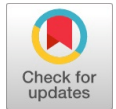


A Comprehensive Strategy for Detecting Credit Card Fraud in E-Commerce Utilizing DNS Authentication



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, particularly credit card fraud, remain significant, resulting in substantial losses for businesses, especially 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 being 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

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

E-commerce 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 once limited to a specific area. Region or country, until the “World Wide Web” was introduced in 1990 by Tim Berners-Lee, which gave the most significant breakthrough to the commerce business around the world, as now you can trade with the whole world from any corner of the world. Any business can expand its customer base to the entire global population.

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 generates huge revenue as it helps acquire customers and build brand value. Customers are no longer dependent solely on content or word-of-mouth before buying a product; they ensure that they read reviews about a product on all the platforms on which the product is listed.

According to recent analysis, 37 million social media visits resulted in approximately 529,000 orders. Out of all others, Facebook helps drive more traffic to the website, which leads to increased sales.

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. It eliminates many fixed costs associated with maintaining brick-and-mortar shops. This allows the companies to enjoy a much higher margin of profit.
- It provides quick delivery of goods with minimal effort on the part of the customer. 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.
- 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.

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

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license <http://creativecommons.org/licenses/by-nc-nd/4.0/>

B. Disadvantages of E-Commerce

- The start-up costs of the e-commerce portal are very high. The setup of the hardware and software, as well as the training costs 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 persists to this day.
- At times, e-commerce can feel impersonal. So, it lacks the warmth of an interpersonal relationship, which is essential for many brands and products. This lack of a personal touch can be a disadvantage for many types of services and products, such as interior design or the jewellery business.
- Security is another area of concern. Only recently have we witnessed numerous security breaches in which customer information was stolen. Credit card theft, identity theft, and other similar concerns continue to be significant concerns for customers.
- Additionally, there are fulfilment problems. Even after an order is placed, issues with shipping, delivery, and mix-ups can still occur. This leaves the customers unhappy and dissatisfied

II. LITERATURE SURVEY

Aries Susanto; Putri Lestari; Sarip Hidayatuloh; Aida Fitriyani [1]-: Trust is a belief that others will behave reliably way in a relationship. Trust is still considered a qualification of consumers in deciding purchases. This study employs a quantitative approach, combining the Technology Acceptance Model with several other variables based on consumer confidence in online transactions. The population in this study consisted of students from a government-owned university who had already engaged in online shopping. The distribution of questionnaires was conducted online using a multi-stage, purposeful random sampling technique. Simple random sampling is used for the first stage, and purposive sampling is employed for the second stage. Furthermore, the data analysis process uses the PLS-SEM approach using SmartPLS 3.0. Trust formation models that leverage the extension of multiple variables have proven influential in measuring trust in online shopping transactions. This research can serve as a consideration for formulators and policymakers in the online shopping business, as well as a benchmark for consumers, by examining the factors that influence 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. E-commerce 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. E-commerce offers several benefits to sellers compared to traditional retailing. Some key benefits include overcoming geographical limitations, lower costs, 24/7 availability of products, gaining new customers through better search engine visibility,

creating targeted information, enabling 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 standard payment method accepted both offline and online, allowing 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 can be argued that as global communication has improved, economic fraud has increased dramatically. 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 to reduce confusion and maintain order. For detecting fraudulent credit card transactions, various techniques are employed, including machine learning, genetic programming, fuzzy logic, and sequence alignment. These approaches have been demonstrated to reduce false alarm rates and increase 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 to non-linear data. 2. It is not capable of handling fraud detection at the time of transaction.
Decision Tree	This method can also handle non-linear data.	1. It involves a complex algorithm, and even a slight change in the data can disrupt the tree's structure. Choosing the splitting criteria is also a complex process. 2. It cannot detect fraud at the time of the transaction.
Hidden Markov Model.	This method is capable of detecting fraudulent activity in real-time during the transaction. The HMM-based models reduce the number of False Positive (FP) transactions predicted as fraud, even though they are genuine customers.	1. It cannot detect the fraud in the initial few transactions.
Support vector machine	This method is capable of detecting fraudulent activity in real-time during the transaction.	1. Sometimes it fails to detect fraud cases.
K-Nearest Neighbour Algorithm	There is no requirement for a predictive model before classification.	1. The accuracy of the method depends on the accuracy of the distance measurement. 2. It cannot detect the fraud at the time of the transaction.

III. PROBLEM STATEMENT

Security is a vast domain, but E-commerce platforms use trusted third-party payment gateways and authentication services. However, there is also a significant problem with online transactions, namely credit card fraud, which is a field of research in its own right. Credit Card fraud causes a loss of billions of dollars annually to businesses; hence, it is crucial to address this problem.

But there are specific 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, ensuring security, offering multiple payment options, and providing competitive prices.

Credit Card fraud is a looming 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. This field is currently open to research.

Security in E-commerce is a vast domain; hence, we focus on only one aspect. We aim to detect and prevent credit card fraud. Additionally, a significant threat to a merchant's security and reputation is credit or debit card fraud.

IV. PROPOSED SYSTEM

The proposed methodology for the problem mentioned above 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, such as transaction amount, frequency, and device behaviour, 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 and analysis.

F. Real-Time Monitoring and Alerts

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

G. Log Flagged Transactions to Refine the Detection Process.

H. Continuous System Updates

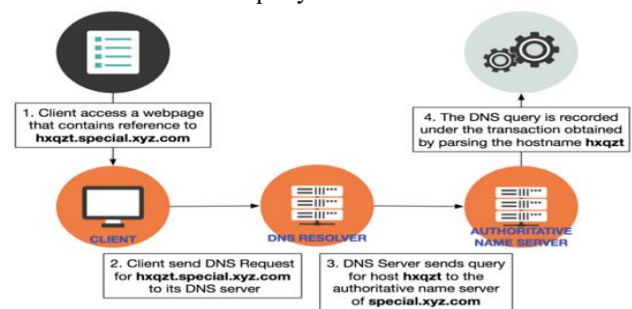
Regularly update detection rules and protocols to adapt to new fraud techniques and technology changes.

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

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

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

A custom-made DNS authoritative name server. 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.



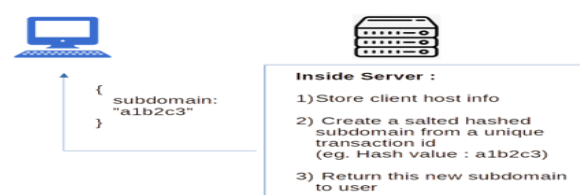
[Fig.1: Design of Proposed System]

The above Figure 4.1 shows the design diagram for using a disposable domain name to get a 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 use to spoof their true origins [5].



[Fig.2: Client Server Request Connection]

Img 2. Inside Application Server (Received request for checkout page)



[Fig.3: Application Server]

Img 3. Inside Client
(Received Unique Subdomain from Server)



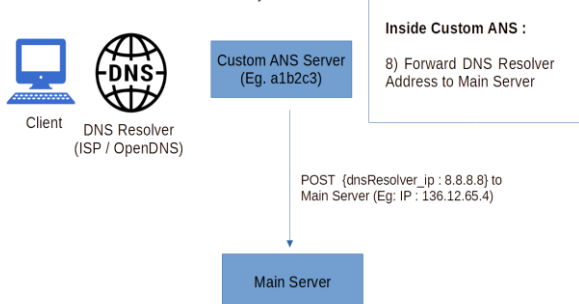
[Fig.4: Inside Client]

Img 4. Inside DNS Resolver
(Received new DNS request from client)



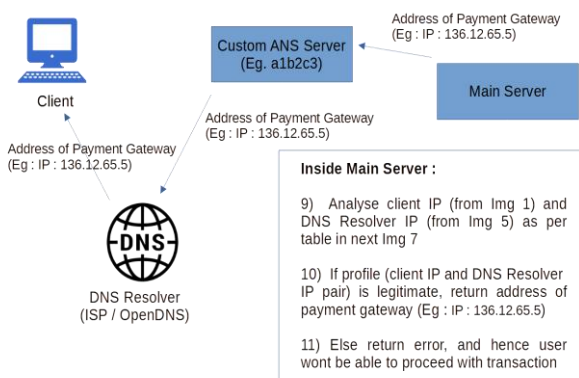
[Fig.5: Inside DNS Server]

Img 5. Inside ANS Server
(Forward DNS Resolver IP Address to Main Server)



[Fig.6: Inside ANS Server]

Img 6. Inside Main Server



[Fig.7: Inside Main Server]

Img 7. DNS Profiling cases

IP = DNS	
Client IP	DNS
108.62.5.130	108.62.5.130
108.62.5.36	108.62.5.36
38.132.120.66	38.132.120.66
173.239.240.159	173.239.240.159
185.153.176.2	185.153.176.2

Table 1. Sample list of transactions where the DNS Resolver IP address is the same as the client's IP address

IP Geo != DNS Geo			
Client IP	IP Geo	DNS	DNS Geo
77.234.46.124	USA	178.18.201.113	Turkey
77.234.46.194	USA	202.152.254.245	Indonesia
138.197.174.117	Canada	180.251.20.148	Indonesia
138.197.174.154	Canada	41.226.16.50	Tunisia

Table 2. Sample list of transactions where the DNS Resolver geolocation is from a high-risk country that differs from the corresponding client's IP geolocation

1. IP = DNS

2. IP Geo != DNS Geo

Same Client IP subnet, too many different DNS subnet		
Client IP	DNS	DNS Org
172.98.87.112	86.51.29.38	Baymont Al-Oula
172.98.87.113	37.107.255.149	SaudiNet
172.98.87.223	216.87.131.212	Verisign
172.98.87.246	66.249.84.58	Google

Table 3. Sample list of transactions where clients from the same subnet (172.98.87.9/24) use DNS Resolvers from many different organizations

Client IPs in the same subnet with DNS farm	
Client IP	DNS
5.62.59.11	5.62.59.212
5.62.59.13	5.62.59.194
5.62.59.17	5.62.59.195
5.62.59.21	5.62.59.196
5.62.59.26	5.62.59.197
5.62.59.29	5.62.59.198
5.62.59.37	5.62.59.200
5.62.59.45	5.62.59.203

Table 4. Sample list of transactions where clients use identical subnet for both IP address and DNS server farm (5.62.59.X)

3. Same Client IP subnet, too many different DNS subnet

4. Client IPs in the same subnet with DNS farm

[Fig.8: DNS Profiling Cases]

Img 7. DNS Profiling cases

Summary of cases and precision In credit card fraud detection

We summarize our findings below. As the usage of disposable domain names is meant to supplement existing fraud detection methods but not to replace them, we are only interested in precision (true positive fraction of all suspected transactions) and not recall. We use the Merchant's existing fraud detection result as the ground truth.

Type	Precision	Nbr of txn
IP = DNS	100%	34
IP Geo <=> DNS Geo	28.18%	1,661
Same subnet, different DNS	97.82%	275
IP/DNS share subnet	100%	208

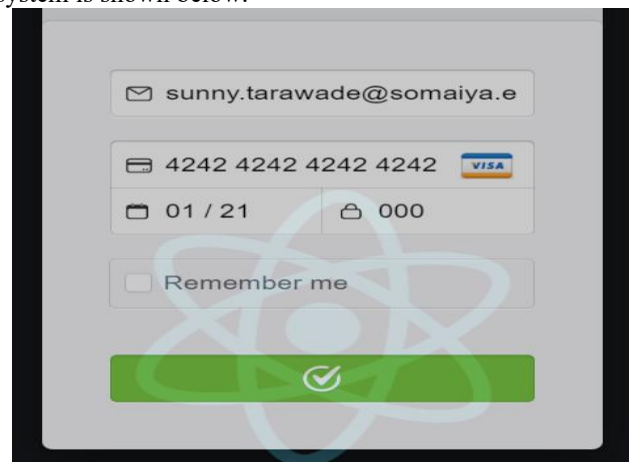
Table 5. Precision of disposable domain method in detecting fraud

The disposable domain names method shows a high degree of precision, except for the case of difference in geolocation between the client's IP and its DNS. However, as mentioned previously, there are legitimate reasons to use different DNS than the one allocated by the client's ISP. Hence, the majority of these cases are benign and it shows in the result.

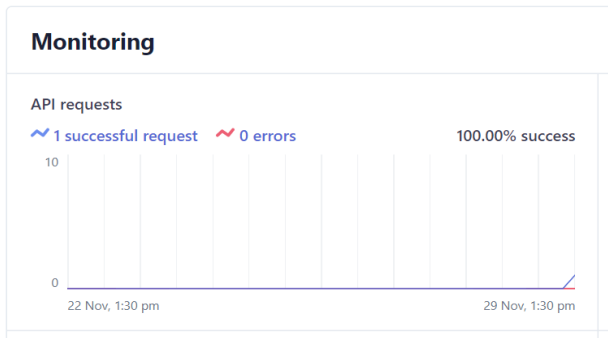
[Fig.9: DNS Profiling Cases]

V. SYSTEM IMPLEMENTATION

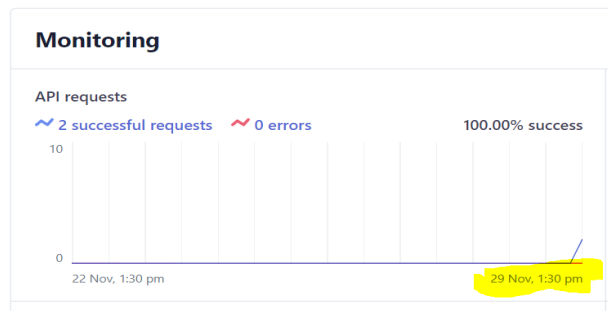
The system has been implemented, and a screenshot of the system is shown below.



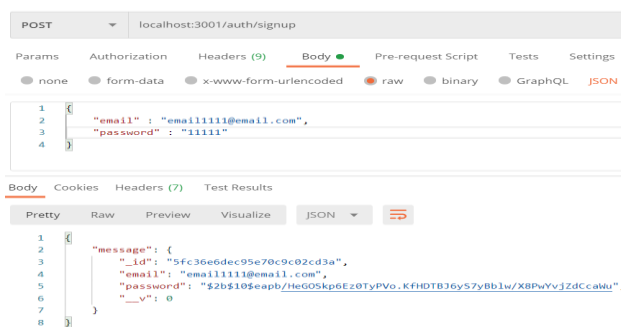
[Fig.10: Make A Purchase]



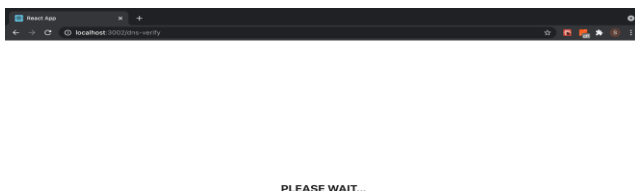
[Fig.11: Stripe Dashboard Before Payment]



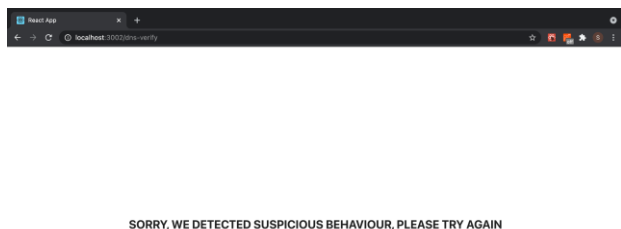
[Fig.12: Stripe Dashboard after Payment]



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



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



[Fig.15: When fraud is detected]

VI. CONCLUSION

E-commerce has revolutionised global trade, providing businesses with an expanded reach and increased flexibility. However, it also presents significant challenges, particularly in the form of 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 in real-time, thereby preventing fraud. 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 provides a proactive solution for transaction validation, fosters trust, and enhances 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 techniques used by hackers to commit 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 the user is using a VPN.
- To make our application more user-friendly and very compatible with all 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 does not have any 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 was conducted without any external influence.
- 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.
- Author's Contributions:** The authorship of this article is contributed equally to all participating individuals.

REFERENCES

- T. Yoroazu, M. Hirano, K. Oka and Y. Tagawa, "Electron Spectroscopy Studies on Magneto-Optical Media and Plastic Substrate Interface," in IEEE Translation Journal on Magnetism in Japan, vol. 2, no. 8, pp. 740-741, Aug. 1987, doi: <https://doi.org/10.1109/TJMJ.1987.4549593>
- 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), 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. Imame 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>.

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 recognised with the prestigious NPTEL Star Award by IIT Bombay, which highlights her contributions to the academic community. In addition to her educational pursuits, she is a certified yoga instructor and actively mentors students on various need-based social projects. She is a committed member of the All World Gayatri Pariwar (AWGP) and holds professional memberships with esteemed organisations, including 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 areas include Artificial Intelligence and Natural Language Processing, among others.



Prof. Pallavi Patil is an Assistant Professor in the Computer Engineering Department at KJ Somaiya Institute of Technology, Mumbai. Her research areas include Artificial Intelligence, Security, and other related fields.



Prof. Priyanka Deshmukh is an Assistant Professor in the Computer Engineering Department at KJ Somaiya Institute of Technology, Mumbai. Her research area encompasses Artificial Intelligence, Machine Learning, and AI-based healthcare projects.



Prof. Trupti Patil is an Assistant Professor in Computer Science and Business Systems at Bharati Vidyapeeth (Deemed to be University), DET, Kharghar, Navi Mumbai, India. Her research area includes Artificial Intelligence, with a focus on geospatial images, among other topics.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of the Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)/ journal and/or the editor(s). The Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP) and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.