wahaj

by S S

Submission date: 26-Sep-2023 11:37AM (UTC-0700)
Submission ID: 2147489929
File name: Week_2_Part_4.docx (20.73K)
Word count: 1085
Character count: 5958

PSD2, the payment directive system 2 (BBVA, n.d.), is a European regulation for online payment services. Its primary purpose was to make payment more secure and smooth in Europe while helping banks adopt new technologies and promote innovation and competition in the financial sector. It became effective in September 2019.

One of the primary effects after its implementation was that it introduced strong customer Authentication by dividing the authentication factors into multiple layers to access someone's account or to perform a transaction such as mobile device and biometrics or password to get into the electronic transactions, which makes it more complex for the criminals to access them.

It has a good impact on businesses such as E-commerce, leading to the development of innovative payment methods such as open banking. It has also improved and made card payments more secure. Before its implementation, only a basic card information from the card was enough to perform a transaction through it, making it easier for the fraudster. With PSD2, the SCA is mandatory for almost all online payments, making it difficult for criminals to do a financial transaction.

This system also has some challenges, and many people find it irritating to go through multiple security layers, often leading to cart abandonment in E-commerce activities, which leads to loss of business and clients in the E-commerce sector, so keeping a good customer balance is also compulsory while ensuring their security.

Introduction

Online transactions have become an integral part of our daily lives, which is why the associated threats are becoming more significant daily. People are shifting towards it as they offer more convenient solutions to daily life activities. Recent statistics (Itexus, 2023) reveal that fraud losses will cross 40 billion dollars by the end of 2027. In order to minimize these activities, financial institutions are shifting their focus towards developing technologies such as Artificial intelligence for fraud detection and to make their systems more secure and reliable. This report covers the significant aspects of AI in these activities and its benefits and drawbacks.

Role of AI in Online Banking Fraud Detection:

AI and machine learning algorithms allow banking systems to continuously learn from new data and perform analysis on it so that they can continuously learn from the data so that the accuracy and adaptability to new fraud activities can be improved. Machine learning, a subset of AI, majorly focuses on developing algorithms that learn from the provided data and improve themselves to detect fraud patterns. They help in detecting fraud activities in the following ways.

- It observes and analyzes the customer's behaviour to detect any unusual pattern, e.g. if the location or any observed parameter suddenly changes, AI algorithms flag this as suspicious.

- It also keeps track of customer anomaly if a customer only makes small transactions and suddenly initiates a significant transaction. The AI system promptly generates a threat alert, which helps identify activities such as CNP fraud and account takeover.
- It can perform analysis on the provided pictures. e.g. if a customer uploads a check for deposit, Ai can verify its authenticity and red flags if there are any signs of forgery.
- It also uses natural language processing techniques to perform analysis on text data, and if the chatbot detects any unusual language, it can forward the issue for further investigation.

Role of AI in Biometric Authentication

AI's role in biometric authentication and a few typical applications are listed below.

- It is now used widely for biometric authentication. By analyzing human facial nodes, it can detect a person's identity.
- It uses AI to analyze provided voice patterns and detect the voice often used for phone-based verifications.
- Many platforms use Fingerprints and Iris scanning for identity verification as they are generally more secure.

The pros and cons of AI systems are listed below.

Pros

- It tracks anomalies and patterns, which helps banks detect fraud more effectively.
- Advanced authentication methods such as fingerprints and facial recognition provide a better user experience for customers
- It helps to reduce the no of false positives, which reduces customer inconvenience

Cons

- Storing personal information for biometrics and face detection has raised privacy concerns as they involve storing and collecting personal data.
- They can deceived and tricked, such as facial recognition can be tracked through photos and videos, while voice recognition can be tricked through voice recordings.

Following are the two examples in which AI is frauds.

- Ai-based voice recordings and videos are being used to access someone’s account during the verification call from customer care.
- AI-based chat boats are also used that pretends to be customer care representative and get all the sensitive information from the customer and then access their accounts. This type of fraud is widespread in countries like Pakistan.

Conclusion:

AI has dramatically helped improve the security of the current banking and financial systems with advanced fraud detection technologies. However, on the other hand, it has raised some serious privacy concerns, so keeping a strict balance between security and user experience is essential. By keeping a good user experience while keeping their data protected is a major challenge that the financial systems have to face in upcoming years.

Sub Domain Take Over

It is a type of cyber security threat in which criminals get access to control a domain of a website or an organization. It can occur due to removing a virtual host or the host has not been published. The hacker can control the subdomain by providing a virtual host to the site and hosting their content. It can lead to substantial business risks such as reputation damage and data breaches.

Following are the steps through which these types of sub domain take overs can be avoided.

- Make a robust procedure for the authentication and authorization of subdomain creation and modification.
- Keep a complete inventory of every subdomain linked to your domain and regularly check for updates to their DNS records.
- Make regular backups of your DNS configurations and keep one handy for speedy restoration in takeover situations.
- Avoid the CNAME usage for the subdomains, and ensure all the target domains are trusted and under your control.
- Use external monitoring tools to look for alterations to DNS records or subdomain configurations that could indicate takeover attempts.
- Create and maintain a list of all of your domains and their hosting providers, and regularly update it in order to ensure that nothing is left unnoticed

Bibliography

BBVA, n.d. *BBVA.com*. [Online]
Available at: https://www.bbva.com/en/everything-need-know-psd2/
[Accessed 26 09 2023].

Itexus, 2023. *Itexus*. [Online]
Available at: https://itexus.com/banking-fraud-prevention-best-practices-success-stories/#gref
[Accessed 25 09 2023].

wahaj

ORIGINALITY REPORT

0%	0%	0%	0%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		