International Journal of Soft Computing and Engineering (IJSCE)
ISSN: 2231-2307 (Online), Volume-14 Issue-5, November 2024

# A Comprehensive Strategy for Detecting Credit Card Fraud in E-Commerce Utilizing DNS Authentication

**Pradnya PatiL, Minal Sonkar, Pallavi Patil, Priyanka Deshmukh, Trupti Patil**

***Abstract:*** ***E-commerce has transformed global trade, enabling businesses to reach audiences worldwide since the World Wide Web's inception in 1990. Companies like Amazon demonstrate this growth, evolving from a small online bookstore to a retail giant. E-commerce's appeal lies in its global reach, cost-efficiency, and 24/7 availability. However, security challenges, especially credit card fraud, remain significant, causing substantial losses to businesses, particularly small and medium-sized enterprises. Addressing fraud in e-commerce through machine learning techniques is crucial. Techniques such as Logistic Regression, Decision Trees, and Hidden Markov Models each offer unique advantages and limitations for detecting fraud, with some able to operate in real time. These methods help reduce false positives and improve fraud detection, making them integral to secure e-commerce environments. This paper introduces a system that uses disposable domain names and custom DNS servers to detect transaction inconsistencies, thus addressing proxy-based fraud attempts. By generating unique hostnames for each transaction, the system enables real-time monitoring and validation of client transactions. This DNS profiling approach strengthens e-commerce security, reduces financial risks, and enhances trust. The findings underscore the need for advanced fraud detection, contributing to safer online transactions and offering valuable insights for future secure e-commerce systems.***

***Keywords:*** ***E-Commerce, Credit Card Fraud, NS Profiling, Fraud Detection, Transaction Security***

## I. INTRODUCTION

Ecommerce, also known as electronic commerce or internet commerce, refers to the buying and selling of goods or services using the internet, and the transfer of money and data to execute these transactions.

**Manuscript received on 27 October 2024 | Revised Manuscript received on 14 November 2024 | Manuscript Accepted on 15 November 2024 | Manuscript published on 30 November 2024.**
*Correspondence Author(s)
**Prof. Pradnya Patil***, Assistant. Professor, Department of Computer Engineering, K.J. Somaiya Institute of Technology, Mumbai (Maharashtra), India. Email ID: pradnya08@somaiya.edu
**Prof. Minal Sonkar**, Assistant. Professor, Department of Computer Engineering, K.J. Somaiya Institute of Technology, Mumbai (Maharashtra), India. Email ID: minal.sonkar@somaiya.edu
**Prof. Pallavi Patil**, Assistant. Professor, Department of Computer Engineering, K.J. Somaiya Institute of Technology, Mumbai (Maharashtra), India. Email ID: pallavi.mp@somaiya.edu
**Prof. Priyanka Deshmukh**, Assistant. Professor, Department of Computer Engineering, K.J. Somaiya Institute of Technology, Mumbai (Maharashtra), India. Email ID: p.deshmukh@somaiya.edu
**Prof. Trupti Patil**, Assistant. Professor, Department of Computer Science and Business Systems, Bharati Vidyapeeth (Deemed to be University), DET, Kharghar, Navi Mumbai (Maharashtra), India. Email ID: tspatil@bvucoep.edu.in



Ecommerce is often used to refer to the sale of physical products online, but it can also describe any kind of commercial transaction that is facilitated through the internet.

The practice of commerce and trading is very ancient and was limited to area. Region or country, until the “world wide web” was introduced in 1990 by tim berners lee, which gave the largest breakthrough to the commerce business around the world, as now you can trade with the whole world by sitting in any corner of the world. Any business can have their customer base expanded to the entire population of the earth.

One of the earliest ecommerce websites [7] was amazon started in 1994 in Washington, US and gained extreme popularity within just 2 months from launch, and today in 2020 it is the largest retail company with more than 280 billion revenues yearly, this shows the brilliant growth of ecommerce over the years and still the demand is exponentially growing.

Using Digital Marketing, E-commerce creates huge revenue as it helps to acquire customers and brand value. Customers are no longer dependent just on content or word-of-mouth before buying a product; they make sure to read the reviews about a product on all the platforms on which the product is listed.

According to the recent analysis, 37 million social media visits led to 529,000 orders approx. Out of others, Facebook helps to get more traffic to the website which leads to sales constituting.

### A. Advantages of E-Commerce

- E-commerce provides the sellers with a global reach. They remove the barrier of place (geography). Now sellers and buyers can meet in the virtual world, without the hindrance of location [3].
- Electronic commerce will substantially lower the transaction cost [9]. It eliminates many fixed costs of maintaining brick and mortar shops [10]. This allows the companies to enjoy a much higher margin of profit [11].
- It provides quick delivery of goods with very little effort on the part of the customer [12]. Customer complaints are also addressed quickly. It also saves time, energy and effort for both the consumers and the company [8].
- One other great advantage is the convenience it offers. A customer can shop 24×7. The website is always functional, it does not have working hours like a shop [13].
- Electronic commerce also allows the customer and the business to be in touch directly, without any intermediaries [1]. This allows for quick communication and transactions. It also gives a valuable personal touch.

### B. Disadvantages of E-Commerce

- The start-up costs of the e-commerce portal are very high. The setup of the hardware and the software, the training cost of employees, the constant maintenance and upkeep are all quite expensive.
- Although it may seem like a sure thing, the e-commerce industry has a substantial risk of failure. Many companies riding the dot-com wave of the 2000s have failed miserably. The elevated risk of failure remains even today.
- At times, e-commerce can feel impersonal. So, it lacks the warmth of an interpersonal relationship which is important for many brands and products. This lack of a personal touch can be a disadvantage for many types of services and products like interior design or the jewelry business.
- Security is another area of concern. Only recently have we witnessed many security breaches where the information of the customers was stolen. Credit card theft, identity theft etc. remain big concerns for the customers.
- Then there are also fulfillment problems. Even after the order is placed there can be problems with shipping, delivery, mix-ups etc. This leaves the customers unhappy and dissatisfied

## II. LITERATURE SURVEY

Aries Susanto; Putri Lestari; Sarip Hidayatuloh; Aida Fitriyani [1]-: Trustis a belief that others will behave reliably way in a relationship. Trust is still considered a qualification of consumers in deciding purchases. This study uses a quantitative approach, combining the Technology Acceptance Model with several other variables based on consumer confidence in transacting online. The population in this study were students of a government-owned university who had already traded online shopping. The distribution of questionnaires was carried out online using a multi-stage purposeful random sampling technique. Simple random sampling for the first stage and purposive sampling for the second stage. Furthermore, the data analysis process uses the PLS-SEM approach using SmartPLS 3.0. Trust formation models that take advantage of the extension of several variables have proven to be influential in measuring trust in online shopping transactions. This research can be used as consideration for formulators and policymakers related to online shopping business and as a benchmark for consumers by looking at factors that influence in conducting online shopping transactions.

Shouvik Sanyala, Shouvik Sanyala [2]-: Ecommerce, also known as electronic commerce or internet commerce, refers to the buying and selling of goods or services using the internet, and the transfer of money and data to execute these transactions. Ecommerce is often used to refer to the sale of physical products online, but it can also describe any kind of commercial transaction that is facilitated through the internet. These business transactions occur either as business-to-business (B2B), business-to-consumer (B2C), consumer-to-consumer or consumer-to-business. Ecommerce provides several benefits to sellers over traditional retailing. Some key benefits include overcoming geographical limitations, lower costs, 24 X 7 availability of products, gaining new customers through better search engine visibility, create targeted information, enable comparisons while shopping and eliminating travel time and costs for customers.

### A. Analysis on Credit Card Fraud Identification Techniques Based on Knn and Outlier Detection

Credit cards are a common payment method accepted offline and online and allow for cashless transactions. Making money and conducting other activities is simple, practical, and fashionable. Along with technological advancement, credit card fraud is also on the rise [4]. Additionally, it may be claimed that as worldwide communication has improved, economic fraud has dramatically increased. Every year, billions of dollars in losses are attributed to these fraudulent activities. These operations are carried out so tastefully that they resemble real business transactions. Simple pattern-related techniques and other less sophisticated approaches won't therefore be effective. All banks now require an effective fraud detection strategy in order to reduce confusion and establish order. For spotting fraudulent credit card transactions, a number of techniques are utilized, including machine learning, genetic programming, fuzzy logic, sequence alignment, etc. Together with these. These approaches are demonstrated to reduce false alarm rates and raise fraud detection rates. Any of these methods can be implemented on bank credit card fraud detection systems, to detect and prevent fraudulent transactions.

| Fraud Detection Techniques | Advantage | Disadvantage |
|---|---|---|
| Logistic Regression | It produces a simple probability formula for classification. It works well with linear data for credit card fraud detection | 1. It cannot be applied on non-linear data. 2. It is not capable of handling fraud detection at the time of transaction. |
| Decision Tree | This method can handle non-linear data as well. | 1. It involves complex algorithm and even a small change in the data can distract the structure of the tree. Choosing splitting criteria is also complex. 2. It cannot detect fraud at the time of transaction. |
| Hidden Markov Model. | This method is capable of detecting the fraudulent activity at the time of transaction. The HMM based models reduce the False Positive (FP) transactions predict as fraud though they are really genuine customer. | 1. It cannot detect the fraud in initial few transactions. |
| Support vector machine | This method is capable of detecting the fraudulent activity at the time of transaction. | 1. Sometimes it fails to detect fraud cases. |
| K-Nearest Neighbor Algorithm | There is no requirement of a predictive model before classification. | 1. The accuracy of the method depends on the measure of distance. 2. It cannot detect the fraud at the time of transaction. |

## III. PROBLEM STATEMENT

Security is a vast domain, but E-commerce platforms use trusted third-party payment

gateways and authentication services. But there is also a major problem with online transactions, which is credit card fraud, which is a field of research of its own. Credit Card fraud causes loss of billions of dollars annually to business; hence it is crucial to deal with this problem.

But there are certain challenges which online merchants face. Some of the aspects identified which will improve customer experience and trust include access, ease of

navigating and using a website, security, multiple payment options, and competitive prices.

Credit Card fraud is a glooming problem in E-commerce. In the case of certain E-commerce companies, they record losses of billions of dollars annually. The condition is even more consequential for Small and Medium sized enterprises. Hence there is a need to detect and prevent possible credit card fraud. And this is the field open to research currently.

Security in E-commerce is a vast domain; hence we only focus on one aspect. We aim to detect and prevent credit card fraud. Also, a major threat to the security and reputation of a merchant is credit/debit card fraud.

## IV. PROPOSED SYSTEM

The proposed methodology for above mentioned problem is explained below:

### A. Data Collection

Collect transaction data, including user information, transaction history, device characteristics, and location.

### B. Data Preprocessing

Clean and standardize data, handling missing values and filtering out inconsistencies to ensure quality.

### C. Feature Extraction

Identify key features, like transaction amount, frequency, and device behavior, to track patterns.

Integrate DNS profiling and IP data to detect possible VPN or proxy usage.

### D. Anomaly Detection Rules

Define rules based on typical fraudulent behaviors, such as unusual transaction frequency or device mismatches.

### E. Flagging System for Suspicious Transactions

Implement checks that instantly flag anomalies (e.g., mismatched locations or rapid, repeated transactions).

Trigger alerts for any flagged activity and provide detailed transaction logs for review.

### F. Real-Time Monitoring and Alerts

Set up a real-time system to monitor active transactions and instantly notify for suspicious activity.

### G. Log Flagged Transactions to Refine the Detection Process.

### H. Continuous System Updates

Regularly update detection rules and protocols to adapt to new fraud techniques and technology changes.

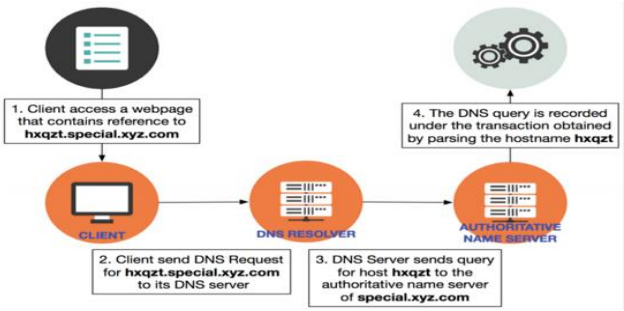
Ensure user compatibility and feedback integration to improve security and user experience.

A web page containing an asset (i.e., image, css, etc.) referenced with the unique hostname. A server-side or client-side scripting can generate the hostname. Client-side scripting is less secure, but we can use obfuscation techniques to hide the script and the hostname to hinder their tampering.

The final html tag on the webpage will look like this:

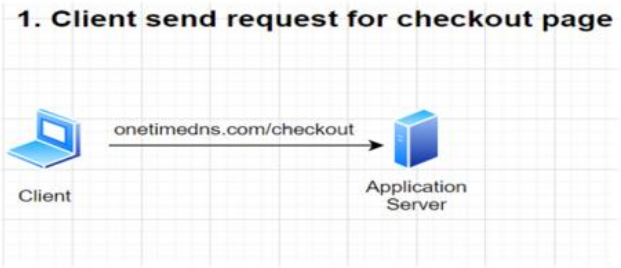
<a href='https://a1b2c3d4.subdom.mybiz.com/a.gif'>

A custom-made DNS authoritative name serv**er**. As every single transaction will generate a unique hostname, we need custom-made DNS authoritative name servers that will answer/respond to all hostname queries. These servers will answer all hostname queries that follow our format and encoding. Furthermore, they will also parse the hostname to recover the transaction ID and update our transaction database with the DNS query that it receives.

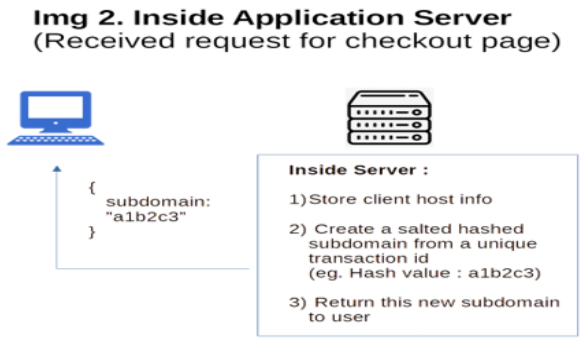



**[Fig.1: Design of Proposed System]**

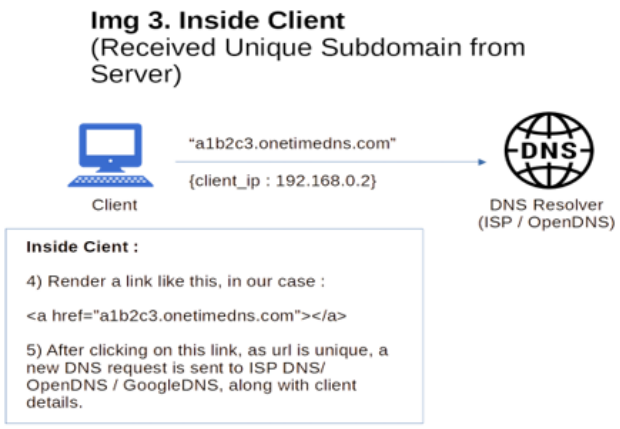
The above Figure 4.1 Shows the design diagram for using disposable domain name to get DNS query; by inserting a dynamically generated unique hostname on the E-commerce transaction webpage, a client will issue an identifiable DNS query to the customized authoritative DNS server maintained by the online Merchant [6]. In this way, the online Merchant can collect the DNS configuration of the client and match it with the client's corresponding transaction to verify the consistency of the client's IP address. Any discrepancy can reveal proxy usage, which fraudsters commonly used to spoof their true origins [5].



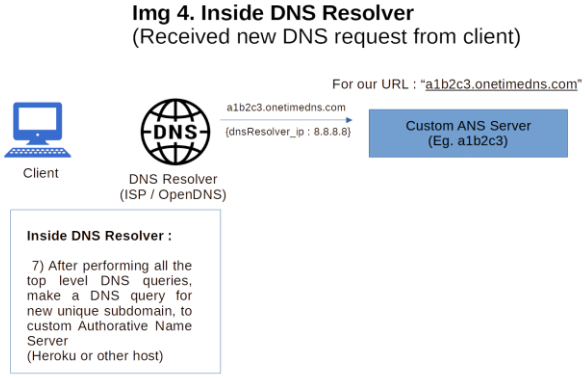

**[Fig.2: Client Server Request Connection]**



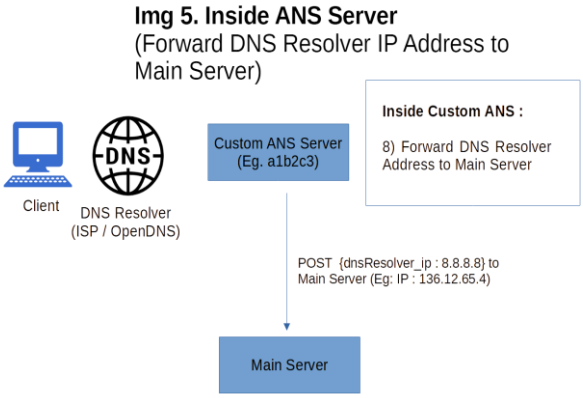

**[Fig.3: Application Server]**



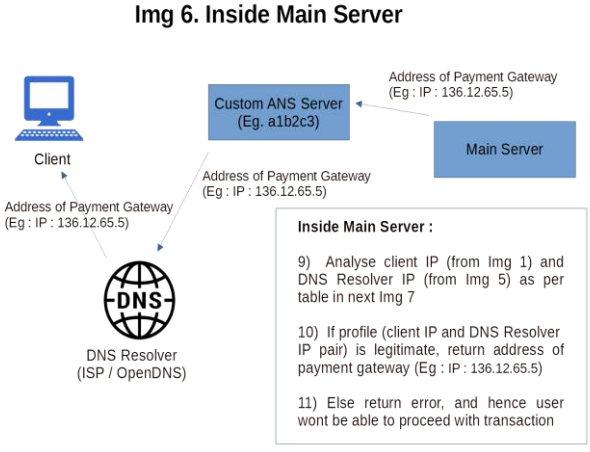

**[Fig.4: Inside Client]**



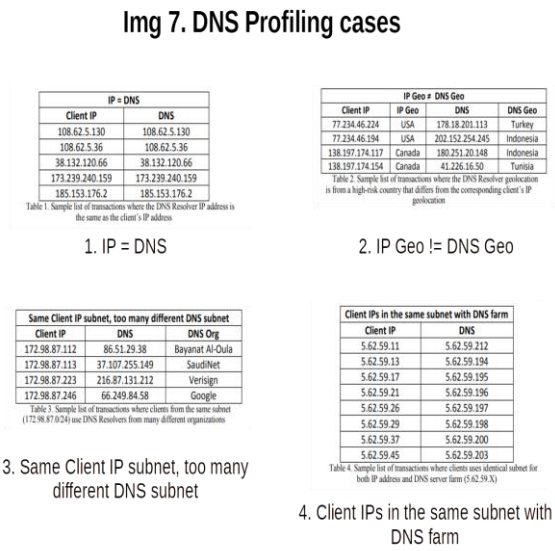

**[Fig.5: Inside DNS Server]**



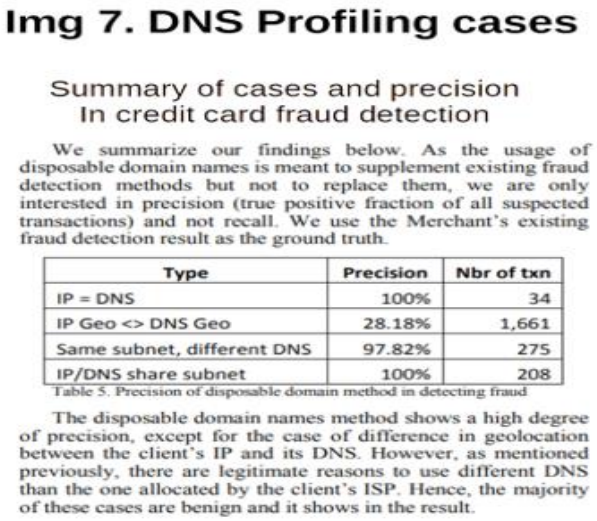

**[Fig.6: Inside ANS Server]**




**[Fig.7: Inside Main Server]**



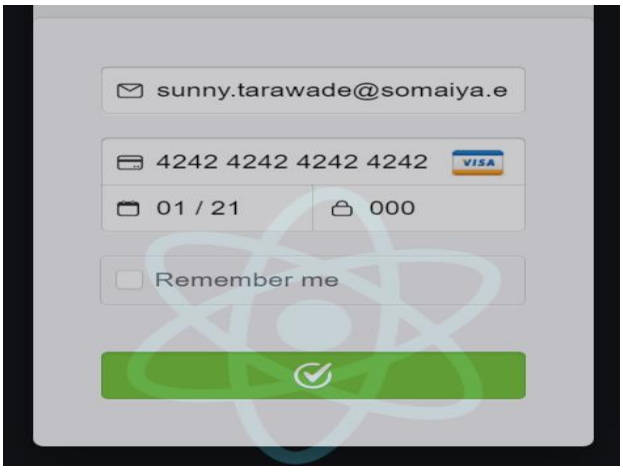

**[Fig.8: DNS Profiling Cases]**




**[Fig.9: DNS Profiling Cases]**

## V. SYSTEM IMPLEMENTATION

The system has been implemented and the system screenshot has been shown below.

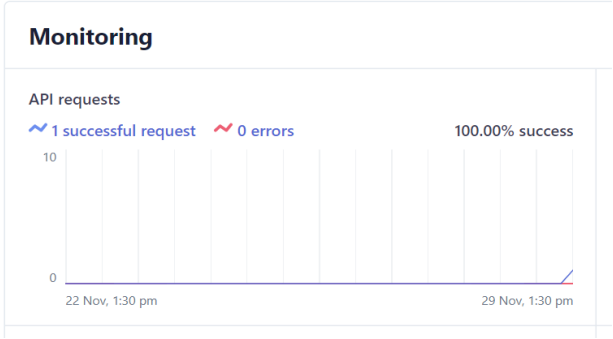



**[Fig.10: Make A Purchase]**

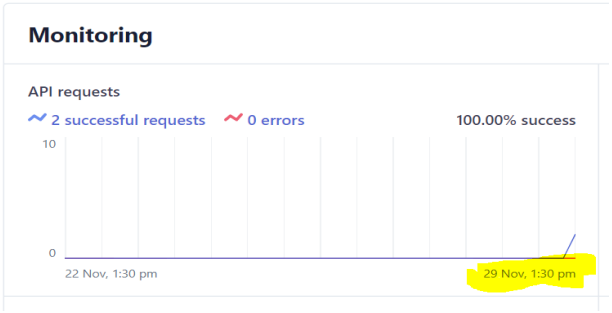
*Retrieval Number: 100.1/ijsce.F365614060124*
*DOI: 10.35940/ijsce.F3656.14051124*
*Journal Website: www.ijsce.org*



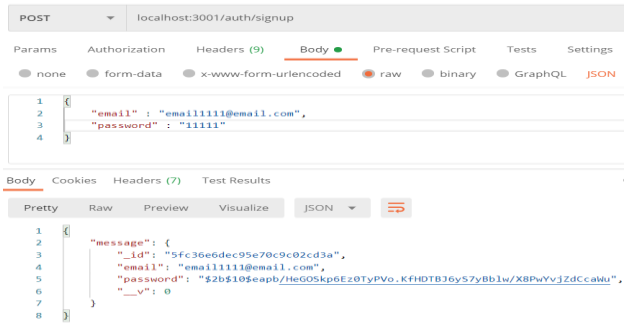
*Published By:*
*Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)*



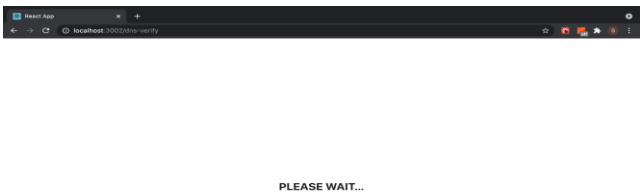

[Fig.11: Stripe Dashboard Before Payment]



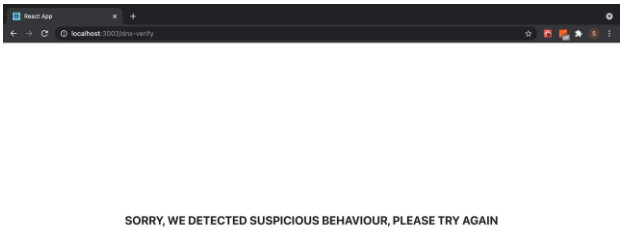

[Fig.12: Stripe Dashboard after Payment]




[Fig.13: POST req at auth/signup Success]




[Fig.14: Website Checking when a user enters website]




[Fig.15: When fraud is detected]

## VI. CONCLUSION

E-commerce has revolutionized global trade, offering businesses expanded reach and flexibility. However, it also presents significant challenges, particularly with credit card fraud, which causes substantial financial losses. Addressing this is crucial for maintaining trust in online platforms.

This study emphasizes the importance of advanced fraud detection methods. By employing DNS profiling with disposable domain names and custom DNS servers, the proposed system identifies inconsistencies in transaction data to prevent fraud in real time. Additionally, machine learning techniques, such as Logistic Regression, Decision Trees, and Hidden Markov Models, enhance detection by reducing false positives and increasing accuracy.

Integrating DNS profiling with machine learning offers a proactive solution to transaction validation, building trust and improving security. Future work should refine these models to keep pace with evolving fraud tactics, ensuring a safer e-commerce environment.

Future scope:

- Consider more scope and technique used by hackers to do credit card fraud and try to eliminate them using Machine Learning and Deep Learning.
- To also implement the technique which can very accurately detect fraud even if user is using VPN.
- To make our application more user friendly and very compatible with all the devices.
- To continually update our application with future upcoming modern technologies and methods

## DECLARATION STATEMENT

After aggregating input from all authors, I must verify the accuracy of the following information as the article's author.

- **Conflicts of Interest/ Competing Interests:** Based on my understanding, this article has no conflicts of interest.
- **Funding Support:** This article has not been sponsored or funded by any organization or agency. The independence of this research is a crucial factor in affirming its impartiality, as it has been conducted without any external sway.
- **Ethical Approval and Consent to Participate:** The data provided in this article is exempt from the requirement for ethical approval or participant consent.
- **Data Access Statement and Material Availability:** The adequate resources of this article are publicly accessible.
- **Authors Contributions:** The authorship of this article is contributed equally to all participating individuals.

## REFERENCES

1. T. Yorozu, M. Hirano, K. Oka and Y. Tagawa, "Electron Spectroscopy Studies on Magneto-Optical Media and Plastic Substrate Interface," in IEEE Translation Journal on Magnetics in Japan, vol. 2, no. 8, pp. 740-741, Aug. 1987, doi: https://doi.org/10.1109/TJMJ.1987.4549593
2. A. Susanto, P. Lestari, S. Hidayatuloh and A. Fitriyani, "Factors Affecting College Students' Trust in Online Shopping Transactions," 2019 7th International Conference on Cyber and IT Service Management (CITSM), Jakarta, Indonesia, 2019, pp. 1-5, doi: https://doi.org/10.1109/CITSM47753.2019.8965359.
3. S. Sanyala and M. W. Hisamb, "Factors Affecting Customer Satisfaction with Ecommerce Websites - An Omani Perspective," 2019 International Conference on Digitization (ICD),



Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Sharjah, United Arab Emirates, 2019, pp. 232-236, doi: https://doi.org/10.1109/ICD47981.2019.910578
4. N. Malini and M. Pushpa, "Analysis on credit card fraud identification techniques based on KNN and outlier detection," 2017 Third International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB), Chennai, India, 2017, pp. 255-258, doi: https://doi.org/10.1109/AEEICB.2017.7972424.
5. Imane Karkaba, EL Mehdi Adnani, Mohammed Errital, Deep Learning Detecting Fraud in Credit Card Transactions, Journal of Theoretical and Applied Information Technology, 15th May 2023. Vol.101. No 9, pp. 3557-3565, doi: https://doi.org/10.1109/SIEDS.2018.8374722.
6. R. Laurens, H. Rezaeighaleh, C. C. Zou and J. Jusak, "Using Disposable Domain Names to Detect Online Card Transaction Fraud," ICC 2019 - 2019 IEEE International Conference on Communications (ICC), Shanghai, China, 2019, pp. 1-7, doi: https://doi.org/10.1109/ICC.2019.8761144.
7. K. Shah, H. Sinha and P. Mishra, "Analysis of Cross-Platform Mobile App Development Tools," 2019 IEEE 5th International Conference for Convergence in Technology (I2CT), Bombay, India, 2019, pp. 1-7, doi: https://doi.org/10.1109/I2CT45611.2019.9033872
8. D. Fortunato and J. Bernardino, "Progressive web apps: An alternative to the native mobile Apps," 2018 13th Iberian Conference on Information Systems and Technologies (CISTI), Caceres, Spain, 2018, pp. 1-6, doi: https://doi.org/10.23919/CISTI.2018.8399228.
9. Ramakishore, S., & Karpagavalli, Dr. P. (2020). K-Nearest Neighbor Based Enhanced-CBIR System. In International Journal of Innovative Technology and Exploring Engineering (Vol. 9, Issue 4, pp. 550–554). Doi: https://doi.org/10.35940/ijitee.b7711.029420
10. Srinivas, B., & Rao, G. S. (2019). A Hybrid CNN-KNN Model for MRI brain Tumor Classification. In International Journal of Recent Technology and Engineering (IJRTE) (Vol. 8, Issue 2, pp. 5230–5235). Doi: https://doi.org/10.35940/ijrte.b1051.078219
11. Jain, N., & Kumar, R. (2022). A Review on Machine Learning & It's Algorithms. In International Journal of Soft Computing and Engineering (Vol. 12, Issue 5, pp. 1–5). Doi: https://doi.org/10.35940/ijsce.e3583.1112522
12. Assegie, T. A. (2021). K-Nearest Neighbor Based URL Identification Model for Phishing Attack Detection. In Indian Journal of Artificial Intelligence and Neural Networking (Vol. 1, Issue 2, pp. 18–21). Doi: https://doi.org/10.54105/ijainn.b1019.041221
13. M, N., Vidyashankara, & Kumar, G. H. (2020). Recognition of Leaves in Videos. In International Journal of Inventive Engineering and Sciences (Vol. 5, Issue 8, pp. 1–3). Doi: https://doi.org/10.35940/ijies.l0946.025820

## AUTHORS PROFILES

**Prof. Pradnya Patil**, is an Assistant Professor in the Computer Engineering Department at KJ Somaiya Institute of Technology, Mumbai. She specializes in the research and application of the Indian Knowledge System (IKS) in real-time environments, focusing on integrating ancient wisdom with modern technology. Pradnya has been recognized with the prestigious NPTEL Star Award by IIT Bombay, highlighting her contributions to the academic community. In addition to her academic pursuits, she is a certified yoga instructor and actively mentors students on various need-based social projects. She is a committed member of All World Gayatri Pariwar (AWGP) and holds professional memberships with esteemed organizations such as the Indian Society for Technical Education (ISTE), Mausam, and IEEE. Pradnya is also an Associate Chartered Engineer with the Institution of Engineers (India). Her research interests encompass a diverse range of fields, including Computational Modelling, Natural Language Processing (NLP), Sanskrit, Machine Translation, and Rainfall Prediction.

**Prof. Minal Sonkar**, is an Assistant Professor in the Computer Engineering Department at KJ Somaiya Institute of Technology, Mumbai. Her research area include Artificial Intelligence, Natural Language Processing etc.

**Prof. Pallavi Patil**, is an Assistant Professor in the Computer Engineering Department at KJ Somaiya Institute of Technology, Mumbai. Her research area include Artificial Intelligence, Security etc.

**Prof. Priyanka Deshmukh**, is an Assistant Professor in the Computer Engineering Department at KJ Somaiya Institute of Technology, Mumbai. Her research area include Artificial Intelligence, Machine Learning, Healthcare AI based projects etc.

**Prof. Trupti Patil**, is an Assistant Professor in the computer Science and Business Systems, Bharati Vidyapeeth (Deemed to be University), DET, Kharghar,Navi Mumbai, India. Her research area include Artificial Intelligence, work on geospatial images etc.