SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY
[DEEMED TO BE UNIVERSITY]
Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE
www.sathyabama.ac.in

National Conference on Computational Intelligence and Communication Networks

Springer CCIS

N C C I C N

24TH – 25TH MARCH 2022

NCCICN

Certificate of Presentation

This is to certify that ***Dr./Mr./Ms. CHAVVA NIKHITA,*** *of* ***Sathyabama Institute of Science and Technology,*** *has presented a paper entitled* ***"Credit Card Fraud Detection with Formula based Authentication",*** *in the National Conference on Computational Intelligence and Communication Networks (NCCICN 2022).*

Dr. T. Sasikala
Conference Chair, Professor & Dean
School of Computing

Dr. L. Lakshmanan
Convener
Professor & Head, CSE

Dr. S. Vigneshwari
Convener
Professor & Head, CSE

SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY
[DEEMED TO BE UNIVERSITY]
Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE
www.sathyabama.ac.in

National Conference on Computational Intelligence and Communication Networks

Springer CCIS

N C C I C N

24TH – 25TH MARCH 2022

NCCICN

Certificate of Presentation

This is to certify that ***Dr./Mr./Ms. BHAVYA BABU,*** *of* ***Sathyabama Institute of Science and Technology,*** *has presented a paper entitled* ***"Credit Card Fraud Detection with Formula based Authentication",*** *in the National Conference on Computational Intelligence and Communication Networks (NCCICN 2022).*

Dr. T. Sasikala
Conference Chair, Professor & Dean
School of Computing

Dr. L. Lakshmanan
Convener
Professor & Head, CSE

Dr. S. Vigneshwari
Convener
Professor & Head, CSE

ABSTRACT

Credit cards have become an important part of digital transactions. Days have come where people don’t have to carry cash in their pockets and just a small card is enough to make all the transactions. The problem with credit cards is that the password can be hacked and can easily lead to fraud. In this project, credit card fraud can be detected using Hidden Markov Model (HMM) and formula based authentication. In the Existing system, credit card transactions have become commonplace today and so are the frauds associated with it. In the proposed system, machine learning supervised and unsupervised algorithms have been applied to detect master card deception in an imbalanced dataset. In the modification process, an application is developed for a banking sector particularly for a credit or ATM card. Users can create an account and get the ATM or credit card along with a unique formula which should be used during suspicious transactions. The user behavior of every transaction is tracked by Hidden Markov Model and if there are any occurrences of suspicious transactions, then a message is sent to the user with the keys that are required to complete the formula. After the user applies the keys to the formula the solution must be entered as the password in order to complete the transaction successfully.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATIONS

ABBREVIATION	EXPANSION
HMM	Hidden Markov Model
FDS	Fraud Detection System
FPS	Fraud Prevention Systems
OTP	One Time Password
EMI	Equated Monthly Installment
OOP	Object Oriented Programming
API	Application Programming Interface
JVM	Java Virtual Machine
JRE	Java Runtime Environment
RMI	Remote Method Innovation
EJB	Jakarta Enterprise Beans
JSE	Java Standard Edition
JEE	Java Enterprise Edition
JDK	Java Development Kit
JME	Java Mobile Edition

CHAPTER 1

INTRODUCTION

Credit cards are being used for digital transactions as a payment method by both online and offline buyers in a huge way. On the other hand, this method has few drawbacks. Criminals, hackers and perpetrators have started targeting credit card based transactions. For any transaction, only the card information has to be entered and the card need not be present physically. In most cases, a One Time-Password (OTP) authentication is used as an extra safety factor. Specifically for international transactions, a method called Card-Not-Present, is used where only the card details are required rather than the physical card for unauthorized purchases. It is very easy to get the card details using methods like shoulder surfing, buying card information, credit card stealing and web traffic sniffing.

The main victims of the credit card frauds are the card holder, the bank, and the merchant. One of the main duties of the credit card holder is to detect any suspicious activities and report fraudulent transactions to the issuing bank. The bank then takes the responsibility to investigate the problem and if any evidence for fraudulent activities are found, then the credit card transaction is reversed.

1.1 OBJECTIVE

The main objective of this project is to detect credit card frauds and authenticate using formula based authentication.

1.2 OUTLINE OF THE PROJECT

Credit card information can be fetched easily through various modernized techniques. Even though many credit card methods are emerging today, so is the fraud associated with it. Digital transactions do not require credit cards to be present physically instead authentication such as OTP methods are used. Even though there are many secured methods of transactions fraudulent activities occur frequently.

It is impossible to find out whether the credit card transaction is genuine or fraudulent. As a result, credit card fraud detection becomes more important to verify the authenticity of the transaction. To overcome this problem, user behavior is monitored using HMM model and formula based authentication is applied for security. In this process the user will be issued with a formula during credit card registration. Every transaction will be monitored by the HMM model and if any suspicious transaction is detected, the authentication key is sent to the user. The user must apply the formula with generated keys to find out and enter the correct solution as password in order to complete the transaction successfully.

1.3 ARCHITECTURE OF THE CREDIT CARD DETECTION AND AUTHENTICATION

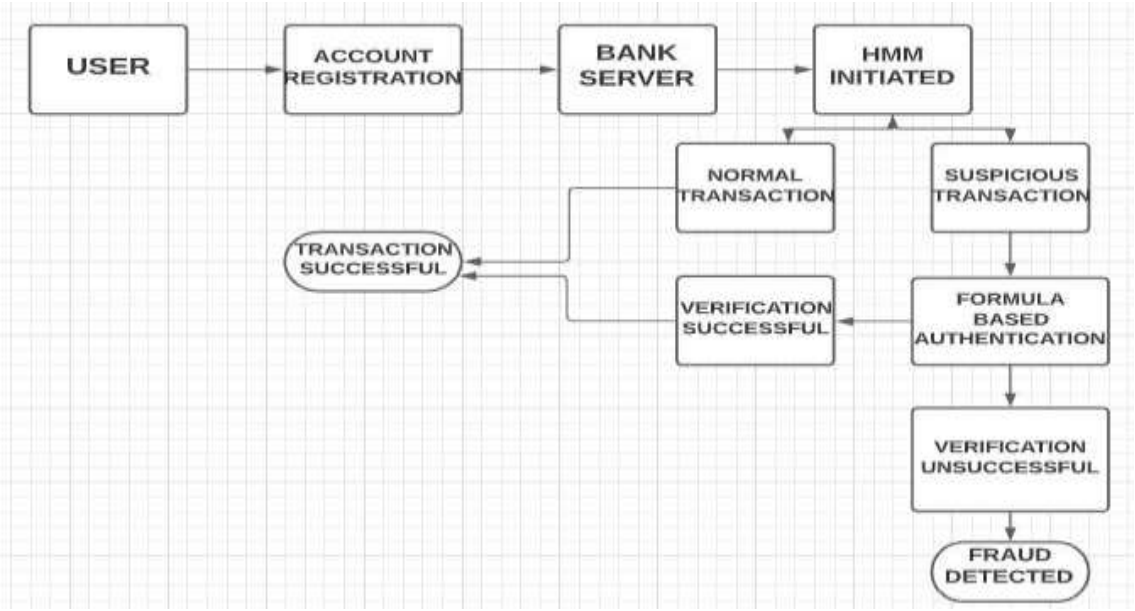

FIG 1.1 System Architecture of Credit card fraud detection system

SYSTEM ARCHITECTURE MODULES:

1. ***USER*** - User is an authorized person allowed to use a credit card. User is issued a credit card at the time of registration in a bank, along with the unique formula. Each of the transaction of the user will be tracked and monitored by the HMM model. Users will also follow the principle of formula based transaction.

2. ***INTEGRATING FORMULA BASED AUTHENTICATION*** - Formula Based Authentication is the main system used by this bank. This type of authentication allows the user to securely transact the money from the bank without having to worry about the fraudsters. This method of security prevents shoulder surfing or web tracking done by the fraudsters to get hold of the user's card information. In this verification process, the user is issued a formula at the time of registration and will use it along with a randomized key generated at the time of each suspicious transaction monitored by the HMM model.

3. ***REGISTRATION OF FORMULA*** - every user at the time of registration is given a unique formula, which is only known to the user. At a time of any suspicious transaction detected by the HMM model a randomized key for this formula will be sent to the user, which can be applied in the formula to get the solution. Once the password is applied, the transaction will be successful. This process is also called Formula Based Authentication.

4. ***SMART CARD*** - Smart card, also known as an interested circuit or chip card, is an authorization device which is used to control access to a resource since it is electronic. Smart card is basically a type or credit card embedded with an interesting circuit chip. Smart cards offer more security and confidentiality for the user. They use encryption techniques which prevent the tracking of information.

5. ***APPLICATION OF CREDIT CARD*** - Each transaction made by the user will be tracked and monitored by the HMM model. For suppose if the user transacts a certain amount of money each month, and suddenly extracts a huge sum of money, the HMM model monitoring the transaction pattern will raise a suspicion and send the user a unique key for the formula. Once the user applies the key to the formula, and answers with the correct solution, the transaction will be successful. In this way, the HMM model as well as the Formula Based Authentication will be demonstrated.

CHAPTER 2
AIM AND SCOPE OF THE PROJECT

2.1 AIM

The main aim of the project is to secure the account by adding formula based authentication along with the user behavior being monitored by using the HMM model. User behavior is monitored based on frequency of withdrawal and the amount of money withdrawn by the user.

2.2 SCOPE

The major benefit of the project is that it cannot be easily manipulated. The formula key which is generated during the transaction cannot be manipulated because it is random every time which will lead to high authentication. Even if the key is hacked by the fraudster, they will not be able to complete the transaction due to the unique formula which is only known to the user.

In the Existing system, card withdrawals are very routine among the people and the frauds corresponding to the improvement of security are increasing. In the proposed system, ML algorithms have been applied to detect master card deception in a disproportionate dataset. In the modification process, an application is developed for a banking sector particularly for a credit or ATM card. Users can create an account and get the ATM card along with a unique formula which should be used during suspicious transactions. The user behavior of every transaction is tracked by Hidden Markov Model and if there are any occurrences of suspicious transactions, then a message is sent to the user with the keys that are required to complete the formula. After the user applies the keys to the formula the solution must be entered as the password in order to complete the transaction