International Journal on Applications in Engineering and Technology
Volume 6: Issue 4 : Decemnber 2020, pp 5 –12 www.aetsjournal.com ISSN (Online) : 2455 - 0523

FACIAL RECOGNITION-BASED CREDIT CARD TRANSACTIONS USING GRASSMANN LEARNING ALGORITHM

PRABAKARAN.S , GOVINDASAMY. R, PALANISAMY.M , PUNITHA.N

Abstract— Money plays a crucial role in today's world, and various payment methods are available at Point of Sales (POS) to facilitate transactions, including cash on delivery, online payments, credit card transactions, and monthly installments. When it comes to online transactions, customers typically have options such as credit/debit cards or internet banking. Credit cards are widely used due to their convenience, but they also present security challenges, as attackers or hackers may attempt to steal sensitive information during these transactions.To address these security concerns, we propose a credit card transaction system that leverages facial recognition and face detection technologies through a web application. One of the primary concerns for credit card users is the potential for privacy breaches, especially when they share their credit card information with unknown individuals or in cases of card loss. Our system aims to mitigate the risks associated with credit card fraud.Our proposed system involves matching the user's facial image with a dataset of registered users, and we maintain a database for authentication purposes. This approach utilizes the Grassmann learning algorithm for facial recognition during the transaction process. If the facial images match, indicating the user's authenticity, the transaction is allowed to proceed. However, if there is no match, the user will be denied the transaction, enhancing security and reducing the risk of fraud.

I. INTRODUCTION

In the traditional credit card transaction method, the cardholder physically provides their card to the merchant for payment processing. For any fraudulent activity to occur in this scenario, an attacker would need to physically steal the credit or debit card. If the cardholder fails to detect the theft of their card, it could lead to substantial financial losses for the credit card company. Typically, only a limited set of crucial credit card details, including the card number, expiration date, and security code, is required to complete the transaction successfully.

This project entails a user making purchases via an E-Commerce Application. Upon selecting a product and completing the purchase, the user has the option to settle the payment through a credit card transaction that incorporates face detection technology. The system verifies the user's identity by capturing their face via a camera. Once a successful face detection process is completed, the user is then allowed to proceed with paying the amount for their purchase.

- Enhance the security of credit card transactions within E-commerce applications by implementing cutting-edge face recognition technology.
- After the successful completion of the face detection process, enable users to seamlessly proceed with the payment process.
- Upon order placement, automatically send email notifications to customers.

By achieving these goals, credit card companies, financial institutions, and businesses can effectively reduce the potential for financial losses and safeguard the interests of their customers.

II. ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

Machine Learning (ML) is a subset of Artificial Intelligence (AI) with a primary focus on utilizing data and algorithms to emulate human learning processes. It employs statistical techniques to train algorithms for tasks such as classification, prediction, and data mining. The industry often uses terms like deep learning, machine learning, and sometimes neural networks interchangeably, though

Prabakaran.S, Faculty of Information Technology, Dhanalakshmi Srinivasan Engineering College.
Govindasamy.R , Faculty of computer science and engineering, Dhanalakshmi Srinivasan Engineering College.
Palanisamy.M , Faculty of Information Technology, Dhanalakshmi Srinivasan Engineering College.
Punitha.N, Faculty of Information Technology, Dhanalakshmi Srinivasan Engineering College.

there are nuanced distinctions among these technologies.

Deep learning is a subset of machine learning that emphasizes training algorithms with minimal human intervention. It accomplishes this by transforming unstructured data into manageable segments through a process known as dimensionality reduction. On the other hand, neural networks, also referred to as artificial neural networks, consist of layers of nodes, including an input layer, multiple hidden layers, and an output layer. Each node has associated weights and thresholds and is interconnected with other nodes. Essentially, if the output layer's value exceeds its threshold, data is transmitted to the next layer in the network. Neural networks come in two forms: basic neural networks with two or three layers and deep neural networks with more than three layers.

ML finds extensive applications, such as automatic speech recognition using natural language processing to convert spoken language into text. It is also widely employed in mobile devices for voice search and serves as a customer touchpoint on websites and apps, addressing common inquiries related to pricing, shipping, delivery, feedback, and returns. Furthermore, ML plays a crucial role in virtual and voice assistants, automating routine tasks. In the realm of computer vision, ML extracts meaningful insights from images, videos, and visual data, particularly in fields like radiology and autonomous vehicles. In marketing, ML analyzes consumer behavior patterns to devise cross-selling strategies and offer personalized recommendations to e-commerce customers.

Machine learning represents an application of artificial intelligence (AI) wherein systems possess the capability to autonomously learn and enhance their performance through experience, without requiring explicit programming. It centers on the creation of computer programs capable of accessing data and autonomously acquiring knowledge.

The learning process commences with observations or data, which may encompass examples, firsthand experiences, or guidance. These inputs are used to identify patterns within the data, subsequently enabling the system to make more informed decisions in the future based on the provided examples. The fundamental objective is to empower computers with the capacity to learn independently, free from human intervention or assistance, and adapt their actions accordingly.

Machine learning algorithms are commonly categorized as either supervised or unsupervised:

1) Supervised Machine Learning:

In supervised learning, a data scientist or machine learning expert provides both input data and the desired output or outcome. During the training phase, the algorithm uses this labeled data to learn and create a predictive model. Feedback on the accuracy of predictions is also given during this process. Data scientists determine which variables or features the model should consider when making predictions. After training, the algorithm can apply what it has learned to make predictions on new, unseen data. It can also compare its predictions to the correct outcomes to make necessary adjustments for improved accuracy.

2)Unsupervised Machine Learning:

Unsupervised learning, on the other hand, doesn't require labeled data for training. Instead, it employs an iterative approach, often referred to as deep learning, to analyze data and discover patterns or structures within it. Unsupervised learning algorithms, including neural networks, excel in handling complex tasks like image recognition, speech-to-text conversion, and natural language generation. These algorithms sift through vast amounts of training data to automatically identify subtle correlations among multiple variables. Once trained, the algorithm can leverage its knowledge to interpret new data. This type of learning has become feasible in the era of big data, as it demands substantial volumes of training data.

Additionally, there are other categories of machine learning:

3)Semi-Supervised Machine Learning:

This falls between supervised and unsupervised learning. It uses a combination of labeled and unlabeled data for training. Typically, a small portion of data is labeled, while a larger portion is unlabeled. Semi-supervised learning can

significantly improve learning accuracy and is chosen when obtaining labeled data is resource intensive.

4)Reinforcement Machine Learning:

This method focuses on interactions between the learning system and its environment. It involves producing actions and learning from errors or rewards. Reinforcement learning often employs trial and error, delayed rewards, and feedback to help agents determine the best actions within specific contexts, with the goal of maximizing performance.

Machine learning empowers the analysis of vast datasets, delivering quicker and more accurate results for tasks like identifying opportunities or risks. However, it may necessitate substantial time and resources for proper training. When combined with artificial intelligence (AI) and cognitive technologies, machine learning becomes even more effective in processing extensive data volumes.

5) Facial recognition:

Facial recognition harnesses the power of AI algorithms and machine learning to identify human faces amidst complex backgrounds. Typically, the algorithm initiates its process by searching for key facial landmarks, beginning with the eyes and progressing to eyebrows, nose, mouth, nostrils, and iris. Once all these facial features are captured, additional validations are performed using extensive datasets containing both positive and negative images to confirm the presence of a human face.

Facial recognition employs various techniques, each with its own set of advantages and drawbacks. These techniques include feature-based, appearance-based, knowledge-based, and template matching methods.

Feature-based methods rely on specific facial features like eyes or the nose to detect a face, but their accuracy can be affected by factors such as noise and lighting conditions.

Appearance-based methods utilize statistical analysis and machine learning to match facial characteristics, offering robust recognition capabilities.

In a knowledge-based approach, facial recognition is based on predefined rules, although creating comprehensive and accurate rules can be a complex and challenging task.

Template matching methods, on the other hand, compare facial images with previously stored patterns or features and correlate the results to identify a face. However, this method may struggle to account for variations in scale, pose, and facial shape.

6) Background and Related Work:

Sahu, A., Harshvardhan, G. M., & Gouri Saria, M. K. [1], In their paper, the authors propose two strategies to enhance the detection of fraudulent transactions in credit card systems. The first strategy involves resampling the minority class (fraud cases) to balance the dataset. In the second approach, they assign higher class weights to fraud instances, making them ten times more important in error calculations.

Panda, A., Yadlapalli, B., & Zhou, Z. [2], This paper addresses credit card fraud as unauthorized and unwanted account usage. The authors emphasize the need to research and understand fraudulent activities to prevent future incidents. They discuss the challenges of treating fraud detection as a classification problem and the limitations of conventional data mining techniques.

Kumar, S., Gunjan, V. K., Ansari, M. D., & Pathak, R. [3], This paper explores how banks can use technology to improve customer satisfaction and offer integrated banking services. It highlights the role of technology in modern banking, including funding and promotions linked to debit and credit cards.

Vinaya, D. S., Basapur, S. B., Abhay, V., & Natesh, N. [4], The authors discuss the security features of credit cards and the efforts of credit card companies to introduce smart cards as alternatives. They also mention the use of computational techniques like Neural Networks (NNs) for tracking and identifying suspicious transactions.

Lucas, Y., & Yurovsky, J. [5], This paper delves into credit card fraud detection using data-driven methods and various machine learning algorithms. It emphasizes the challenges posed by unbalanced datasets and the need for specialized approaches.

Singh, G., Kaushik, D., Handa, H. [6], Similar to the previous paper, this work focuses on credit card fraud detection using data-driven methods and machine learning algorithms. It highlights the complexities of dealing with unbalanced datasets in fraud detection.

Aziz, A., & Ghouls, H. [7], This paper addresses the widespread problem of fraud in various industries, including finance, insurance, and law enforcement. It discusses the use of data mining and facts to identify and mitigate fraud efficiently.

Shah, A., & Mehta, A. [8], The authors discuss the rising use of credit cards for online transactions and the subsequent increase in credit card fraud incidents. They mention common fraud types, including those perpetrated by hackers and cardholders.

Muttipati, A. S., Viswanathan, S., Senapathi, R. [9], This paper focuses on credit card fraud scenarios, such as application fraud, lost or stolen cards, and account theft. It specifically addresses Card Not Present (CNP) fraud and its various forms.

Iwari, P., Mehta, S., Sakhuja, N. [10], The authors highlight the versatility of credit cards for various purchases and the perks they offer. They mention the growth of credit card usage in India and its significant impact on sales and the economy by 2022.

III.METHODOLOGY

In the credit card transaction method, the cardholder physically hands over their card to the merchant for payment. To carry out fraudulent activities in this type of transaction, an attacker must physically steal the credit or debit card. If the cardholder doesn't detect the theft promptly, it can lead to significant financial losses for the credit card company. Typically, such purchases occur over the phone or online, where scammers only need access to a few key credit card details, including the card number, expiration date, and security code, to execute fraud. In many cases, the actual cardholder remains unaware that their card information has been compromised.

One effective way to identify this fraudulent activity is by scrutinizing the spending history of each card and identifying any deviations from the cardholder's usual purchasing patterns. Detecting fraud by examining a cardholder's historical purchase data shows promise in reducing the success rate of fraudulent activities. Various algorithms and techniques have been developed, making facial recognition a pivotal element for cardholder authentication.

It's worth noting that these cards are distinct from standard office cards or other types of cards. Many institutions utilize electronic ID (e-ID) cards for access control authorization, granting access to resources like rooms or elevators. In such cases, having possession of the card alone can provide access to these resources, making it possible to steal or duplicate a legitimate user's e-ID card. This also opens up the possibility of borrowing such e-ID cards from third parties without limitations.

Given these concerns, existing frameworks propose innovative solutions to prevent unauthorized individuals from using electronic cards and restrict the misuse of stolen cards. The goal is to design a system that remains user-friendly, minimizes disruptions to users' habits, and enhances security.

The existing system having the disadvantages of following things:

- Customers often experience frustratingly long wait times during the checkout process.
- The billing process in a store can be the most time-consuming part of the shopping experience.
- Damaged or dirty barcodes may not be readable by scanning devices.
- Barcodes typically have limited data storage capacity, primarily accommodating numeric data, and require more space as they are one-dimensional.

The proposed system has been meticulously developed following a comprehensive analysis of user requirements. It represents a computerized solution that effectively addresses the shortcomings of manual systems. This online shopping system, integrated with credit card transactions and face recognition technology, simplifies the operational aspects and creates a user-friendly environment that offers enhanced flexibility.

The system offers several advantages:

- **Efficiency**: It compensates for the limitations of

manual processes, allowing for streamlined and efficient operations.

- **User-Friendly**: The user interface has been designed with user convenience in mind, providing a seamless and user-friendly experience.
- **Report Generation**: Retailers benefit from the system's ability to generate reports quickly and produce more accurate results.
- **Security**: The system employs face recognition technology to ensure the secure authenticity of credit card holders during online shopping transactions.

The core of the face recognition component relies on the Grassmann Learning approach, a dimensionality reduction algorithm. It maps subspaces as points onto a curved surface, facilitating geodesic distance measurements between subspaces. Grassmann learning's key advantage over traditional manifold learning techniques is its ability to handle high-dimensional feature representations that may not conform to Euclidean space. This method maps subspaces based on orthogonal constraints, enhancing between-class discrimination through geometric structuring and accommodating missing data via subspace spanning. Grassmann learning effectively embeds high-dimensional subspaces and kernelizes the embedding onto a projection space, facilitating efficient distance computations.

In this project, users can browse and purchase products through the website. After making their selections, users can complete their transactions using credit card payments with face detection verification. The face detection process captures the user's face through a camera, and upon successful verification, the user can proceed to make the payment.

Proposed system having the advantages of following things,

- **Data Storage**: The system can store data both horizontally and vertically, optimizing storage efficiency compared to barcode systems.
- **Security**: It ensures safe and secure transactions, enhancing user trust.
- **Automation**: It automates existing manual information systems, reducing the need for manual processing.
- **Administrative Oversight**: The system allows administrators to monitor daily information exchanges on the server.
- **Speed**: It increases the processing and transfer speeds of information across the network, improving overall efficiency.

The project utilizes a Windows operating system, with Python as the front-end language and MySQL serving as the back-end database. The integrated development environment (IDE) chosen for this project is PyCharm.

System architecture encompasses the overarching structural framework of a software system, achieved through the processes of decomposition and composition, while adhering to specific architectural styles and quality attributes. The design of a software architecture should align with the primary functional and performance prerequisites of the system, in addition to meeting non-functional requirements like reliability, scalability, portability, and availability.

IV. Experiments And Results

1)Framework Development:

Framework creation involves the development of an E-commerce application with a range of proposed features. Within this application, the admin has the capability to input product details such as product ID, name, type, price, quantity, and more. Users, on the other hand, are able to create their accounts by providing essential information to the system. The user registration form includes fields such as username, email, gender, mobile number, address, and credit card details, among others. To enhance security, the user's facial image is captured via web cameras and stored in a database for future verification. All of these details are meticulously stored in the database.

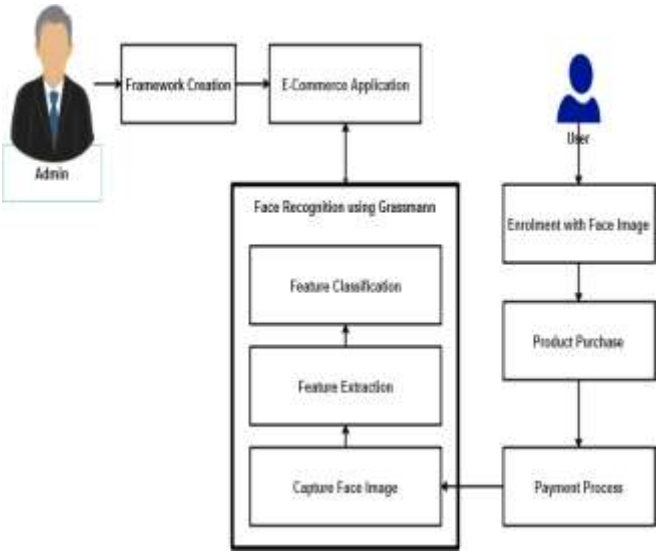
2)Product Purchase

In the product purchase module, users can log in to the E-commerce application and browse products for potential purchase. They can access detailed information about each product, including its name, type, price, description, and more. After reviewing the available products, users can select the items

that align with their needs. The user's purchase details are then relayed to the administrator.

3)Face Image Acquisition

Within the proposed E-Commerce application, users can securely complete their payments using a face recognition approach. This module encompasses the user's card details, such as their name and card number, as well as the transaction amount. Upon successful entry of these card details into the system, the user's facial image is captured using a web camera. Subsequently, the captured facial image is compared to the database of cardholder accounts. If there is a match between the user's facial image and the database, the payment is processed. In the absence of a match, the payment transaction is not authorized.



4)Facial Classification

Facial classification is a process that involves the extraction of facial features, which are then compared with a database to verify a user's identity. Key facial features, such as the nose, eyes, and lips, are extracted as feature values and stored in a grid. This framework can be effectively constructed using the Grassmann manifold learning algorithm. The feature data extracted from specific facial images serves as a biometric identifier for individual recognition. Unlike traditional systems that rely on authorized IDs or keys, facial recognition systems focus on establishing the presence of an authenticated individual.

5)The Grassmann Algorithm:

The representation of data on Grassmann manifolds is widely utilized in various image and video recognition tasks. To enhance the utility of input Grassmannian data, several techniques are applied. These include creating complete rank mapping layers for transforming input Grassmannian data into more suitable forms, implementing orthogonal re-normalization layers to standardize resulting matrices, incorporating projection pooling layers to simplify model complexity in the Grassmannian context, and designing projection mapping layers to convert the resulting Grassmannian data into Euclidean forms for standard output layers.

In the training process of deep neural networks, stochastic gradient descent is employed on manifolds where the connection weights reside. A matrix generalization of backpropagation is utilized to update the model's parameters. Grassmannian data applications inspire the construction of deep neural network architectures for Grassmannian representation learning. This novel network architecture aims to deeply understand Grassmannian data within an end-to-end learning framework.

Discriminant learning on Grassmann manifolds typically involves embedding the Grassmannian into a Euclidean space. This can be achieved through tangent space approximation or by leveraging specific kernel functions to embed the manifold into a reproducing kernel Hilbert space. Once embedded into a Euclidean space, traditional Euclidean methods can be applied to the data, as Hilbert spaces respect Euclidean geometry.

The Grassmann manifold G(m, D) represents m-dimensional linear subspaces of R^D, and it is a compact Riemannian manifold with dimensions m(D-m). Points on this manifold are represented by orthonormal matrices Y of size D by m. However, the matrix representation of a point on the Grassmann manifold is not unique, and equivalence is determined by the span of the matrices. The Riemannian distance between two subspaces on the Grassmann manifold is typically measured as the

length of the shortest geodesic connecting the two points, but it can also be defined using principal angles for computational efficiency.

6)Payment Process

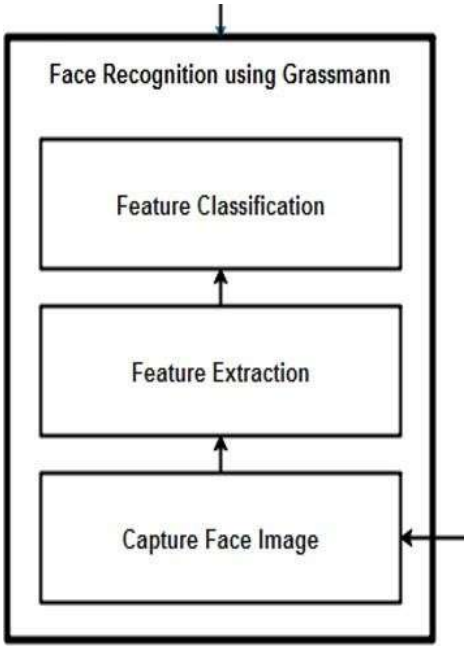
Once the face detection process is successfully completed, users can proceed to the payment process. During this phase, users can input the amount they wish to transfer, and the transaction is executed with a high level of security. If, for any reason, the classification process fails to detect the user's face image or identifies a fake user, the system will automatically send an email notification to the customer, indicating the issue during the Payment Process.

7)Overall Process

E-commerce is rapidly gaining acceptance and becoming a prevalent business model. Increasing numbers of businesses are implementing websites that enable commercial transactions over the internet. Online shopping has become a common practice. The objective of this project is to develop a versatile e-commerce store where customers can purchase various products, including books, CDs, computers, mobile phones, electronic items, and home appliances, all from the comfort of their homes via the internet.

An online store functions as a virtual shop on the internet where customers can browse a catalog, select products of interest, and add them to a shopping cart. At the time of checkout, the items in the shopping cart are presented as an order. Additional information is typically required to complete the transaction, including billing and shipping addresses, shipping preferences, and payment details such as credit card information. This project implements credit card transactions using face recognition technology, ensuring that the face detection process is successfully completed before proceeding to the next step. An email notification is promptly sent to the customer once the order is placed.

Sellers who offer products online often seek feedback from customers regarding their purchases. As e-commerce continues to grow in popularity, the volume of customer feedback about products also increases significantly. For popular products, feedback can accumulate into the thousands, making it challenging for potential customers to read and make informed decisions about their purchases. This project aims to address this issue by providing a system for managing and organizing customer opinions and reviews, which can be particularly valuable for both customers and product manufacturers who produce a wide range of products.



The motivation behind credit card fraud detection lies in the imperative need to safeguard individuals and businesses from substantial financial losses stemming from illicit transactions. Credit card fraud constitutes a form of financial misconduct where an individual illicitly employs stolen credit card details to carry out unauthorized purchases or withdrawals. The ramifications of such fraudulent activities can be financially devastating, potentially leading to bankruptcy or severe financial turmoil. Furthermore, these illicit transactions can tarnish the reputation of the financial institution or business that issued the compromised credit card.

Hence, the detection and prevention of credit card fraud are of paramount importance. This endeavor not only serves to shield the financial well-being of individuals and businesses but also plays a pivotal role in upholding trust and confidence within the financial system. Beyond monetary losses, credit card fraud can result in a myriad of adverse

consequences for victims, including identity theft and the compromise of personal information. By effectively detecting and thwarting credit card fraud, individuals and businesses can avert these detrimental outcomes, ensuring the preservation of their financial security.

8)Face Classification

Face classification refers to the process of extracting facial features and comparing them with a database for user verification. Key facial elements such as the nose, eyes, and lips are extracted as distinctive feature values. These attributes are stored in a grid format. The system is designed by employing Grassmann manifold learning computations. The feature data derived from specific facial images serves as a biometric identifier for individual recognition. Face recognition systems establish the presence of an authorized individual by evaluating the similarity between the presented face image and stored data, rather than simply verifying the use of a valid ID, key, or the user's knowledge of personal ID numbers (PINs) or passwords. When the resemblance between the two compared faces is highly significant, the face image is verified as authentic.

V. CONCLUSION

The project, titled " Facial Recognition-Based Credit Card Transactions," has been developed to meet all the specified requirements. It simplifies the process of recording details for online shopping, significantly reducing the likelihood of errors and ensuring efficient data management. Notably, this system stands out for its user-friendliness. It has the capability to generate reports on demand and offers a high level of interactivity, making it adaptable for future enhancements.

The codebase is designed with simplicity and comprehensibility in mind, allowing other teams aiming to improve the project to do so with minimal difficulty. Likewise, the documentation is presented in a straightforward and concise manner, aiding in the development process.

VI. FUTURE WORK:

Although face recognition technology can serve as an efficient method for fraud prevention, it is not entirely infallible. Subsequent efforts could center on the creation of supplementary security measures, including multi-factor authentication or the integration of biometric sensors, to further bolster the security of credit card transactions. Additionally, there should be a concerted effort to broaden the accessibility of this technology so that it becomes accessible to a wider range of consumers and businesses.

REFERENCES

1) Aanchal Sahu&HarshvardhanGM,"ADual Approach for Credit Card Fraud Detection using Neural Network and Data Mining Techniques, "*ieee*,pp. 1-7,2020.
2) Agyanpanda&.ZhiZhou,"Credit Card Fraud Detection Through Machine Learning Algorithm, "*ieee*,2021.
3) Sheo Kumar&VinitKumarGujan," CreditCard Fraud Detection, "*ieee*,pp.27-37,2022.
4) VinayaD&VanishreeAbhay,"CreditCardFraudDetectionSystems(CCFDS)usingMachineLearning,"*ieee*,2020.
5) YvanLucas&JohannesJurgovsky,"Creditcardfrauddetectionusingmachine,"*ieee*,2020.
6) GurpreetSingh&SuniKumar,"BioPay:ASecurePaymentGatewaythroughBiometrics,"*ieee*,pp.65-76,2021.
7) AmirAziz&HamidGhous,"FraudulentTransactionsDetectioninCreditCardbyusingDataMiningMethods:A Review,"*ieee*,2021.
8) AnkitShah&AkashMehta,"Comparative StudyofMachine LearningBased,"*ieee*,pp.53-59,2021.
9) AppalaSrinuvasuMuttipati&.SangeetaViswanandham, "Recognizing Credit Card Fraud Using Machine Learning Methods, "*ieee*,2021
10) Pooja Tiwari &. Simran Mehta"CREDIT CARD FRAUDDETECTION USING MACHINE LEARNING:ASTUDY,"*ieee*,2021.