North American Journal of Engineering and Research

Est. 2020

Security Threats in Today's Payment Processing and Advanced Technological Solutions

Rajesh Kotha
Email: rajesh.kotha28@gmail.com

Abstract

Recent advancements in information technology have brought numerous complications that put the financial processing systems at risk, hence, many safety challenges that current payment systems experience in the emerging digital economy. This paper focuses on the top security risks like data loss and payment fraud and the new technological approaches of data encryption, tokenization, and fraud detection by an artificial intelligence system. Encryption encodes the payment information so that unauthorized persons cannot intercept their contents, and tokenization replaces regular payment information with tokens, making hacking difficult. A fraud detection system based on AI applies machine learning techniques to stop fraudulent actions in real-time. This word examines the challenges hampering the implementation of these technologies. The paper further analyzes the uses of security threats. The final section of the paper explores the scope of the solutions studied. This paper concludes by asserting that implementing tech-based solutions to security risks ensures the trust of the masses in digital payment systems.

Key words: Encryption, tokenization, security threats, payment processing, data breaches, artificial intelligence, and fraud detection

Introduction

Customers are increasingly paying for goods and services in cashless transactions, so the security of payment processing systems is of significant focus. The recent addition of e-commerce, mobile payment services, and digital wallets has made new entries for exploitation by hackers. Preserving the accuracy, privacy, and accessibility of payment information is critical to maintaining consumer confidence and protecting transactions. This paper discusses the main security risks characteristic of today's payment processing systems, along with the advanced technological systems developed to combat these risks

Problem Statement

The two significant risks in the current payment processing system are unauthorized individuals accessing customers' payment information and actual or relative payment scams. These threats can lead to considerable losses in revenues, market share, and brand image, fines, and penalties, among other challenges to the firms. Organizations require a dependable security mechanism to guard against threats that are in a constant state of evolution.

Literature Review

The security of payment processing systems has emerged as a major research topic of discussion and study within the last decade precisely because of the trend towards more frequent use of cashless transactions. Many publications have analyzed different aspects of payment security, the threats modern systems face, and possible solutions. The data breach problem affecting online payments is quite common and can be associated with low levels of encryption [6]. The importance of tokenization in payment security cannot be underestimated, as it helps protect data effectively, especially in the e-commerce environment.

Some researchers have also investigated employing artificial intelligence (AI) in fraud detection. Alzahrani and Aljabri (2022) assess AI-based systems by pointing out their effectiveness in detecting fraud as they work in real-time [4]. These studies indicate that AI is gaining new importance as payment security, especially in dealing with unusual payment trends. Also, in a combined analysis published in 2023.

The shift of consumers to online purchases has necessitated the adoption of these technologies to secure transaction data. Mobile applications have become a standard means of payment. Therefore, tokenization, AI, and encryption technologies are much more needed [11]. For instance, to protect data sent over wireless networks, mobile payment apps and wallets like PayPal, Apple Pay, and Google Wallet use encryption. [13]. However, there are limitations concerning the efficiency and economic viability of adopting such technologies in a cross-sectoral environment for small and medium enterprises (SMEs). For instance, research by Morrow and Zarrebini noted that encryption technologies can be expensive for small-scale firms [10]. The adoption of these technologies ensures secure transactions, boosting customer’s confidence in online payment systems [8]. The existing literature confirms the need to upscale the adoption of information security technologies for online payment systems to avoid costly data breaches.

Solutions

Today, many solutions can be implemented in payment processing systems to reduce security risks. These solutions include encryption, tokenization, and artificial intelligence fraud detection. All these technologies have their advantages when used individually and jointly and offer a comprehensive security solution for shielding sensitive payment data.

Encryption

Encryption is an important technology used to safeguard payment data by converting the information into a different form that appropriate parties can only read. In encryption, an algorithm and a fundamental change a plain text message to cipher text [1]. Only the person who holds the decryption key can reverse the cipher text to mean the plain text form.

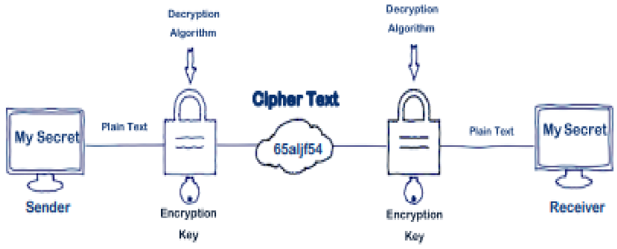

Figure 1: Encryption illustration. Adapted from [1]

Types of Encryptions.

Symmetric Encryption

This method employs a single key for data encryption and decryption [1]. Due to the optimized performance, this algorithm is perfectly suitable for encryption of tremendous volumes of data. However, responsibly sharing the key among entities is one of the significant challenges.

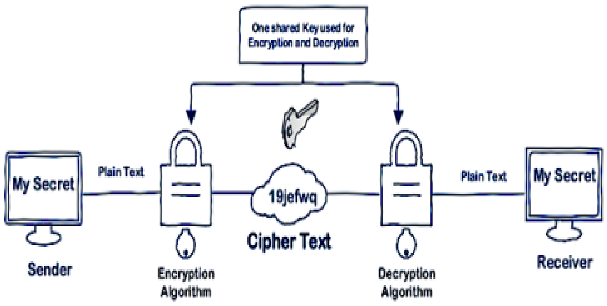

Figure 2: Symmetric Encryption. Adapted from [1]

Asymmetric Encryption

This method exploits the service of two keys; one is the encrypting key, also known as the public key, and the other one is the decryption key, referred to as the private key [1]. Since the private key is non-disclosed, its usage is efficient. However, it is noted to require better computation ability compared to symmetric encryption.

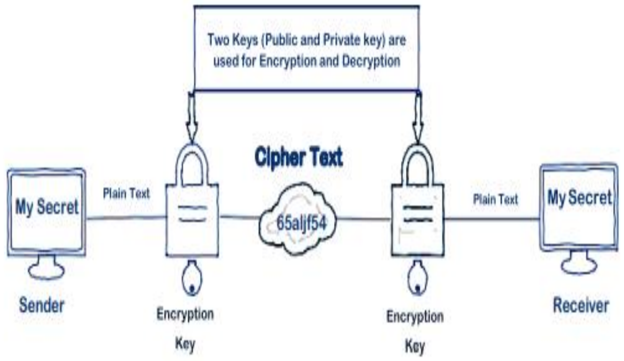

Figure 3: Asymmetric Encryption. Adapted from [1]

End-to-End Encryption (E2EE)

End-to-end encryption ensures that data collected at a specific point in the communication cycle is encrypted up to the concluding stages of the transmission process [2]. This approach ensures that the hackers do not get to access the data while it is being transmitted [3]. With E2EE, the payment information sent by companies cannot be intercepted and read by other people during its transfer.

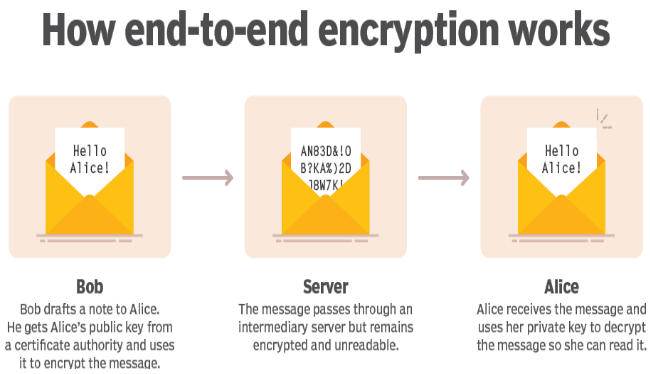
How end-to-end encryption works
Hello Alice!
AN83D&!O B?KA%)2D J8W7K!
Hello Alice!
Bob
Bob drafts a note to Alice. He gets Alice's public key from a certificate authority and uses it to encrypt the message.
Server
The message passes through an intermediary server but remains encrypted and unreadable.
Alice
Alice receives the message and uses her private key to decrypt the message so she can read it.

Figure 4: How E2EE encryption works. Adapted from [3]

Tokenization

Tokenization is a technology that replaces sensitive payment information with unique identifiers known as tokens. These tokens have no exploitable value outside the specific transaction or system for which they were created.

How Tokenization Works

The customer starts by going to an online store and initiating a payment with their credit or debit card [3]. In place of the actual transaction processor information, the acquiring bank (the bank of the merchant) receives tokenized card information from a token service provider. Tokenized credit card information is made up of data that is generated at random [3]. With this token, the buyer can contact the appropriate credit card associations, such as Visa or American Express, asking for clearance. Their financial institution safely stores the customer's payment information in a token vault. After the bank receives the token from the credit card company and matches it with the account number, the transaction will be confirmed. The merchant will get their payment token back after the transaction goes through. A new token series will be used for each subsequent transaction by the same client.

Artificial Intelligence (AI)-Based Fraud Detection

Strategically, AI-based fraud detection uses an algorithm where the system screens transaction data to determine patterns that depict fraud [4]. They offer a preventive measure on security and outlook at fraudulent dealings before they lead to huge losses. These systems can also be updated and optimized gradually, which makes them work better even in the face of new and previously unseen fraud strategies.

Critical Components of AI-Based Fraud Detection.

The main processes involved in AI-based fraud detection are data acquisition, preprocessing of data, training of the model for subsequent real-time analysis, and model evaluation. The data acquisition process includes capturing a massive amount of data concerning the transactions that occur within the industry to train the AI models. Feature engineering is a process of formulating a feature vector list that contains potential features or characteristics that may be helpful in the identification of fraudulent transactions, such as transaction amount, time, and place, among others [5]. The model training process implies utilizing the data on previous activities to orient the machine learning models to detect fraud patterns [5]. Real-time analysis entails analyzing the transactions to alert suitable alarms and highlight several activities. Finally, model evaluation is meant to determine a model's ability and effectiveness in the context of a testing set [5].

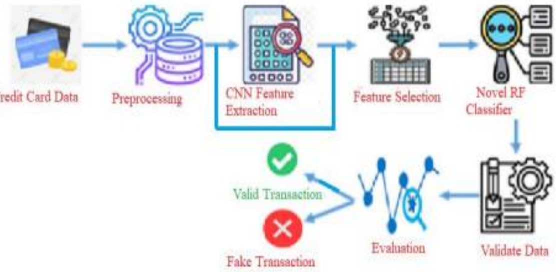

Figure 5: AI Fraud Detection. Adapted from [5]

Impact

Applying encryption methods, tokenization, and artificial intelligence in payment processing systems adds a degree of security. It reduces fraudulent activities while making the payment systems compliant with the regulations. Encryption, tokenization, and artificial intelligence fraud detection technologies achieve this by improving data security, minimizing fraud cases, meeting regulatory requirements, and boosting customer confidence.

One benefit that may be attributed to the use of encryption and tokenization is that there is a significant improvement in data security. "The most effective method for achieving data security is encryption" [6, p. 2789]. Encryption is particularly effective in the concealment of payment information, which, when processed and in its original form, is highly vulnerable to misuse by unauthorized parties. Tokenization, on the other hand, translates the original data into unique tokens that cannot be exploited in case of a data breach. Encryption and tokenization safeguard payment information from being captured and utilized for unlawful purposes while in transit and database. Even after a successful attack on the encrypted information, the adversary cannot apply or even comprehend the content without a decryption key. Likewise, stolen tokens are meaningless items that lack the necessary tools for the process of de-tokenization. These technologies keep the payment information both confidential and secure, which helps to retain the confidence of consumers as well as safeguard the financials of companies. Encryption helps to ensure that unauthorized individuals cannot read the data, and tokenization maintains the payment information stream's coherence through the use of a secure token.

Another benefit is reduced fraud incidents. Automated fraud detection control mechanisms are very effective for fraud prevention as they identify any fraudulent transaction as it occurs. These systems have incorporated different aspects of machine learning to analyze the patterns of the transactions being made and have the ability to detect fraud [5]. Compared to the manual processing of transaction data, machine learning helps one quickly process large volumes of transaction data instantaneously and, at the same time, detect and manage fraud cases as and when they occur. For this reason, this approach dramatically shortens the period between the occurrence of fraud activities and their detection, which, in the long run, lessens the loss. Given AI-based approaches to fraud detection that use machine learning algorithms like Convolutional Neural Networks (CNN) [5], it becomes a progressive process in which the system training recognizes new methods employed in fraud. This versatility means that, in essence, the system will maintain its effectiveness in identifying threats regardless of the fraudsters coming up with a new and even more complex fraud approach.

Additionally, the use of the use of encryption, tokenization and AI fraud detection enhances compliance with pre-set regulations. The mitigation of risks is crucial to organizations that process details of payments; it has to meet requirements such as the Payment Card Industry Data Security Standard (PCI DSS) . Such measures as encryption, tokenization, and automated fraud identification help businesses meet such specifications. Several controls are mandatory for storing and processing cardholder data for compliance with PCI DSS, and encryption and tokenization are among them. Through these technologies, the business can quickly implement these standards and do away with associated fines and penalties. Besides, other regulations like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) have various rules and recommend that enterprises use strong security to protect data [7]. These regulations are observed by encryption and tokenization as they protect the payment information of businesses and clients.

Lastly, safe practices in payment handling systems affect consumers' confidence and trust in the used systems [8]. Customers will be more inclined towards companies that focus on the safety of their payment details. Overall, when businesses show that they are taking payment data security seriously and implementing measures such as encryptions and tokenization, greater trust will be established with the consumers. Therefore, such trust is vital for businesses to keep holding their loyal clients and attract new ones. Among every organization that has faced a data leakage or any form of payment fraud, their business is significantly affected by its negative impact on their reputation. Measures such as ethical-security-compliance practices protect the business from witnessing such acts, maintaining the business's reputation and brand value.

However, encryption, tokenization, and AI-based fraud detection techniques have several pros, yet several cons accompany it. Adopting these technologies may be expensive and involves many integration processes that are mainly challenging for small firms. "Data encryption can be expensive and a resource-intensive proposition" [10, p.2]. On the other hand, the cost of acquiring AI-based fraud detection systems and installing and managing the systems might be expensive for some organizations.

Additionally, encryption and decryption practices may affect the system's performance differently depending on the nature of the transactions involved. For instance, query processing times can be impacted by encryption, especially for procedures that include sorting encrypted data. That means ensuring these processes do not create noticeable delays or contribute to congestion is equally essential.

Lastly, AI-driven fraud detection systems involve a lot of data gathering and processing. Organizations involved in the generation, use, or analysis of consumer data must guarantee that these activities conform to the provisions of the privacy legislation about the probable issues of data privacy and user consent [9].

Generally, it is important to note that the more general implications for the deployment of these safety features for businesses go beyond the mere framework of individual actors in the financial system. Improving the security of payment processing systems is beneficial for the protection of the economic environment. When firms apply appropriate security measures, then they are able to minimize fraud and data breaches to the entire spectrum of the payment network. The use of security technologies establishes growth and development in the field as a result of technology adoption. Indeed, as more organizations adopt and fine-tune these innovations, there are newer and more advanced solutions in the shape of improvements to current technologies.

Uses

Cryptographic protection, tokenization, and artificial intelligence fraud detection have multiple applications as integrated components in payment processing systems across different industries. This means that in addition to increasing the security of an organization, these technologies also improve operations and fulfill compliance requirements.

Encryption

Payment processing is an area that uses encryption in one way or another due to the need to protect data from unauthorized use and modification.

E-commerce platforms apply encryption to protect customers' data from the moment they enter their sensitive information till the time when they make a payment [12]. This makes it hard for hackers to intercept, and hence, vital information such as credit card numbers and details are secure.

Mobile wallets and payment applications such as Apple Pay, Google Wallet, and PayPal employ encryption to secure information transmitted over wireless networks [13]. This is very important, especially in the protection of information that the user may be accessing by using a computer or even a smartphone on the internet using unsecured wireless networks that are readily available.

Merchants implement encryption in POS systems to secure data entered at physical cash registers used to process payments [14]. This portrays end-to-end encryption as a critical layer of security, and even if POS systems are at one point compromised, the encrypted data cannot be compromised.

Tokenization

Tokenization is most helpful in minimizing the vulnerabilities concerning the storage and processing of payment information. Payment processors and gateways use tokenization to manage and process credit card details safely. By using tokens instead of the actual details on the card, they reduce the risks of data breaches and make it easier to meet the demands of PCI DSS.

Mobile apps that include an in-app purchase function utilize tokenization to secure users' financial details. This makes transactions taking place within the application more secure and thus develops user confidence.

AI-Based Fraud Detection

Using artificial intelligence in the protection of main financial assets implies dynamic and proactive safeguards against fraudulent activities. Banks and financial institutions use artificial intelligence to detect fraud [5]. They constantly analyze vast amounts of transaction data. In turn, this facilitates quick fraud detection and prevention of actions that may compromise a customer's account.

E-commerce utilizes Artificial intelligence to monitor for suspicious behaviors [15]. Thanks to such systems, fraudulent transactions and chargebacks are avoided since they alert users to them.

Some of the big players in the industry, such as Visa, MasterCard, and PayPal, widely employ artificial intelligence for fraud detection, which is refined constantly [16]. Such systems can develop their algorithms based on past data and emerging fraud strategies, which ensures their efficiency.

Merchants use AI-based fraud detection to protect their and clients' online and offline purchases. Artificial intelligence systems can identify the buying habits and tendencies of consumers so that retailers can counter fraud easily and in a timely manner.

Scope

Since security solutions for payment processing systems are a global concept, their application areas and potential future developments are as vast as the domains and industries.

E-Commerce Platforms

Promptly, the relevant features in the field of e-commerce include encryption, tokenization, and AI fraud detection to secure online transactions. Since consumers have shifted to online shopping and shifting more of their transactions online, their payment details must be secure. These technologies enhance data security and prevent multiple frauds and breaches, increasing service trust.

Mobile Payment Applications

Mobile payment apps have become very popular due to the increased availability of smartphones. Hence, encryption and tokenization are strategic in safeguarding transactions conducted via mobile wallets and payment applications [11]. AI-based fraud detection systems constantly check various transactions and alert the concerned authorities in case of any suspicious activity.

Point-of-Sale (POS) Systems

Like payment card processing, POS systems in retail environments also reap comparable advantages with these security measures. Tokens, created from the actual payment information, are used instead of the actual sensitive data to minimize the risks. Real-time detection of fraud minimizes fraud incidences at the point of sale.

Financial Institutions

Various banks and other financial institutions use these technologies to protect different payment facilities, which include online banking, ATM, and credit cards. AI has proved to be very helpful in identifying and addressing modern and complex frauds that seek to compromise the financial institution's systems and data [5].

Emerging Technologies

These security solutions are more comprehensive than conventional payment procedures. Cryptocurrencies and Blockchain transactions, which are relatively new practices, also require encryption for the security and anonymity of the transactions. Machine learning fraud detection can be scaled to prevent and detect fraud in these new payment models.

Future Advancements

These security solutions are likely to grow further as new types of digital payments are developed. More features that are likely to be developed in the future include better algorithms for fraud identification, improved forms of encryption, and better tokenization procedures. Keeping up with the new security threats and challenges that are ever emerging and for the stability of the payment processing systems, there will always be the need to invest in research and development.

Conclusion

Security is a common and vital aspect of payment processing systems that must be worked on and researched persistently. Encryption, tokenization, and AI-based fraud detection systems also provide a good solution for the security risks that endanger modern payment systems. Implementing these technologies helps secure the consumers' credit card data and decreases fraud vulnerabilities. Such helps develop trust among the masses in the modern online payment systems. Further advancements and innovations to counter the growing threats will be crucial in developing digital payment systems security.

References

[1] M. N. Alenezi, H. Alabdulrazzaq, and N. Q. Mohammad, "Symmetric Encryption Algorithms: Review and Evaluation study," International Journal of Communication Networks and Information Security (IJCNIS) , vol. 12, no. 2, pp. 256–272, Aug. 2020, Accessed: May. 07, 2023. [Online]. Available: https://www.researchgate.net/profile/Haneen-Alabdulrazzaq/publication/349324592_Symmetric_Encryption_Algorithms_Review_and_Evaluation_study/links/602acfa7a6fdcc37a82c0189/Symmetric-Encryption-Algorithms-Review-and-Evaluation-study.pdf

[2] W. Bai, M. Pearson, P. G. Kelley, and M. L. Mazurek, "Improving Non-Experts' Understanding of End-to-End Encryption: An Exploratory Study," IEEE Xplore, Sep. 01, 2020. https://ieeexplore.ieee.org/abstract/document/9229664/

[3] B. Lutkevich and M. Bacon, "end-to-end encryption (E2EE)," Security, Jun. 25, 2021, Available: https://www.techtarget.com/searchsecurity/definition/end-to-end-encryption-E2EE#:~:text=End%2Dto%2Dend%20encryption%20(E2EE)%20is%20a%20method,intended%20recipient%20can%20decrypt%20it.

[4] R. A. Alzahrani and M. Aljabri, "AI-based Techniques for Ad Click Fraud Detection and Prevention: Review and Research Directions," Journal of Sensor and Actuator Networks, vol. 12, no. 1, p. 4, Dec. 2022, DOI: https://doi.org/10.3390/jsan12010004.

[5] B. C. Rohith and N. Madhusundar, "Artificial Intelligence Based Credit Card Fraud Detection for Online Transactions Optimized with Sparrow Search Algorithm," International Journal of Performability Engineering, vol. 19, no. 9, p. 624, Jan. 2023, Available: https://www.ijpe-online.com/EN/article/downloadArticleFile.do?attachType=PDF&id=4807

[6] M. S. T, M. S. M. Rahim, F. Y. H. Ahmed, M. M. Hashim, and A. Zainal, "Hiding Financial Data In Bank Card Image Using Contrast Level Value And Text Encryption For Worthiness A Robust Steganography Method," International Journal of Advanced Science and Technology, vol. 29, no. 7, pp. 2783–2801, Jan. 2020, Accessed: May. 07, 2023. [Online]. Available: https://www.researchgate.net/profile/Mohammed-Hashim-4/publication/341651865_Hiding_Financial_Data_In_Bank_Card_Image_Using_Contrast_Level_Value_And_Text_Encryption_For_Worthiness_A_Robust_Steganography_Method/links/5ecd3fbd92851c9c5e5f2f2c/Hiding-Financial-Data-In-Bank-Card-Image-Using-Contrast-Level-Value-And-Text-Encryption-For-Worthiness-A-Robust-Steganography-Method.pdf

[7] J. M. Blanke, "Protection for 'Inferences Drawn': A Comparison Between the General Data Protection Regulation and the California Consumer Privacy Act," Global Privacy Law Review, vol. 1, no. Issue 2, pp. 81–92, Jun. 2020, DOI: https://doi.org/10.54648/gplr2020080

[8] S. Talwar, A. Dhir, A. Khalil, G. Mohan, and A. K. M. N. Islam, "Point of adoption and beyond. Initial trust and mobile-payment continuation intention," Journal of Retailing and Consumer Services, vol. 55, p. 102086, Jul. 2020, DOI: https://doi.org/10.1016/j.jretconser.2020.102086

[9] J. Wieringa, P. K. Kannan, X. Ma, T. Reutterer, H. Risselada, and B. Skiera, "Data analytics in a privacy-concerned world," Journal of Business Research, vol. 122, pp.915–925,Jan.2021,doi: https://doi.org/10.1016/j.jbusres.2019.05.005

[10] N. Morrow and N. Zarrebini, "Blockchain and the tokenization of the Individual: Societal implications," Future Internet, vol. 11, no. 10, pp. 1-20, Oct. 2019, DOI: https://doi.org/10.3390/fi11100220

[11] S. Agrawal, "Integrating Digital Wallets: Advancements in Contactless Payment Technologies," International Journal of Intelligent Automation and Computing, pp. 1–14, 2021, Available: https://research.tensorgate.org/index.php/IJIAC/article/download/111/105

[12] S. E. Cebeci, K. Nari, and E. Ozdemir, "Secure E-Commerce Scheme," IEEE Access, vol. 10, pp. 10359–10370, Jan.2022, doi: https://doi.org/10.1109/access.2022.3145030

[13] A. Sikri, S. Dalal, N. P. Singh, and D.-N. Le, " Mapping of e-wallets with features," Cyber Security in Parallel and Distributed Computing: Concepts, Techniques, Applications and Case Studies, pp. 245–261, 2019, Accessed: May. 07, 2023. [Online]. Available:https://www.researchgate.net/profile/Alisha-Sikri/publication/331993122_Mapping_of_e-

Wallets_With_Features/links/5cf0cdb9299bf1fb184bb00b/Mapping-of-e-Wallets-With-Features.pdf

[14] S. S. Ahamad, “A Novel NFC-Based Secure Protocol for Merchant Transactions,” IEEE Access, vol. 10, pp. 1905–1920, 2022,
doi: https://doi.org/10.1109/ACCESS.2021.3139065

[15] S. Sharma and A. A. Waoo, “Customer Behavior Analysis in E-Commerce using Machine Learning Approach : A Survey,” International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 10, no. 2, pp. 163–170, Mar. 2023, Accessed: May. 07, 2023. [Online]. Available: https://www.researchgate.net/profile/Akhilesh-Waoo-2/publication/369967977_Customer_Behavior_Analysis_in_E-Commerce_using_Machine_Learning_Approach_A_Survey/links/6436e13a609c170a13111400/Customer-Behavior-Analysis-in-E-Commerce-using-Machine-Learning-Approach-A-Survey.pdf

[16] V. Tretyakov and S. Golyatina, “Applying Big Data technologies to counter cyber fraud,” Revista Amazonia Investiga, vol. 11, no. 49, pp. 9–16, Feb. 2022. Available: https://www.amazoniainvestiga.info/index.php/amazonia/article/download/1869/2302