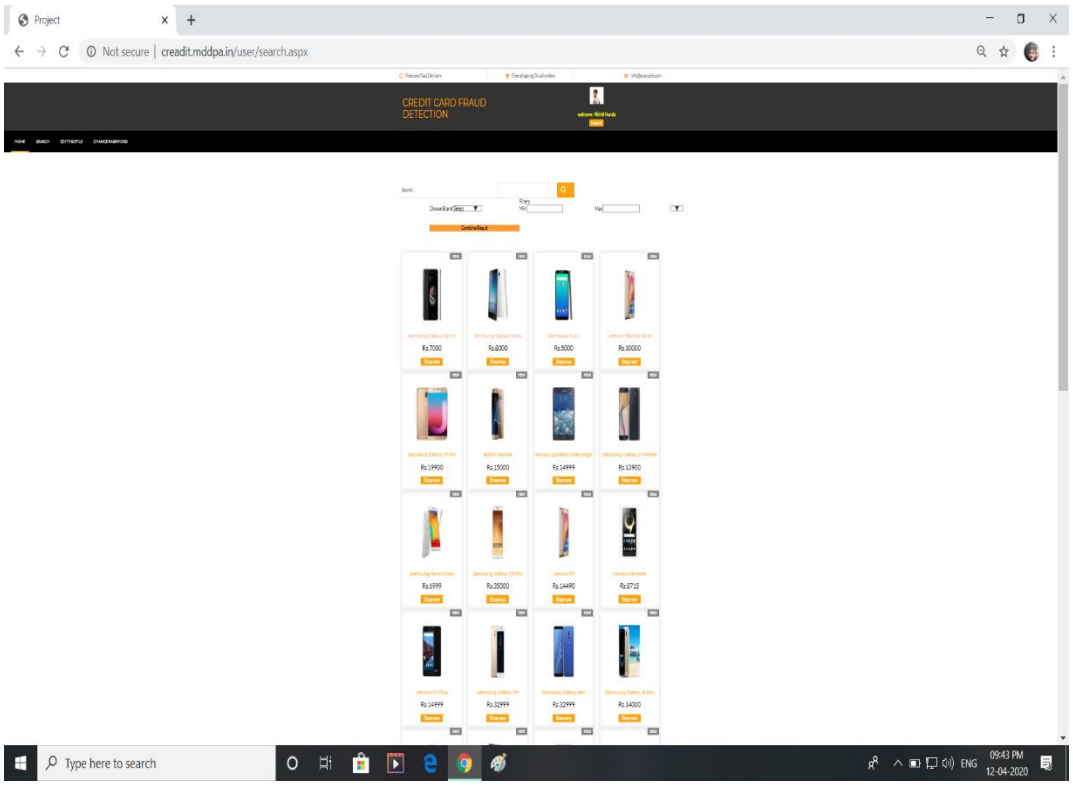

FIG 4.7: - SEARCH PRODUCTS.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 9, September 2020||

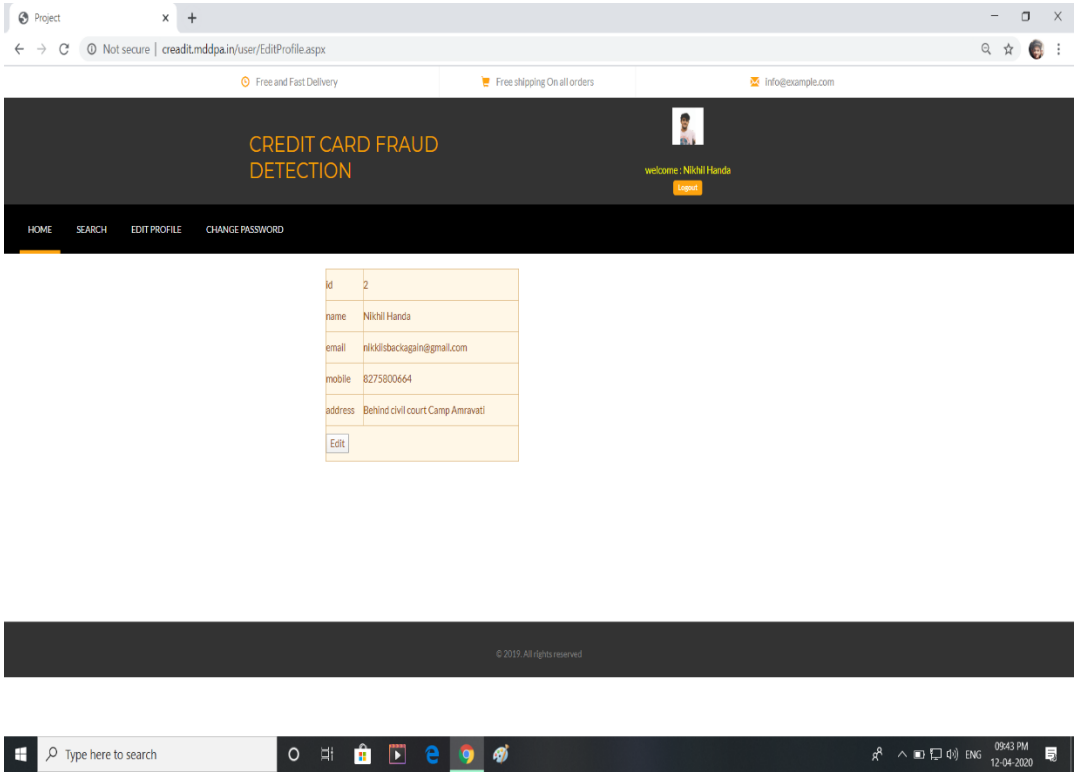

FIG 4.8: - EDIT PROFILE.

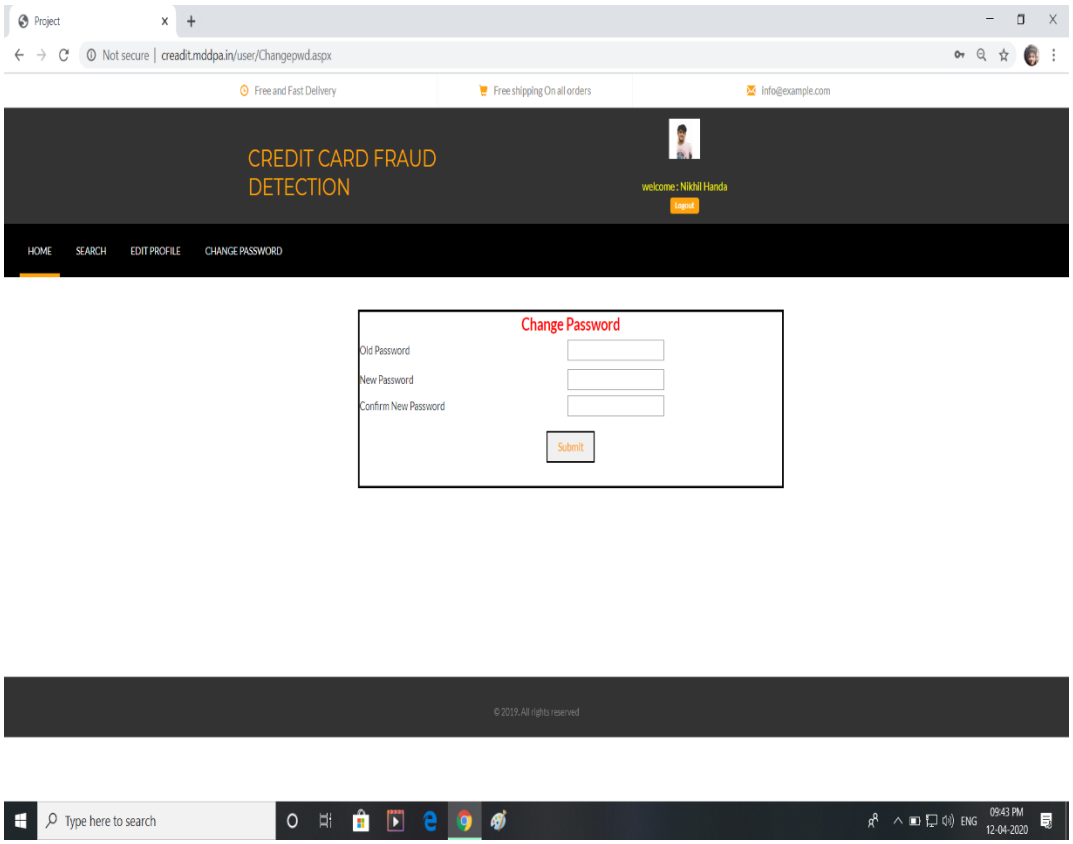

FIG 4.9: - CHANGE PASSWORD.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 9, September 2020||

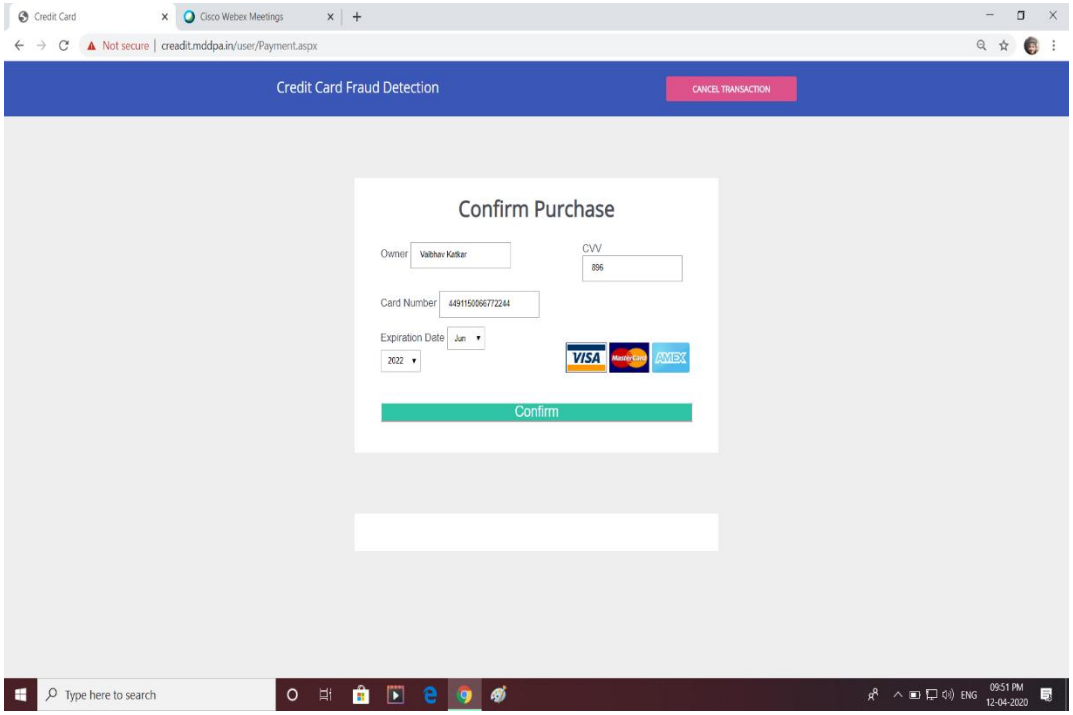

FIG 4.10: - FRAUDANTAL CARD DETAILS.

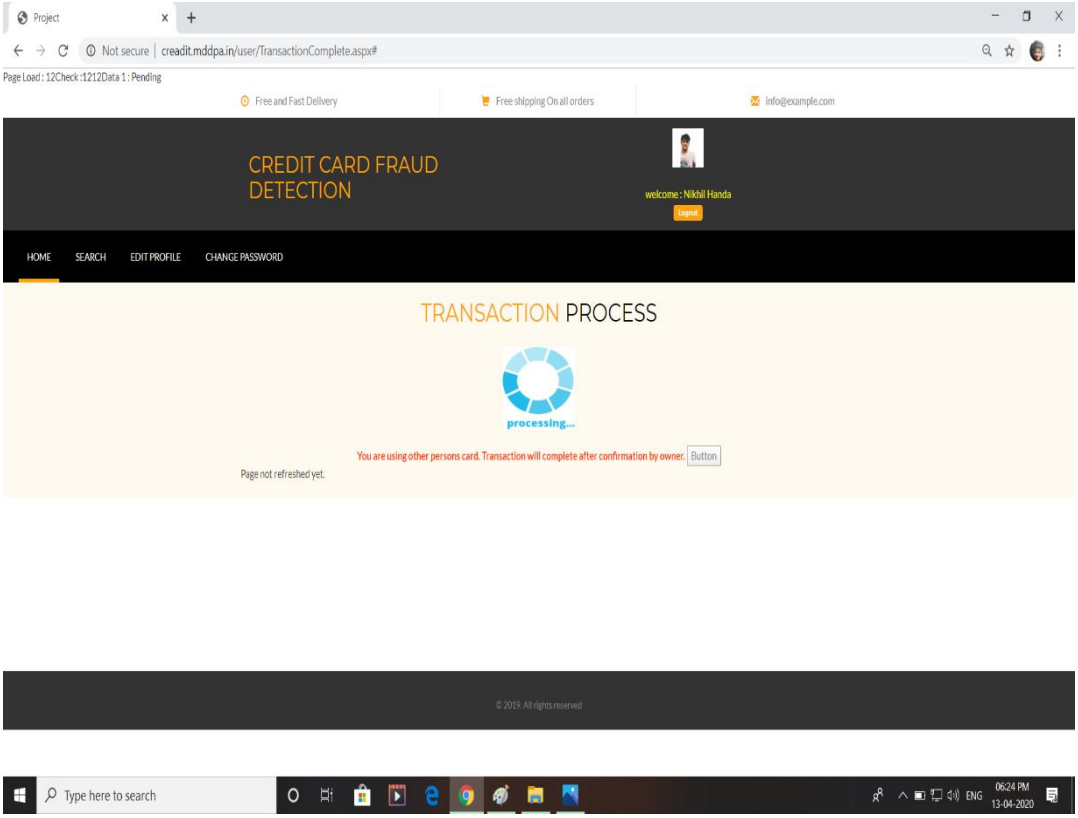

FIG 4.11: - UNUSUAL ACTIVITY DETERMINED.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 9, September 2020||

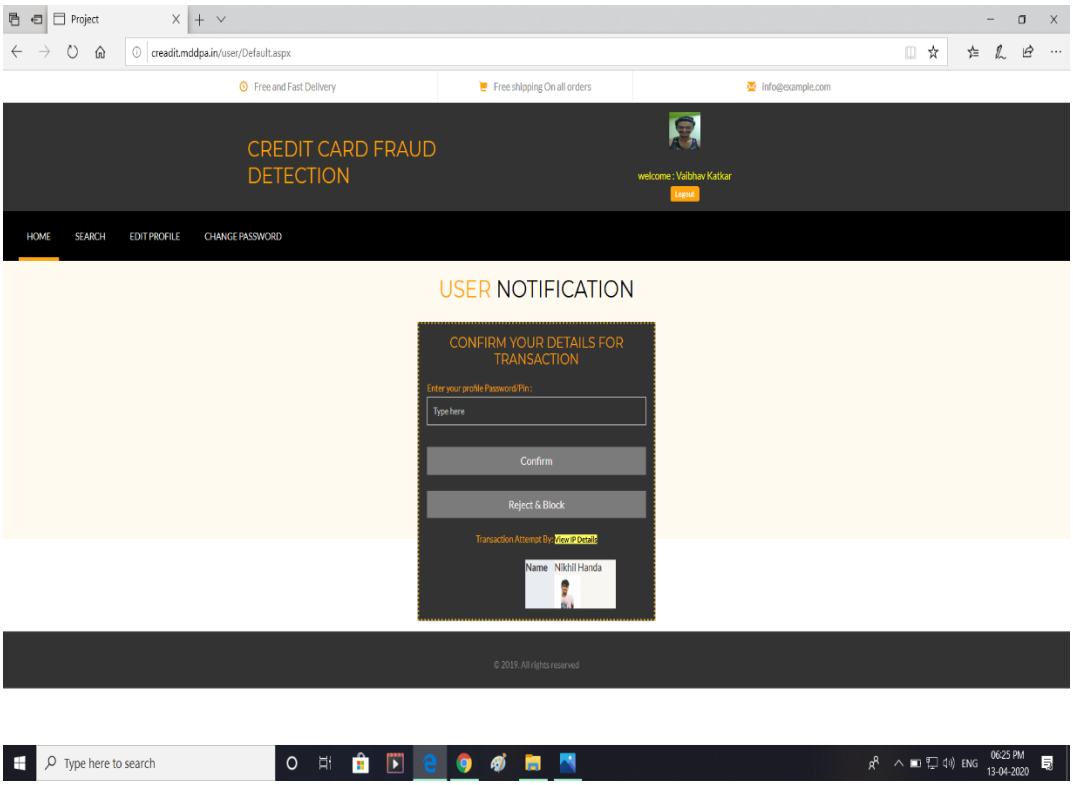

FIG 4.12: - FRAUD DETECTED BY THE CARD OWNER.

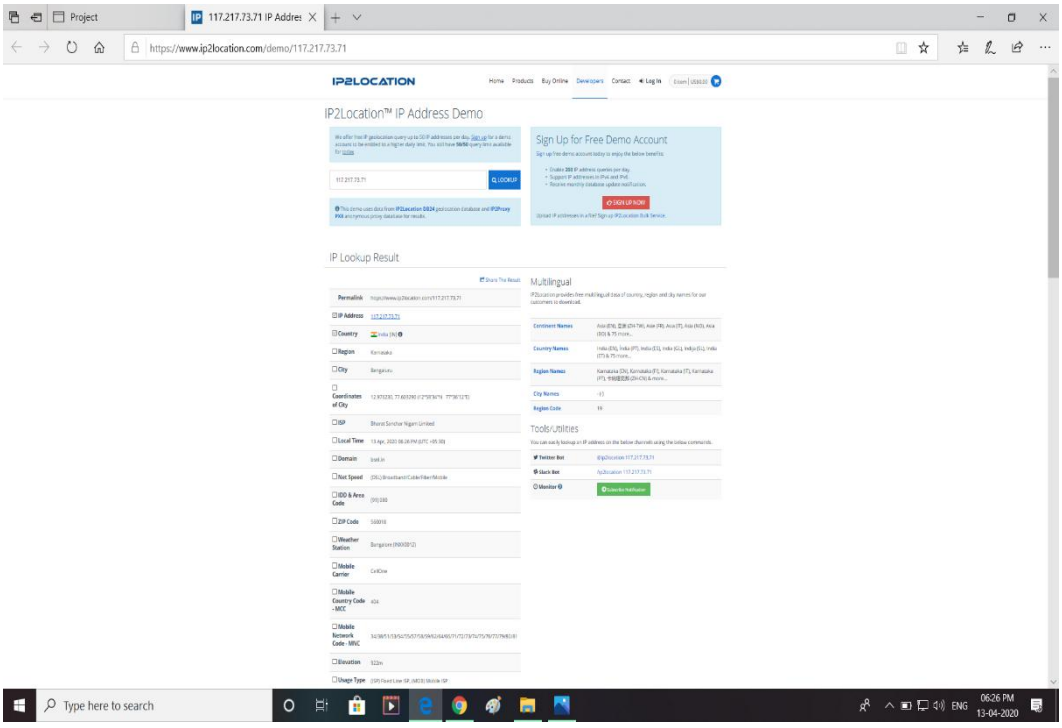

FIG 4.13: - DETAILS OF THE FAKE USER.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 9, September 2020||

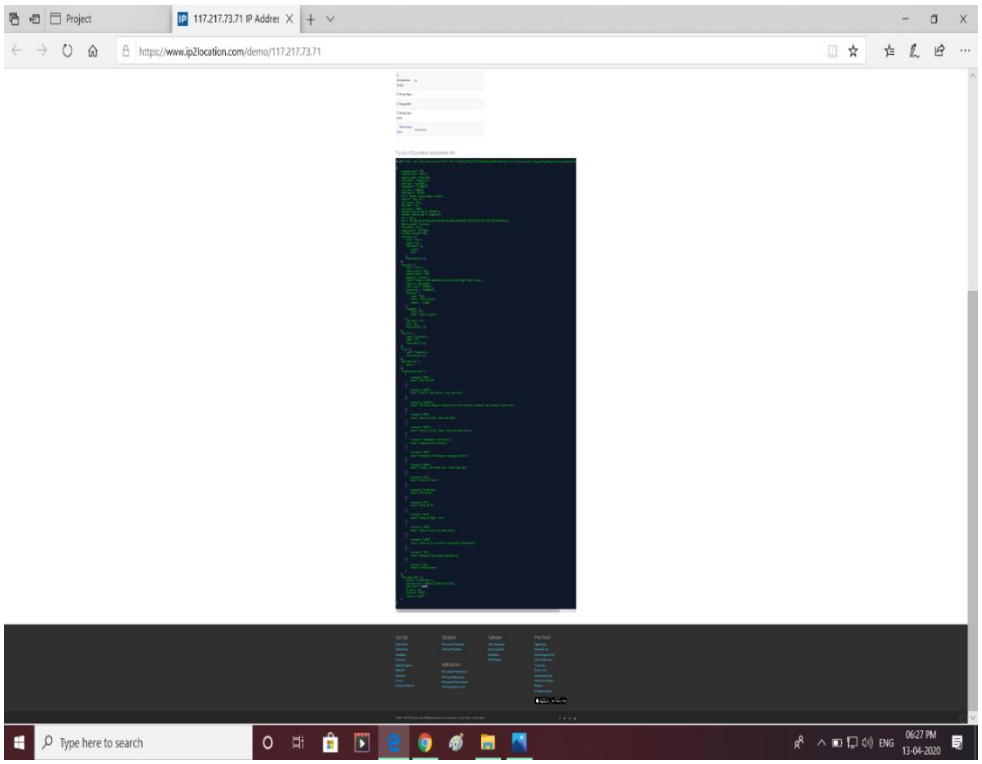

FIG 4.14: - IP ADDRESS & SERVER LOCATION OF THE FAKE USER.

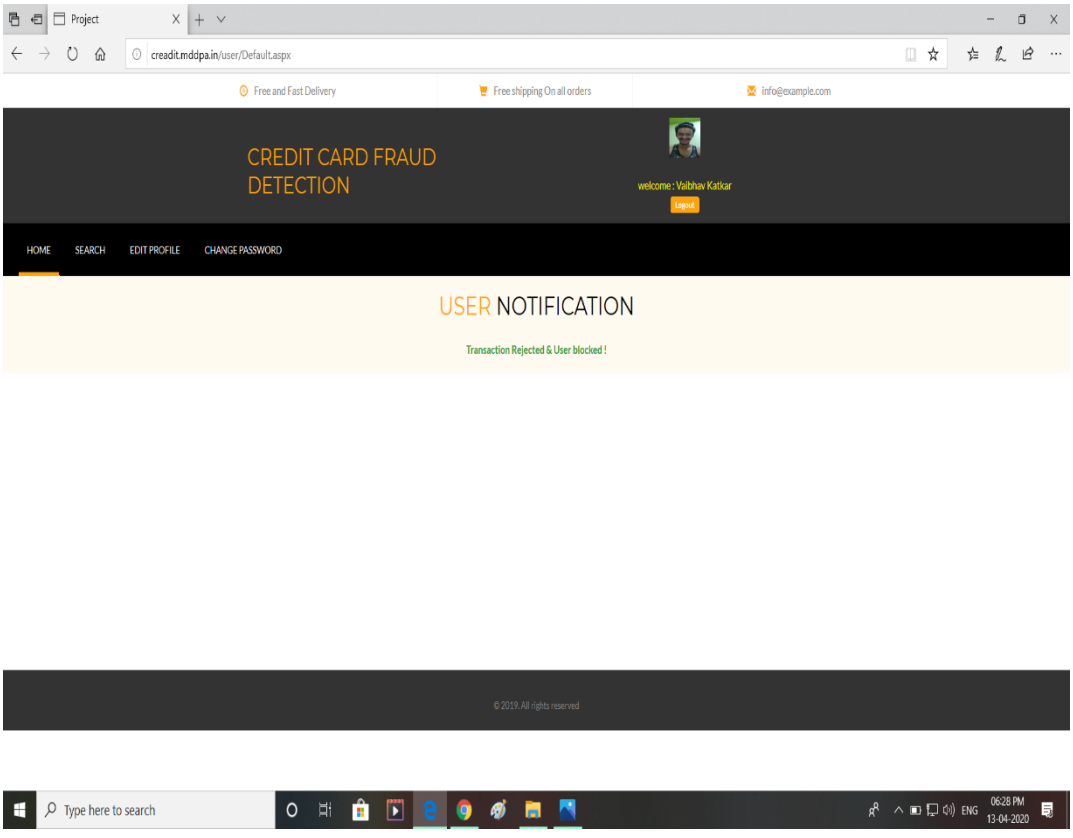

FIG 4.15: - TRANSACTION REJECTED & FAKE USER BLOCKED.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 9, September 2020||

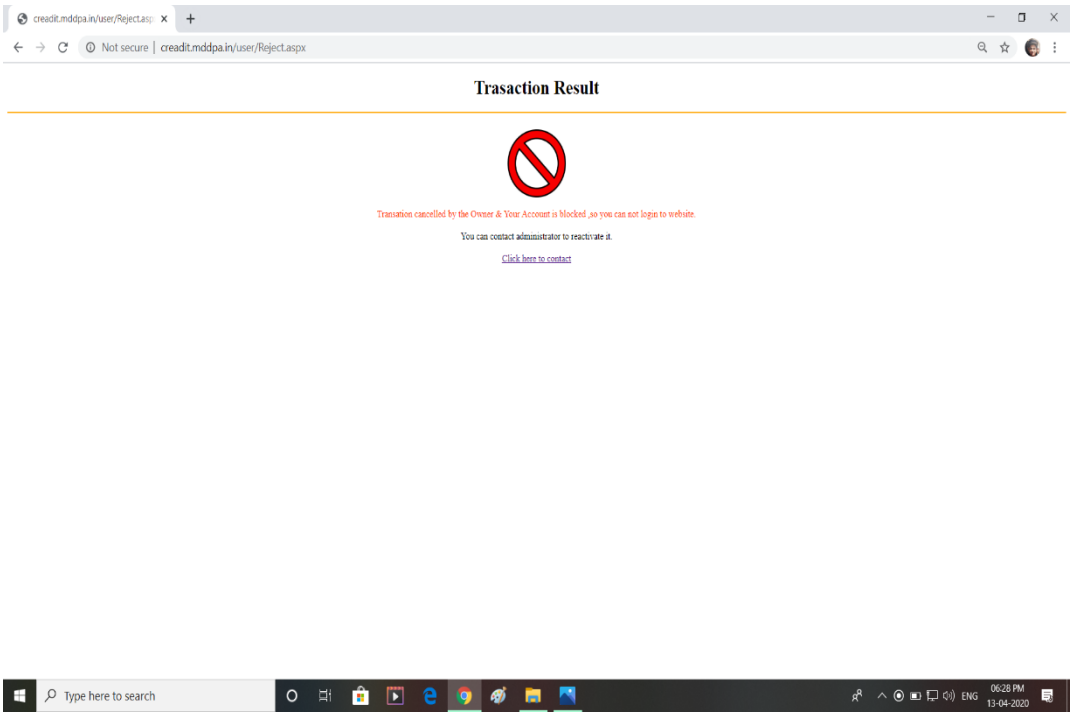

FIG 4.16: - USER BLOCKED BY THE ADMIN.

IV. CONCLUSION

Clearly, credit card fraud is an act of criminal dishonesty. This article has reviewed recent findings in the credit card field. To improve merchants' risk management level in an automatic and effective way, building an accurate and easy handling credit card risk monitoring system is one of the key tasks for the merchant banks. From an ethical perspective, it can be argued that banks and credit card companies should attempt to detect all fraudulent cases. The main tasks will be to build scoring models to predict fraudulent behaviour, taking into account the fields of behaviour that relate to the different types of credit card fraud identified in this paper, and to evaluate the associated ethical implications.

There are many ways of detection of credit card fraud. So basically, we had created one e-commerce website where user can register and login and can able to buy the goods. In payment section we have applied the Luhn's Algorithm to identify which type of card the user has been using and also applied AES algorithm to securely save the card details of the user to the database. Although there are several fraud detection techniques available today but none is able to detect all frauds completely when they are actually happening, they usually detect it after the fraud has been committed. If the user is valid then the payment will be done successfully but if someone else will using the another user card then by using data mining techniques the system will able to find out that fraud user is using valid user card at this time one message has been send to the original user, if the user approve the transaction then the payment has been done successfully but if user deny the transaction then he can be able to find the location of fraud user and also able to block the account of the fraud user who is using his credit card. So, the major task of today is to build an accurate, precise and fast detecting fraud detection system for credit card frauds that can detect not only frauds happening over the internet like phishing and site cloning but also tampering with the credit card itself.

V. FUTURE WORK

Though overall the project is completed successfully, further study could be conducted to track the exact location of the fraud. Furthermore, such security can be applied to different modes of online transactions in order to provide a secure and safe atmosphere for the online transactions to an E-commerce website.

REFERENCES

1.AkinbohunFolake and Atanlogun Sunday Kolawole, "Credit Card Fraud Detection System in Commercial Sites", European Journal of Engineering Research and Science Vol. 3, No. 11, November 2018

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 9, September 2020||

2.Kaneeka Joshi, "A review of Credit card Fraud Detection techniques in ecommerce", Academic Journal of Forensic Sciences,ISSN: 2581-4273, Volume 01, Issue 01, April-2018
3.G.Suresh and R.Justin Raj , "A Study on Credit Card Fraud Detection using Data Mining Techniques", International Journal of Data Mining Techniques and Applications Volume: 07, Issue: 01, June 2018, Page No.21-24, ISSN: 2278-2419
4.Linda Delamaire , Hussein Abdouand John Pointon (UK),"Credit card fraud and detection techniques: a review",Banks and Bank Systems, Volume 4, Issue 2, 2009
5.Suman and Nutan, "Review Paper on Credit Card Fraud Detection", International Journal of Computer Trends and Technology, volume 4, Issue 7,July 2013
6.R.J. Baton and D. J. Hand (2002), "A review on statistical fraud detection: statistical science. International Journal of Science and Technology" Volume 17, issue I, pp 15.
7.T.P. Bhatla, V. Prabhu and A. Dua (2003),"Understanding credit card fraudsreview on card Business", pp 20.
8.D.Kayong, Z.Ru and G.Hong (2012), "Analysis and study of detection of credit card fraud in E-commerce"Vol.13, pg 12-17.
9.M. S. Khan and S. S. Mahaptra (2011), "Service quality evaluation in internet banking website quality in India,A webqual approach great lakes herald", pg 40-58.
10.Paterson and Ken, "Credit card issuer fraud management, report highlights. Mercator Advisory Group", Archived from the original (PDF) December 2008.
11.Hassibi, Khosrow, "Detection payment card fraud with neural networks in book. Business Applications of neural networks, Singapore-New Jersey-London-Hong Kong", World Scientific, 2000, pp. 141–158.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.512

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details