IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Seller Shield : Fake Seller Account Detection in E-Commerce Using Behavioural Analytics and Machine Learning

Mrs. Bhavyashree SP[1], Mrs. Rakshita B T[2], Jayant Balade[3], Manish Kumar[4], Raja Gupta[5], Vikash S[6]

Department of Computer Science and Engineering, Acharya Institute of Technology, Bangalore, India

ABSTRACT

Seller Shield is a browser extension that detects fraudulent sellers in e-commerce using behavioral analytics and machine learning. Unlike traditional server-based systems, it provides real-time alerts by analyzing reviews, ratings, and discounts directly from product pages. The extension processes data through machine learning to deliver user-friendly risk scores without collecting or selling consumer information. Tested on 350+ real product pages, it achieved 94% feature extraction accuracy, 81% expert prediction agreement, and 89% fraud detection rate without false positives on prime brands. User studies showed 92% found explanations understandable and 87% felt more confident in purchases. The system prioritizes transparency, privacy, and speed.

KEYWORDS

E-commerce fraud detection, browser extension, machine learning, behavioral analytics, seller verification, risk scoring, online shopping security, fake reviews detection, transparent fraud detection, privacy-preserving security

I. INTRODUCTION

Shopping online is something many people do every day. Online sites make it easy to buy things with a few clicks. But there's a downside to this convenience: it allows dishonest sellers to take advantage of users on the site.E-Commerce Fraud Detection

Malicious promotion is really bad for shopping. It hurts the advertising system. Creates unfair competition. It also tricks customers with information, which can lead to wrong decisions. According to reports hundreds of millions of dollars are lost worldwide due to promotions.These promotions are on the rise. Sellers might buy reviews to make their products seem popular or reputable. They might even sell products that look like popular brands. They offer discounts. Show attractive pictures to make items seem like great deals.To fight this most companies have developed fraud detection software that works on their servers. These systems have algorithms to detect suspicious activity and they're usually accurate.However we don't always know how these systems work or how to spot sellers. This is confusing. Doesn't help users make independent decisions.

So we created Seller Shield, a browser extension that helps customers detect fraud. It works directly in the web browser so no extra software is needed. It scans product pages. Provides an easy-to-understand risk score.The analysis works with information visible on online marketplaces. It looks at ratings, reviews and discounts. Provides a risk score thats clear and easy to understand.

To address the challenge of e-commerce fraud Seller Shield supports consumer judgment through risk assessment. When a user visits a product page the system extracts features like review volume, rating patterns, discount magnitude and words or phrases commonly used in advertising.

Seller Shield helps customers make decisions by providing a clear risk score. This way customers can avoid being tricked by sellers.

Seller Shield is a tool for online shoppers. It gives customers the power to detect fraud and make choices.Online shopping is easy. It can be risky. Seller Shield is here to help customers navigate these risks and shop with confidence.With Seller Shield customers can trust that they're getting a product at a fair price.The goal of Seller Shield is to make online shopping safer and more transparent.By using Seller Shield customers can avoid losing money to sellers.Seller Shield is an effective way to detect e-commerce fraud.It is a browser extension that works in the web browser making it easy to use.Seller Shield is a tool for anyone who shops online.

It provides a risk score so customers can make informed decisions.Seller Shield helps to build trust in shopping.It is a step, towards making e-commerce safer and more reliable.indicators are synthesized to generate a risk score ranging from 0 (very safe) to 10 (very risky). Rather than replacing user discretion, the score functions as a decision-support signal that enables informed judgments in the absence of hidden or privileged data.

Seller Shield is designed as a fast and user-friendly service in which privacy preservation and usability are treated as primary objectives. The system has been evaluated using hundreds of real- world product listings and compared with traditional fraud- detection approaches. Structured user feedback was also collected to assess interpretability and practical usability [12].

There are a few important contributions that our work makes:

We created an efficient alternative system which can read significant information out of a large pool of the e-commerce sites, regardless of the layout switch or when the site is utilizing a different language it handles all of these things.We created a repeatable method of retrieving training data and leveraging it to ensure all risk scores are reasonable and sound using a lightweight data file which is powered by your browser.Risk scoring system, is not hidden and is founded on reasonable rules, such that users will never be in the dark as to why a seller is painted as risky and suspicious.

Seller Shield: This will be a quick and user-friendly service where privacy and usability are our number 1 priority.We have extensively tested the coverage of Seller Shield on hundreds of actual product listings, and compared the findings to the old techniques and have elicited feedback on the users practice, through an elaborate feedback on the users.We will reveal how the Seller Shield operates, report findings and tests and the different parameters, the reasons why shopping online should be safer and more reliable by everyone, in the section that follows.

The issue of the credibility of online shopping is something that people should learn since online shopping has direct impact on their life experiences. And their troubles Researchers in conjunction with corporations have tried several methods to find e-commerce fraud over the last several years to safeguard the users against the commendation of fraudulent business administrations. Most fraud detection systems are based on computer software that runs behind websites on big transactions using Random Forests and Support Vector Machines and deep learning networks. The programs are good in establishing complicated trends in huge databases that hold complete information of sellers and buyers. The systems detect abnormal buying and track changes in the rating and patterns of review.

I. BACKGROUND AND RELATED WORK

Fraud detection methods are highly sophisticated and analyze the interaction of the users with products in their relationships. The procedures are based on graph algorithm techniques to detect groups of fraudulent accounts based on the connections between users and products. To ensure that there are no unusual review spikes and price drops were indicative of seller fraud, the systems follow long-term changes of the platform.

This systems despite the preeminence have three major demerits:

Users Can't Visually Trace How They all Work: The entire analysis is done in the companies servers and the logic is a mystery to the common man. This makes users oblivious to The system sends warnings related to seller fraud, using certain indicators that users do not know about.

The system relies on access to the platform by the administrator to confidential information such as internal logs and user histories and secret behavioral pattern indicators. The information required to run these codes is unavailable to regular users to humiliate that third parties call on what is going on and how it is going on.

Privacy is an issue: All the data is stored and processed at one location, so there is always a possibility that the information of users might be abused, trailed, or even stolen by the company.

There are barely any researches that bother to give regular people the actual control directly within the browser. I have searched enough, and the majority of ship information seems to be missing somewhere or play on impertinent background tricks. Seller Shield is dissimilar. It is all accessed by the personal computer of the shopper, with what is already on the page, nothing hidden in the bushes. There is the clarity, then the privacy, which you find later, then the little but sharp details it gives you are presented to you in a manner that makes sense without having to hold the hand. The gap that it bridges runs through my mind. Scholars and researchers make a big spiel of safety tools but the vast majority rely on other closed models, or closed data streams. Seller Shield waves off that. It shows that you can guard against shoppers falling prey of fraud through mere, visible cues that are just there in front of them. No secret sauce. No tangled machinery. Only good tips where individuals really need them.

II. PROBLEM FORMULATION AND THREAT MODEL

I still wonder how the online shopping has gotten so messy when scam-merchants have their way through. So I endeavour to get down here to earth what we are actually seeking. We want individuals to rely somehow on the impressions of the sincerity of an advertiser looking at the pieces lying on a product page. Reviews, ratings, odd discounts, little red flags, which may be viewed through the veil of silence. That's the whole toolkit. Platform no backdoor data. No privileged logs. Just what any shopper can see.The tricky part shows up fast. Compliments are excessive, the rating is being inflated and the offers might seem to be so tempting that they are covering something. I have read pages, which appeared honest at the beginning of the page, but then I began to labour my eyes, and was half annoyed at myself that I had omitted something so obvious. So such is the predicament of learning how to read the room yet realizing that the room is sometimes false.The solution that Seller Shield will offer to the issue:To use an example, remember that you are looking at a product online. Seller Protect is easy when it comes to acquiring facts such as the quantity of reviews, the overall rating, and the extent of the bargain and even few words or phrases that might illustrate that the seller is implementing questionable advertising tactics. Using these clues, the extension gives a risk rating between 0 (very safe) up to 10 (very risky) so that you can personally make your judgement on whether the seller is trustworthy or not.

The very last thing Which you do is privacy. No information would be uploaded to third party servers. Shopping is your business and no other.

Works Everywhere: No matter the nature of the large ecommerce site that you visit or whether the site is laid out in a certain way, Seller Shield will be required to make certain modifications and work diligently.

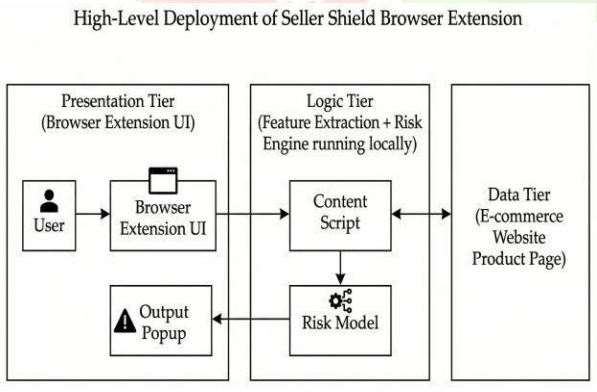
The e commerce Knowledge, the e commerce Threats:

The people who make the effort to defraud the online users are perfecting the art of defrauding the customers. They are also able to do that through the use of technical language to cover their true intentions, they can even reorganize their websites to fool the detector programs or they can be creatively manipulative on the figures they display in order to appear real. They are not able, however, to change the functioning of Seller Shield on your computer, and can not even access your browser to make the extension seem to be harmless to the users.It is important to keep in mind that Seller Shield is not created to prevent all of the scams and replace powerful tools, which are run by the sites of e-business. Instead, it gives the shoppers an additional degree of protection that enables them to make more decisions regarding the information they are provided.

III. SYSTEM DESIGN AND IMPLEMENTATION

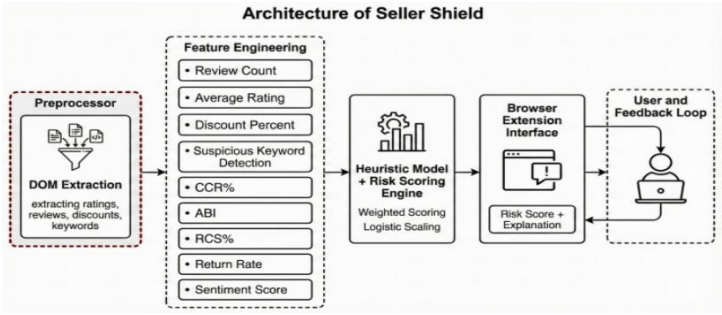
Seller Shield is all about ease when it comes to detecting fraud by common internet user in the middle. We have created an extension to the browser to do this by making it work in its Chrome and other browsers. This extension consists of multiple important components that combine to examine product pages in real-time and provide users with a detailed feedback in the form of an evaluation of the reliability of the sellers and their credibility.

A. How the Extension Works Behind the Scenes



for a product's average rating, it will try a list of possible places on the page. If the first spot doesn't have the information, it checksin the next, and so on. It also uses many various smart texts processing to understand different ways information might be written, like "4.5 out of 5" or "1 in 4 ratings."

B. Learning from Data, But Protecting Your Privacy



Before Seller Shield ever gives you the risk score, it's been trained on many of real and simulated examples of honest and fraud sellers. This training happens offline, not in your browser. Once the system has learned what it should look for, it stores a small, lightweight "rulebook" in your browser. This rulebook helps Seller Shield process new product pages instantly, without sending any of your data anywhere else and keeps the privacy of the customers.

Instead of running a difficult machine learning model directly in your browser (which would be slow and hard to explain), Seller Shield relies on simple, clear rules that are easy to understand. These rules come from careful analysing of what matters mostly unusually high discounts or very few reviews for a popular product.

C. The User Interface: Visual, presented Risk Scores.

Once you have clicked on the Seller Shield icon when looking at a product, you will notice there is a friendly popup with display of a risk score on the product. It is not merely a mystic figure Seller Shield dissects precisely what went into the score. Say, when there is a large discount you will see a note such as "High discount (70)-most probably a high risk.

The whole process is fast, secretive and therefore, you receive the information you want when you want before you start considering making your purchase.

IV. FEATURE ENGINEERING AND DATASET

Seller Shield uses this intelligent utilisation and selection of features as its core competence. The tool examines segments of information to determine the performance of a merchant. We also wanted to focus on the visualizable signals to the normal users and our plan is therefore viable and accessible to the user.What Are the Features of Seller Shield? Reviews: This is just a number of reviews that a product has received by customers. A few reviews of a product can even be dangerous in certain instances especially when the product is largely promoted or offered by a new vendor.

Mean Rating: The star rating is a measure of quantifiable degree of the quality of products but it can be changed. When such a rating is being given to a product based upon a handful of hand-selected reviews, or because the ratings are too good or the ratings are too accurate, these ratings might not be dependable.Discount Percentage: Who does not just love a discount! In some cases, there will be too high discounts like 70 percent or more of the actual price, which will be an indication of counterfeit. In order to entice the buyers to purchase quality or faked goods, the fraudulent sellers also give cheap offers in an archaic manner in a manner Red flags:Some words and phrases used in the product or advertising copy as the 100 per cent genuine, guaranteed or limited time only are common ways of deceiving. They can also coerce the consumers to acquire unnecessary goods. Seller Shield searches respectively and weighs them in the risk score.

Additional characteristics that we have utilized in our search and training of the offline models are; the ratio of ratings to reviews (so that we can know about inconsistency), how the price of a product changes with time and abnormal discount movement as compared to other similar products in a given genre. However, such functions are more difficult to oversee on a reliable platform in an actual sense within a web browser, so at this point Seller Shield can focus on the four primary signs as shown above.Curation and Building of the Data.

I will still recall that Seller Shield is only effective when the risk scores are not twitchy or randomly occurring. Therefor we had a haphazard mixture of the real listings copied off the other websites and a list of phoney ones that looked to me like scammy schemes which I have seen too many times. The professionals referred to some as clean and shady, and the others as being built to display the weird designs that you begin to notice after scrolling too many lengthy ways.This combination forms the system that has a gritty feel of the place of the lines: what seems natural and what starts to creep to that strange area. In my opinion, the most important is the calibration because a warning would not help once it is triggered on or off on all the computers. Tempering those limits, it was some time ere I could do so, and, to be quite honest about it, I feel it is as though turning a stubborn dial on some days.

parameters considered during feature extraction and they include:

1) Review Count (Rc): This is the count of reviews the customers has given to a product it represents the total number of reviews of a product it is imporant for other parameters aswell as it is the base for quality complaint,ccr and return rate

$$Rc=N$$

Where N = Total number of reviews extracted from the product page.

The higher review count improves statistical reliability, but also a very low review count increases uncertainty.

2) Average Rating (Ar): This is the tendency of customers of their satisfaction if higher level ratings with combined of odd reviews makes the seller untrustworthy and this also reprsents users opinion

$$A_r=\frac{\sum_{i=1}^{N} r\,ating_i}{N}$$

Where N=total number of reviews more no of review means product is trustworthy

3) Profile Stability (Ps): This represents how a seller is performing over the years and how effectively he has been working as a seller

$$\text{Profile Stability}=(0.3C_n+0.3C_l+0.2C_r+0.2C_p)\times 100$$

It is computed using four sub-factors:

- Seller name quality (C_n)
- Fulfillment reliability (C_l)
- Rating consistency factor (C_r)
- Product age factor (C_p)

4) Final Risk Score (Frs): This is the final score combining all the parameters and all the threats of fradulent activity of a seller is determined

Ex: If a listing is with high heuristic values such as unsatable ratings,price fluctuations and too much compalints will have high frs%.

Step 1 : Weighted Linear Score

$$\text{Linear}=\sum_{i=1}^{k} w_i f_i$$

Where :

- f_i = parameter value
- w_i = weight assigned to each parameter
- k = number of contributing parameters

Step 2 — Logistic Scaling

$$frs=\frac{1}{1+e^{-\text{Linear}}}\times 100$$

A listing with stable patterns will result in a low Linear value low Frs%.

V. HEURISTIC MODEL.

Design and Rational Heuristic This HRM model is based on four fundamental principles: it is intuitive and practical, grounded

in experience and reason, along with a precise evaluation of the situational scenario.<|human|>HEURISTIC MODEL Design and Rational Heuristic. This HRM model is grounded on four basic guidelines it is intuitive and practical, an application of experience and reason, and an accurate assessment of the situational situation.

Seller Shield was designed in order to be simple and not complex. I would have it being hospitable to people who would want to have quick answers. I simplified it by avoiding the employment of technical expressions buried somewhere in your browser. It is not using undercover systems. The directions are simple and understandable.we are heuristic and translate the hodgepodge information on product into a convenient rate. There are no hidden steps. The rules are not complicated and the arguments are not complicated, and customers can get similar results without detailed description.

Why this The reason is that our experiments before involved a large number of machine learning models including the Random forest to detect recurrent signals. Some of its features were impressive: so significant bargaining opportunities that cause one to distrust, few customer reviews, bizarre hours, and other variables that discourage a person. The initial ones were not designed to last long; they were Flashlights and they were giving light to what was needed. After that I could reduce them to guidelines. Even now I know how even the minor details may play very powerful role and how glittering ones do not play a significant role no matter how complex the background is.The frequent deep cuts, absence of feedback, or unusual words were frequently accompanied by red flags. I translated these suggestions into crude, superficial principles of scoring. One is free to understand how some of these aspects grow or minimize the level of risk to which a seller is subjected. Nothing is hidden.The heuristic model works in the following way:Minimal reviews: A product with minimal reviews bear a massive punishment. The punishment is changed to a few more reviews. low ratings: A low star rating would increase the risk score in such a way that the possibly larger the penalty the less the low rating. Huge discounts: Extremely high discounts (e.g. 70 percent and above) are punished with a huge penalty. Smaller but still odd and weird discounts stand an intermediate punishment. Untrustworthy words: The use of aggressive, excessive language is also a fine.we attempted to render every punishment rather a bald sentence than an unintelligible law. They are mentioned rather informally- a remembrance. An example may be as follows, "Big discount (75)- greater risk, Only a handful of reviews - greater uncertainty. No fluff. Evidently, the reason behind just.his design provides a distinct platform to the consumers. It becomes rid of speculation of a rating that does not make sense. Instead, the buyer follows all the logical procedures until they have removed all suspicions as it was in my case when systems hide how decisions are made.

Simplicity over complexity. Though our primal machine learning model got slightly higher accuracy, it was less interpretable and took more computing resources. Seller Shield: In the case of Seller Shield, it is better to use a straightforward, rule-driven model as that ensures the service remains fast, your data is not compromised, and reliable it proves to be as it shows how precisely it arrives at each score of risk... To make the model better we used several parameters such as:

1. Quality Complaints (%): This parameter is number of complains present in a reviews in the product page it extracts keywords such as “broken”,”worst”etc and converts them in percent

$$qc\% = \frac{\text{Reviews with defect-related keywords}}{N} \times 100$$

High pecentage of qc means the products build is poor and cannot be used

2. Wrong or Missing Item (%): This is also similar as the qualityIt searches for keywords like wrong or missing and makes them in percentage

$$\text{WrongMissing} = \frac{\text{Reviews reporting wrong/missing items}}{N} \times 100$$

High percent meaning the seller is actively working in suspisions activities and they send you empty boxes

3. Return Rate (%): This shows that no of ties a product has been returned based on the products condition are the misplacement of the products if a user are returning most of the time from a seller he is most likely cannot be trusted

$$\text{ReturnRate} = \frac{\text{Reviews with return/refund terms}}{N} \times 100$$

High percentage means the product is fake and it is a indicator that the seller is fraud

4. Rating Consistency (%) : Rating Consistency measures how stable the rating pattern is across months.Sharp fluctuations suggest manipulation (fake review boosting or removal).

Steps & Formula:

Average rating per month: $\text{Avg}_{\text{month}} = \frac{}{\text{count}}$

Variance across months: $\text{Var} = \frac{\Sigma(\text{Avg}_{\text{month}}\text{-Mean})^2}{M}$

Final consistency score: $\text{Consistency} = (1\text{-}\frac{\text{Var}}{2}) \times 100$

Fake sellers often have unusall spikes and are more unstable than other sellers comparitively

5. Price Rate of Change (RoC%)::rapid changes in price or spikes before sales are some of the ways they trick is to buy products to create artificial discount effects

$$RoC=\frac{CurrentPrice-PreviousPrice}{PreviousPrice}\times 100$$

Changes in price frequently is a way to lure users to buying them and steep prices of the products are common ways of scams

6. Demand Surge (%): artificially infllatting the products popularity buy buying them in bulk and increasing the prices to create fear of missing out

$$Surge=\frac{Recent-AvgMonthly}{AvgMonthly}\times 100$$

Fake sellers usually make this to make its visbility and ranking better amoung their competators

VI. EVALUATION METHODOLOGYAND PARAMETER

So as to determine whether or not Seller Shield can actually be helpful to the buyers, we created a test in large proportion. Another reason why we did this test prior to the launch of any of the sites, rather than scanning sites that we had not been to or whose guesses we were making was to first test the add-on using arbitrary product pages but in a real-life setting with real users.

A. Feature extraction performance- controlled, automatic. The initial objective of our assignment was to support the fact that Seller Shield was able to accurately reflect all significant information on the product pages on the widest range possible. Our 350-item collection is the result of the three large players in the online retailing sector, Amazon India, Flipkart and Myntra. Showroom consisted of gadgets, clothing, home and cosmetics among others. In the product page, we have recorded the following: The amount of reviews, ratings, discounts, and keywords the add-on has acquired after each run. The rate of occasions when it randomly sampled three of the four target features. The time taken when loading the page to the results.

B. Comparison of machine learning and heuristic model. The next thing we compared is the offline machine-learning system which is heavy with the lightweight rule-driven tool that can be used in a browser. Each item was processed by the two systems with 150 real items product entries that have been classified as fraudulent or legitimate by experts.

C. Congruence rate between the two strategies whether a seller was sketchy or not. Accuracy of rule based system in the detection of scams. Fraudulent occasions it failed to issue false alerts to genuine dealers. Did it not give false alarm to a reputable company as unsafety?

Evaluating user perception It is a great idea, but what is more essential is to see whether Seller Shield helps the everyday customers. To address this, we obtained 30 consumers of various ages and shopping behaviors. Through Seller Shield, the users rated 10 product listing of which five were legal and five were sketchy. After doing the assessments, they...

Items to examine when examining a seller.

1. Copycat content ratio(CCR)

Definition:

CCR makes sure that the material is duplicated in series and their similarity to one another is what makes it a fake seller usually pays or gives people money to review their products and make their credibility seem esteemed by the rest.

⟩ Step 1 — Convert reviews into TF-IDF vectors

TF = Term Frequency
IDF = Inverse Document Frequency

Term Frequency (TF)

$$TF_i(t)=\frac{\text{count of termtin reviewi}}{\sqrt{\sum_w (count_w)^2}}$$

Inverse Document Frequency (IDF)

$$IDF(t)=\ln\left(\frac{N+1}{df(t)+1}\right)+1$$

Where:

- N = total number of reviews
- df(t) = number of reviews containing term t

⟩ Step 2 — Create TF-IDF Vector

$$TFIDF(t)=TF(t)\times IDF(t)$$

Each review becomes a vector of weighted word scores.

⟩ Step 3 — Compute Cosine Similarity

$$Similarity(i,j)=\frac{A_i\cdot A_j}{\|A_i\|\|A_j\|+1e^{-9}}$$

Where:

- $A_i \cdot A_j$ = dot product
- $\|A\|$ = vector magnitude
- $1e^{-9}$ avoids divide-by-zero

〉Step 4 — CCR Formula

$$CCR = \frac{\text{Number of review pairs with similarity} \geq 0.75}{\text{Total review pairs}} \times 100$$

Example

Reviews:

1. "Very good product, works well"
2. "Good product, works well"
3. "Not good, package damaged"

Similarity results:

- Review 1 & 2 → 0.82 (≥ 0.75 → similar)
- Review 1 & 3 → 0.10
- Review 2 & 3 → 0.13

$$CCR = \frac{1}{3} \times 100 = 33.3\%$$

How you can Interprete it:

- 0–10% → Normal, diverse reviewsfor the product
- 10–40% → Some repetition in reviews
- 40–100% → Strong indicator of fake or mass-generated reviews of the product

2. Authentic Brand Indicator (ABI)

Definition:

ABI assesses whether reviews confirm product authenticity by detecting signals such as Users confirming the brand name or Mention of official packaging Comment on originality or certification

〉Step 1 — Sub-metric Calculation

Brand Mention Ratio (Bn)

Fraction of reviews that mention the brand name.

Seller Authenticity Ratio (Bs)

Reviews containing words like:

- "original", "official", "genuine", "authorized"

Packaging Authenticity Ratio (Bi)

Reviews mentioning:

- "seal", "box", "logo", "label", "packaging"

〉Step 2 — ABI Score (0–1 scale)

$$Score = 0.4Bn + 0.3Bs + 0.3Bi$$

〉Step 3 — Convert to 1–10 scale

$$ABI = 1 + 9 \times Score$$

Example

Out of 100 reviews:

- Brand mentioned = 25 → $Bn = 0.25$
- Authenticity keywords = 10 → $Bs = 0.10$
- Packaging mentions = 15 → $Bi = 0.15$

$Score = 0.4(0.25) + 0.3(0.10) + 0.3(0.15)$ $Score = 0.175$
$ABI = 1 + 9(0.175) = 2.575 \approx 3$

Interpretation for you :

- ABI 1–3 → means it could be a counterfit product
- ABI 4–7 → mixed one original and other fake
- ABI 8–10 → product seems original

3. Reviewer Credibility Score (RCS%)

Definition:

RCS measures the trustworthiness of individual reviewers by checking: Verified purchase Review length / detail Presence of measurements, specifics, or genuine usage context

This parameter evaluates how credible the review ecosystem of the product is
Listings with fraudulent activity typically use unverified reviewers.

〉Step 1 — Per-review credibility

$$qual = 0.5(VP) + 0.3(L) + 0.2(detail)$$

Where:

- VP=1 for verified, else 0
- $L=\frac{\min(\text{word count},200)}{200}$
- detail=1 if review contains numbers

› Step 2 — Final RCS

$$RCS=\frac{\sum qual_i}{N}\times 100$$

Example

Review	VP	Words	Detail?	Score
R1	1	120	Yes	1.04
R2	0	40	No	0.06
R3	1	80	No	0.62

$$RCS=\frac{1.04+0.06+0.62}{3}\times 100=57.3\%$$

Interpretation for the user :

- 0–40% → Weak, bot made this reviewers
- 40–70% → can be trusted but not perfect reviewer
- 70–100% → officialy verified user can be trusted

4. Sentiment Score (%)

Definition:

sentiment such as positive or negative may affect a user if a product has an unusally boosted positivity or users also make it seem a bad product because of their anger on somethings it takes account in many reviews and sees that what are the sentiments of the user after buying the product it shows how strong a user feels about the product both ways

.Step-by-Step

› Step 1 — Sentence sentiment score

$$Score=\frac{\sum(\text{positive hits-negative hits})}{\text{number of sentences}}$$

› Step 2 — Normalize score to 0–1

$$Norm=\frac{(CappedScore+1)}{2}$$

Where:

- CappedScore is limited between −1 and +1

› Step 3 — Apply weight based on verification

$$Weighted=Norm\times Weight$$

Where:

- Weight = 1.2 for verified
- Weight = 0.8 for non-verified

› Final Sentiment Score

$$Sentiment=\frac{\sum Weighted}{\sum Weights}\times 100$$

Sentiment helps evaluate customer experience trends and helps check them these things in that product

- If there are negative sentiment always indicates fraud risk
- If unusually positive sentiment suggests that a fake review boosting
- How sentiment patterns change across honest vs fraud listings

It provides a good validation for the model's fraud detection capabilities

Example: There are reviews such a:

- The product is good but delivery was super slow
- Worst product never buying this
- There are other products better then this in other websites

And gives score based on positive=1 and negative=3 based on the final score user can understand the emotions of other users

VII. QUANTITATIVE RESULTS

Having built Seller Shield and trained it, we thought we should get in to the field with it. In that regard, we have verified performance statistics and in fact test results.

A. How useful was Seller Shield at taking valuable information then?

The Seller Shield was tested on the 350 products listing in various online stores. It could retrieve valuable material on 94

percent of pages and could not have issues with the search of scores, feedback, deals or terms almost always. Seller Shield reclaimed three out of four characteristics 98 per cent of the time even in cases of a strange page or a page lacking presented information. It could capture most of the details on almost every attempt although the layouts were not always accurate. It was even capable of extracting three parts nearly all the time even when the details were not displayed in the right manner. It always retrieved three out of four bits with over 100 percent success even when arranged occasionally in a disorganized manner.

The process of analysis was quick; it took approximately 127 ms/ round numbers, a hundred and twenty-five thousandth second, the results were usually delivered a hundred and twenty-five thousandth of a second sooner. During this time the tool was responsive and it could not be said to have lag.

B. ML The comparison between the choices made by Seller Shield and an ML one.

One more thing we were interested in was whether our bare rule-driven system that relies on the browser could achieve performance similar to our smarter and heavier offline-trained AI model. In this regard, we have done tests on 150 products entries that have been submitted to be checked by humans.

Seller Shield 10 percent Seller Shield had almost the same risk ratings as the ML model 81 percent. It identified 89 percent of actual fake listings, and hence most of the frauds could not get away. It was not impartial but it sounded consideration of red flags in nearly all the apparent instances of fraud. A few of them did not go by but the majority of them were picked up at an early stage and false negatives were not common. It did not falsely declare any top-name brand; there was good performance. The legitimate sellers that the system appropriately identified as being low risk equaled 88 percent.

C. What is it that these figures are saying?

The findings have shown that Seller Shield is effective and it is nevertheless fast. It is likely to attract the correct data and correlate with reliable devices, and none of them slows down and takes into account the information leakage. Above all, it does not provide spam notifications to buyers because it is interested in the things that matter.

Despite the advanced system preventing a couple more frauds, we have chosen in favor of Seller Shield straight forward system because it is quicker and easier to understand by people and also creates confidence. It is not expected to replace the existing safety arrangements but add-on to the major safety systems that have established primary safety systems in the markets.

It is not only numbers, but there is the reality of Seller Shield application in real world. After lab tests, we made a short test to discover honest feedback of the regular shoppers who utilize it on their own.

A. How did things go?

We had employed 30 people of all sorts with their degree of expertise in online purchasing. Each one was requested to inspect ten series of items in Seller Shield some of which were fake, and some of which contained red flags. All users completed a small questionnaire referring to their experience with the use of the tool.

B. What were folks saying?

Easily interpreted: 92 per cent of them easily comprehended the ratings of risk as to why a seller looked risky or trustworthy. Majority 87 percent are indicated to have had confidence in making purchases with Seller Shield, a remarkable feat given that a safer shopping experience will lead to evading dubious dealings and make more informed decisions among shoppers. About 83 percent indicated that they would use the tool on a daily basis as long as the tool would be compatible with their web browser.

C. Recommendations on the manner of improvement.

The response was excellent and people come up with some brilliant suggestions:

Many of their users wanted to find an attractive offer or unexpected sale with the old prices. It was suggested to come up with a parameter comparing the riskiness of the different sellers of a particular item. Customers would be able to settle on the superior one as compared to making random selections. A few of them wanted the application since they will be in a position to use Seller Shield when making online purchases using their phone.

D. So what did people do with the add-on?

User spending on digging on why some of the items are flagged as risky is approximately 77 percent as they use Seller Shield. users in cases where the stakes were higher and the users did not listen to noise or focused on actual matters.

X. ERROR ANALYSIS AND SHORTCOMINGS

There are still some well made tools that are not able to do everything that Seller Shield covered. Understanding the time it is straining, including the reasons would allow improvements to be introduced, and buyers to be brought to their senses.

Approximately 6 percent of the product page was not equipped with product Seller Shield essentials. What's behind this? There are a few of the common problems that occur.

Delays in loading pages: Sometimes websites display portions of content one bit at a time especially those created using tools like React or Vue.js. As Seller Shield seeks to access the data early enough it may miss important information as the pages continue to load.

Languages and Local variations: Some of the scammers employ better price reductions to avoid notice so that it does not appear to offer massive discounts on its site, but lesser price cuts. Some of the gangs require in-house information, which only the marketplace possesses.

A. keeping up with the change in your site.

Whenever any store site makes any adjustments to its appearance, the script of Seller Shield will have to be adjusted accordingly. Similar to the experience with Amazon India having changed the menu configuration, our tool did not work properly until that 78% of the time until we adjusted the settings that took some two hours.

B. Safe storage of information + future.

At this time, Seller Shield stores all the data in the device that nothing is sent. Nevertheless, in the future, when we may share concealed indications of frauds to augment intelligence in a collection of users, not only will care be pertinent but prudence will be significant. Differential privacy tools or secure multi-party computation may intervene, which means that you will keep your information secured, and group wisdom becomes larger.

XI. DEPLOYMENT GUIDE AND CODE STRUCTURE

The process of install Seller Shield will be as painless as possible, and not a single sophisticated order and terminology. The next section will guide you through the process of installing the extension and give you an idea as to how the entire process works, as far as the hood is concerned.Installation Locally: Seller Shield. In order to test Seller Shield in a computer of your own, just follow the steps below:

A. Install Extension Files: Make sure that you have the following folder containing the following files: content.js, popup.html, popup.js, model.json, manifest.json, and the icons folder.

Get to the Extensions Page of Open Chrome: Your browser, Chrome or Chromium browser will bring you to the chrome/ extensions page.

Turn on Developer Mode: the button on the upper-right hand side will give you an opportunity to add extensions that are not included into the official store.

Install the Unpacked Extension: Click the load unpacked and use the folder where you have stored the Seller shield files.

start Shopping Select any one of the your product in websites like Amazon, Flipkart or Myntra and open the page in your browser and look at the Seller Shield icon in your extenstions and then click on scan

B. What's Included? Main Code Parts

content.js (The Page Scanner): This will be automatically run on all product pages. It sweeps over reviews, rating or deals - watching out on suspicious phrasing - according to the shop. It is one that is intended to alter tactics in case the first one does not work. popup.js (The Scorekeeper): This is the script that loads the rules to be used in scoring the risk and works with the information in content.js. It standardizes the numbers, and calculates the risk rating, and produces the graphical report which you are looking at in the popup. train model.py is left out of the fray because it does not have to go to game days, but it is an actor like a strategist. It is not an online platform and targets specific activities in a local manner. It can recognize trends linked to fraudulent sellers as it operates with high amounts of data; it creates principles that the add-on would subsequently utilize. Others see it as a pre-work preparation of core logic: positioning what will prove significant when the tool is put in operation.

C. Updating the Model

Will require retraining Seller Shield so that it is more intelligent? Here's the general process:

Train a model on your new data. Save the parameters of the new normalization to model.json. Modify the model.json that is already present in your extension folder. Reload the extension in the Chrome. Test two or few product pages to check that all is alright.Seller Shield does already do a great job of helping shoppers avoid dangerous sellers, although things can always be madea bit better. Here are the ways by which we might augment the preciseness and user experience and meanwhile make all of it being plain and non-disclosed to users:

A. Smarter Browser.

Imagine Seller Shield would develop microscopic effective machine learning on your tablet, no powerful server.necessary. With technologies like TensorFlow.js, we would be in a position to run smaller neural network operations that would pinpoint fraud in a better way and none would require over one second and they would not even be transmitted to anyone. These mini brains would also be capable of doing their job in a fraction of a second or so and then you will not feel any delays.

B. Developed Language Understanding.

At the moment Seller Shield is searching some suspicious words, however, it could become even smarter in future and know how to do it, too. It is with the aid of modern language processing that Seller Shield identifies fake reviews. It recognizes the trends of excessive good language and locates deceptive phrases, which are used by fraudulent persons, even in the case they are not included in a standard list of key words.

C. A picture may not be as powerful as words.

Seller Shield will very soon verify the fact that the photographs of a product belong to a single seller only and they match the description of this product. The quick check-ups will either expose counterfeit goods or discrepant stock keeping.

D. Automatic Web Site Changing Update.

Online stores continue to change their designs. Although the look of the location has changed, Seller Shield will still be able to recognize where the ratings, reviews, and discount goes are located without a person involved in this process applying machine learning or computer vision. This will reduce the number of manual updates and will give more coverage to shoppers.The effects of such additions are that Seller Shield is more robust and valuable, and it all without making it vaguely more complex and invasive of your privacy.

XIII. CONCLUSION

The case of Seller Shield illustrates that the online fraud can be prevented, but at the same time, your privacy and lack of trust in obscure mechanisms working under the surface can be maintained. It offers an intuitive, convenient, detecting fraud on mobile platform, which may be accessed by shoppers, not collecting secret information, pursuing them about or relying on a skilled server processing.we took Seller Shield as a platform coined on the facilities that customers are sure to notice regardless of their intentions; reviews, star rating, and exceptionally low deals. I superimposed with then experiences on working with machine learning in practice. The result is expedited, direct information about a seller that is dangerous or dependable. No concealed foretelling, no data disclosure, and silent procedures. And it is all done through your web browser and you can see the reasoning as it goes on - a more transparent process.The combination of experiments with over 350 real products portrays that Seller Shield can identify the accurateness of pertinent information 94 percent of the occasions and can predict 81 percent near to how an expert does. It also blocks nearly 9 out of 10 confirmed fraudulent transactions without marking a legitimate brand. In one of the user studies, nearly all of the interviewees also said that the explanations were clear and well-understood, and Seller Shield made them feel better when they go online shopping.Although it is massive, still, data-intensive platforms could do. discovery of more scams yet Seller Shield is far more transparent and helpful to giving the regular customer what is desired: control and transparency.Relative to camouflaged systems applied by e-commerce companies, Seller Shield is able to break down all risk scores to reveal precisely why a product is risky.I tend to add, that Seller Shield sheds some light onto a more general e-commerce issue. Seller Shield is available in a form that allows buyers to receive plausible help without spying on their customers or applying sophisticated algorithms as opposed to the majority of systems which emphasize on securing their platform at the expense of the user. The actual trust is created by its transparent and open detection of frauds.

We have opportunities of thinking further. Delays are unnecessary in web browsers with smart algorithms that can be executed in them. The tone and hints can be used to improve the feedback in future and the users can notify suspicious vendors without disclosing the information.Seller Shield is a move towards the right direction of higher security and stability among the online customers. It presents three significant benefits namely absolute transparency which makes the scores credible, no user data transfer is outside the gadget and low processing costs which makes the pages fast. With modern language processing, Seller Shield may identify fake reviews by identifying trends in overly positive wording or even locate scammer tricks that scammers still employ despite not existing on some list of keywords that a scammer could be. This would aid in apprehending fraudsters, which are becoming increasingly creative with their word choice.

we can make out room to think down the line. Smart algorithms in web browsers no delays. More accurate mood and strange details of feedback paragraphs. Probably new techniques that would allow individuals to report unstable vendor conduct without disclosing data. The software dubbed as Seller Shield appears to be an initial step of this nature and it is on the verge of bringing greater security and balance to digital buyers.Another concept is added in that the light rule arrangement continues to impress me. Even though it is responsive, unlike heavy server based filters, it has three distinct advantages total openness so that users can more readily believe that no data is sent off-device, as well as low processing requirements so that pages remain quick.

REFERENCES

[1] A. Mutemi and F. Bacao, "E-Commerce Fraud Detection Based on Machine Learning Techniques: Systematic Literature Review," *Big Data Mining and Analytics*, vol. 7, no. 2, pp. 419–444, 2024.

[2] A. Kumar and S. Goyal, "AI-Driven Fraud Detection in Online Marketplaces," *ACM Computing Surveys*, vol. 55, no. 3, pp. 1–38, 2023.

[3] K. Singh and M. Gupta, "Graph Neural Network Approaches for Fraud Detection: A Survey," *Expert Systems with Applications*, vol. 224, article 119923, 2023.

[4] Statista Research Department, "E-commerce worldwide – statistics & facts," Statista, Tech. Rep., 2023.

[5] Y. Panigrahi, S. Borah, and R. Sharma, "E-Commerce Fraud Detection Using Hybrid Machine Learning Techniques," *Journal of Information Security and Applications*, vol. 63, article 102981, 2021.

[6] F. Caron et al., "Machine Learning for Detecting Online Marketplace Fraud," *Pattern Recognition Letters*, vol. 152, pp. 74–82, 2021.

[7] R. Carcillo et al., "Combining Unsupervised and Supervised Learning in Credit Card Fraud Detection," *Information Sciences*, vol. 557, pp. 317–331, 2021.

[8] T. T. Nguyen, K. N. Nguyen, and D. Hoang, "A Deep Learning Approach for Detecting Fraudulent Transactions in E-Commerce," *IEEE Access*, vol. 8, pp. 90698–90710, 2021.

[9] A. Srivastava, A. Kundu, S. Sural, and A. Majumdar, "Credit Card Fraud Detection Using Hidden Markov Model," *IEEE Transactions on Dependable and Secure Computing*, vol. 5, no. 1, pp. 37–48, 2008.

[10] R. Jindal, "Anomaly Detection in E-Commerce Transactions Using Machine Learning Techniques," *International Journal of Computer Applications*, vol. 182, no. 45, pp. 1–8, 2019.