IJMRSETM

e-ISSN: 2395 - 7639


# INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

## IN SCIENCE, ENGINEERING, TECHNOLOGY AND MANAGEMENT

Volume 11, Issue 6, June 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.802

International Journal of Multidisciplinary Research in Science, Engineering, Technology & Management (IJMRSETM)

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 7.802 | A Monthly Double-Blind Peer Reviewed Journal |

| Volume 11, Issue 6, June 2024

# Reduction of Problems in the Online Payment System through Hybrid Model

**Pranay Sunil Pandere, Rohit Baban Somvanshi, Aquila Shaikh, Sheetal Waghmare**

Department of MCA, Late Bhausaheb Hiray S.S. Trust's Institute of Computer Application, Bandra (East) Mumbai, Maharashtra, India

**ABSTRACT:** Online purchasing, electronic invoicing, auctions, and other similar applications all have the risk of fraudulent transactions. One of the difficult areas of web development and online phantom transaction is the occurrence and detection of online fraud. Since research databases provide secure specifications of online frauds, methods for identifying and preventing them are also being studied. We offer a method that uses mobile implicit authentication and the Hidden Markov Model (HMM) to determine whether or not an online user is a fraud. In order to combat the fraud that has happened and stop the client from leaving, we provide a model based on these strategies. Since our method is more parameterized than conventional methods, there is a lower likelihood of misidentifying a real person as a fraud.

## I. INTRODUCTION

Because online buying only requires one click, crowded storefronts are being replaced by it worldwide.It has grown in popularity among customers. As per the February 2008 global consumer survey, "Trends in Online Shopping," over 85% of people worldwide use the internet for shopping, a 40% rise from the previous two years. The majority of these users are regular online shoppers, meaning they shop online at least once a month. The increasing prevalence of e-commerce is a really worldwide phenomenon.The biggest number of online consumers worldwide is found in South Korea, where 99% of internet users purchase online. Then come consumers in Germany, the United Kingdom, and Japan.

The increasing number of credit card users worldwide is giving fraudulent users greater chances to commit fraud, such as stealing card credentials and using them to conduct unlawful transactions. In the United Kingdom alone, credit card fraud totaled over 535 million pounds in 2006, while in the United States, it was between 750 and 830 million dollars.

One of the most dangerous problems in the credit card business is fraud, which may cost a customer a great deal of money. Therefore, stopping fraud and preventing consumers from being duped are the primary goals. One way to commit fraud is to either steal the actual card or obtain critical card information such as the security code, validity, and card number. This kind of information can be utilized to commit online fraud. Since the legitimate user might not be aware that someone else is using his card details, this kind of fraud is difficult to identify.

## II. LITERATURE REVIEW

1.Increasing Online Payment Security
Examine research aimed at improving security by means of hybrid models that incorporate technology such as blockchain, biometrics, AI, and encryption.
Talk about how these hybrid models deal with security flaws including phishing scams, data breaches, and illegal access.

2.Enhancing Transaction Trustworthiness
Examine the literature on hybrid techniques designed to lower failure rates and increase transaction success rates. Examine approaches that combine predictive analytics, real-time monitoring, and fault-tolerant systems to improve reliability.

3.Fraud Prevention and Identification
Analyze the body of research on hybrid models that combine AI/ML algorithms with rule-based systems to detect fraud.
Talk about case studies or practical research that shows how well these models work to identify and stop fraudulent activity.

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 7.802 | A Monthly Double-Blind Peer Reviewed Journal |

| Volume 11, Issue 6, June 2024

4.Improving the User Experience
Examine research on hybrid models intended to improve online payment systems' user experience. Examine strategies that enhance usability, reliability, and contentment via user-friendly interfaces, feedback systems, and customized offerings.

5.Case Studies and Examples of Implementation
Provide case studies or examples of hybrid model implementations in live online payment systems. Write a summary of the results, difficulties encountered, and knowledge gained from these implementations.

## III. RESEARCH METHODOLOGY

### 3.1. HMM model

The work of Abhinav Srivastava et al. suggests that fraud can be identified using hidden markov models. The order in which the funds are spent in every transaction is tracked by HMM.

HMM creates a cardholder's spending profile based on their spending history. Typically, it employs three profiles: low, moderate, and high. The user receives a spending profile tailored to his spending habits after computation. In this case, a series of card transactions is created, and each new transaction is followed by a deviation check. In order to determine fraud, the percentage of deviation is compared to a threshold in the event that there is one.

The new transaction is added to the sequence if the variance exceeds the threshold, which indicates fraud. The system's accuracy in this method is very nearly 80%. More restrictions could be added in this case to improve the false positive.

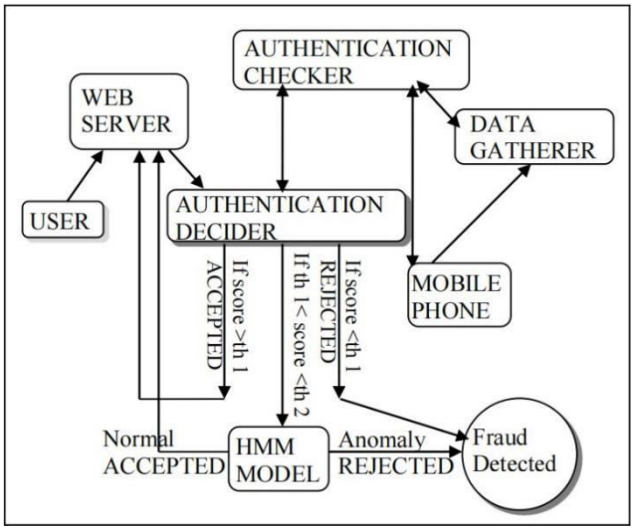



Figure 1.Proposed Hybrid Model

### 3.2. Hybrid model

By this proposed model, see figure 1, we are combining the two approaches as discussed above i.e. HMM technique and the authentication by the user mobile.

Table 1. Algorithm for Proposed Hybrid Model. Step 1 User accesses the web server and makes the payment request to the authentication decider. Step 2 Authentication decider asks for the authentication details from the authentication checker. Step 3 Authentication checker refer to mobile device and /or data gatherer for the authentication details based on mobile behavioural pattern. Step 4 Authentication checker then generate the score (discussed below) and send it to authentication decider. Step 5 Authentication decider then compare score with the thresholds than follow any of the three cases discussed below.

The detail explanation of the complete process is discussed in this section and with the help of the case studies in the next section. Normal ACCEPTED USER AUTHENTICATION DECIDER AUTHENTICATION CHECKER DATA GATHERER REJECTED If score th 1 Anomaly REJECTED Fraud Detected HMM MODEL MOBILE PHONE WEB SERVER In this architecture we consider the following types of blocks i.e. mobile phone, data gatherer, authentication checker and authentication decider, HMM model block(this block includes complete HMM model which is based on

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 7.802 | A Monthly Double-Blind Peer Reviewed Journal |

| Volume 11, Issue 6, June 2024

spending habits of consumer as discussed in part B, [11]). In this approach user made a payment request (for any article, commodity) from a web page to the authentication decider. The data gatherer collects the mobile data from mobile information like SMS history, phone call history, history of browser, information of the network and device location regularly. The authentication checker takes the data from the data gatherer or directly from the client device. The authentication checker makes all the decision with the help of the data collected and the policies of authentication. These policies are given to the authentication by the authentication decider which is obtained from the user request (payment request). After that authentication decider compare the probability score obtained from authentication checker with the two threshold namely threshold 1 and threshold 2 (assuming: threshold 1 < threshold 2). The score mention above is the probability of matching the behavior, it is computed with the past and recent behavior of the user .the thresholds can differ for different applications and there security parameter. The comparison of score and threshold is used for making decision for authentication. If the score is less than threshold 1 then request will be directly rejected. This means there is high degree of mismatching in the pattern of behaviour so there is definite chance of a fraud. The figure 2 shows how model will flow in this case.

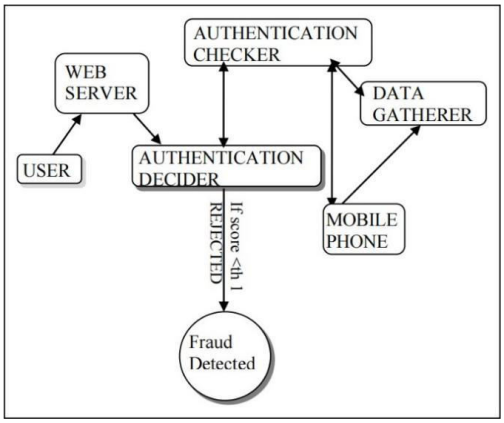



**Figure 2. Flow diagram for case 1**

In the event that threshold 1 < score < threshold 2, the requested transaction is sent to the hmm model since there is a slight or partial pattern match.Now, if the card holder's spending profile deviates from normal in accordance with the HMM model, an alarm will sound; otherwise, the request will be performed. The flow of this model in this instance is depicted in figure 3. The request is immediately approved if the score is greater than the second criterion since there is a strong likelihood of matching, or that the pattern behavior is almost identical to that of the authentic user. Figure 4 illustrates the flow of this model in this instance. The mobile phone operating system collects the data that includes user's activities on the mobile like phone call patterns, SMS activities, location, web access etc.

Following that, it regularly updates the data gatherer on this. These data are temporarily saved on the mobile device until the data collector has obtained them all, at which point they are removed from the device's local memory. With the aid of specific encryption techniques that are used beforehand, this data exchange is carried out safely. This is being done in order to safeguard the customer's privacy. In this manner, the customer's privacy will be respected while the patterns are identified.

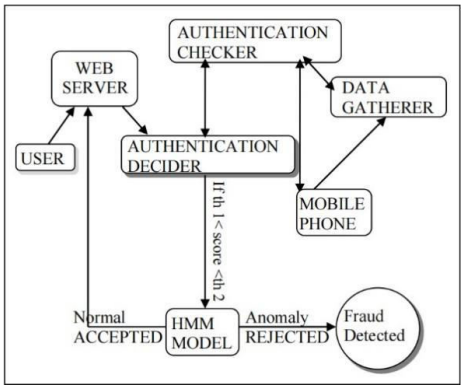



Figure 3. Flow diagram for case 2.

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 7.802 | A Monthly Double-Blind Peer Reviewed Journal |

| Volume 11, Issue 6, June 2024

Data is gathered by the authenticity checker from the data gatherer and occasionally straight from a mobile device. It gathers information in accordance with the guidelines given by the authentication decider.
When a payment request reaches the authentication decider, it is forwarded to the authentication checker, which uses the information provided to it to send the query to the data gatherer or mobile device.

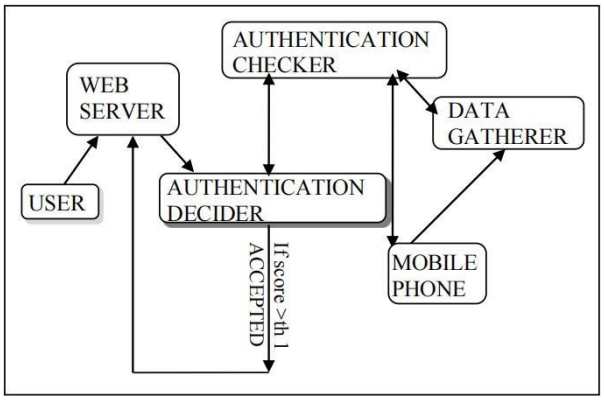



Figure 4. Flow diagram for case 3.

The data gatherer respond to the query and send back the required details to authentication checker. It then computes the authentication result based on the policy .the authentication Normal ACCEPTED USER WEB SERVER AUTHENTICATION DECIDER AUTHENTICATION CHECKER DATA GATHERER If th 1< score th 1 MOBILE PHONE WEB SERVER checker also calculate the score of the matching pattern with help of the past and recent behavior. This score is send to authentication decider where it compares it with the threshold 1 and threshold 2 as mentioned above.

## IV. CASE STUDY AND RESULTS

In our proposed model here we study it on two scenarios namely mobile theft and card theft (details).

### 4.1. Mobile theft

We are limited to relying solely on the pattern that the authentication system observes when using the mobile authentication strategy. Therefore, there's a good chance that in this instance, the genuine user will be seen as fake. Mobile theft has no effect on the HMM model. Therefore, mobile theft is irrelevant in this situation; what matters is how the cardholder's spending patterns are observed. We rely on more than just the movable detail pattern in the hybrid model. Depending on the likelihood of the pattern matching by the first phase, we employ both the card holder's spending behavior and the mobile device's pattern in this instance. The following scenarios are possible:

**Case 1:** High profile indicates a high likelihood of matching between the pattern seen in the first phase. For example, authentication score > threshold 2. However, there is little probability of a high score in the event of mobile theft because the thief's usage patterns will undoubtedly diverge from those of a legitimate user.

**Case 2:** Middle profile: this indicates that there is a chance that the pattern seen in the first phase will partially match. That is, authentication score < threshold 1 < threshold 2. Since merely mobile patterns cannot guarantee against mobile theft, it is most likely that there has been mobile theft. Accordingly, our model will employ the HMM phase, which is the second phase, to further verify the transactions. This increases our likelihood of identifying the fraud user compared to the prior strategy, which was the mobile authentication approach, and decreases the possibility of a false positive—the identification of a genuine user as a fraud user.

**Case 3:** Low profile: this indicates that there is very little chance that the pattern seen in the first phase will match, or that the authentication score will be less than 1. It is equally likely that a mobile device will be stolen, but in this situation, the thief's observation patterns should be more closely aligned, with a high degree of pattern mismatch. In this instance, the user will be recognized as a scam and may be turned down outright. For instance, the user's mobile device may have been pilfered. Let's now assume that our thresholds 1 and 2 are at 25% and 75%, respectively.

Since the mobile device in this instance has been stolen, call patterns, location, and other patterns will differ from reality. As a result, pattern mismatching will occur, and there is very little likelihood that the authentication score—that

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 7.802 | A Monthly Double-Blind Peer Reviewed Journal |

| Volume 11, Issue 6, June 2024

is, the percentage of matching—would exceed threshold 2, or 75%.The middle situation, where the score falls between thresholds 1 and 2, or 25 and 75, has the highest probability. Here, the user will once more be asked to verify its legitimacy using the hmm model, which is based on their buying habits.

Additionally, the user will be immediately rejected if the authentication score or percentage of matching is really low—let's say less than 25. Overall, there has been very little shift in how we treat genuine users as fraud users, thus we verify much more thoroughly than we do with other methods. For illustration, let's look at a week's worth of mobile usage data. Here, we just take into account the numbers for phone calls and SMS (see table 2).

## V. CONCLUSION

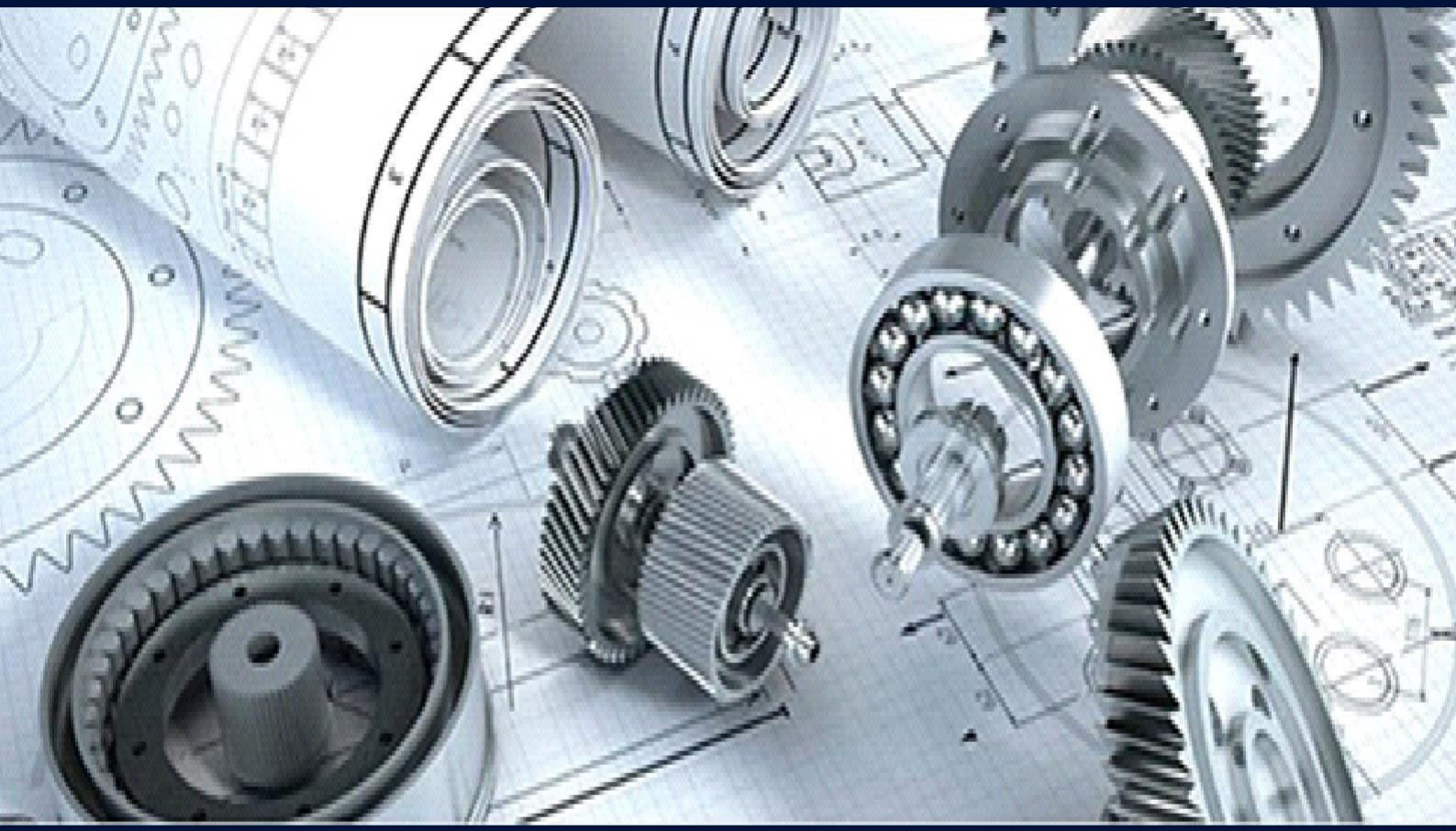
In this research, we have suggested a strategy that combines mobile implicit authentication based on mobile data patterns with hmm model based on user spending profile. Due to its consideration of both spending patterns and mobile usage patterns, this approach places a high level of security on the cardholder. This reduces the likelihood that a genuine user will be viewed as fraudulent, which lowers the number of false positives. We plan to expand this methodology to include various other online frauds and their specific methods of detection. Regarding a fraud, it is still necessary to specify the fraud detection mechanism. Online communication and business will benefit more from this kind of detection approach, which combines comprehensive detection and prevention mechanisms.

## ACKNOWLEDGEMENTS

As the author, I extend my gratitude to Prof. Aquila Shaikh & Sheetal Waghmare Professor of (MCA)Department, for her valuable guidance and support throughout the development of this research paper.

## REFERENCES

[1] Trends in Online Shopping Global Consumer Report‖ http://id.nielsen.com/news/documents/GlobalOnlineShoppingReportFeb08.pdf.
[2] "Plastic card fraud goes back up". BBC. March 12, 2008. http://news.bbc.co.uk/2/hi/business/7289856.stm. Retrieved January 2, 2010.
[3] USDGBP=X: Basic Chart for USD to GBP — Yahoo! Finance.
[4] J.R Dorronsoro, F. Ginel, C. Sgnchez, C. S. Cruz ―Neural Fraud Detection in Credit Card Operation‖ IEEE Transactions on neural network vol. 8 no.4, July 1997.
[5] E. Aleskerov, B. Freisleben, and B. Rao, ―CARDWATCH: Neural Network Based Database Mining System for Credit Card Fraud Detection,‖ Proc. IEEE/IAFE: Computational Intelligence for Financial Eng., pp. 220-226, 1997.



INTERNATIONAL STANDARD SERIAL NUMBER INDIA

# INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

## IN SCIENCE, ENGINEERING, TECHNOLOGY AND MANAGEMENT

+91 99405 72462 +91 63819 07438 ijmrsetm@gmail.com

www.ijmrsetm.com