UDC: 004.8:338.48
343.85:343.53
DOI: 10.69899/limes-plus-en-24212-3253t
Original scientific work

APPLICATION OF ARTIFICIAL INTELLIGENCE IN DETECTING FRAUD IN TOURISM

***Ivan Trifunović*[1]**
Tourist Organization of Vrnjačka Banja, Vrnjačka Banja
***Žaklina Spalević*[2]**
Faculty of Tourism and Hospitality Management, Belgrade
***Dejan Rančić*[3]**
Faculty of Electronic Engineering, Niš
***Filip Marković*[4]**
Faculty of Technical Sciences, Kosovska Mitrovica
***Milan Simić*[5]**
RMIT University, Australia

Abstract: *Tourism has become a key sector of the economy in many countries during this century, offering immense potential for job creation and economic growth. The development of information technologies and artificial intelligence is transforming the tourism industry, enabling personalized experiences, travel optimization, and enhanced customer support. With the rise of online payments in tourism, the risk of various forms of fraud also increases.*

1 ivantrifunovic75@gmail.com
2 zspalevic@singidunum.ac.rs
3 dejan.rancic@elfak.ni.ac.rs
4 filip.markovic@pr.ac.rs
5 milan.simic@rmit.edu.au

Therefore, the role of artificial intelligence, particularly machine learning and deep learning is becoming increasingly important in detecting fraud and ensuring secure financial transactions in e-tourism. While artificial intelligence continues to improve the tourism industry, it also faces challenges related to online fraud, offering opportunities for enhanced customer support, personalized experiences, and improved efficiency while addressing security issues in online transactions.

Keywords: *tourism, artificial intelligence, online payments, machine learning, deep learning.*

INTRODUCTION

At the beginning of this century, tourism became one of the most dynamic sectors of economic activity worldwide, simultaneously representing a key job generator. Economically, tourism is an important factor in the recovery of national economies of countries with significant tourism resources that know how to properly use them. Considering the practically unlimited tourism resources, tourism is regarded as a sector with exceptional potential for long-term development. State tourism organizations play a crucial role as distributors of accurate, updated, and relevant information for potential tourists and the tourism industry as a whole. On the other hand, the state's role is to collect information and use it to formulate laws, policies, and strategies that support tourism development. The development of information technologies represents the future of the tourism industry, enabling fast distribution and efficient use of information. Owners of well-organized and trustworthy websites gain significant benefits. It is important to ensure the protection of users who access and purchase from such websites, which can be achieved through security and privacy measures provided by producers and distributors of tourism products via the internet, with state support to intervene in cases of non-compliance with national legislation (Nedelea & Bălan, 2010, p. 492).

The global tourism industry has experienced significant growth and attracted millions of travelers eager for new destinations and cultural experiences. However, a concerning and widespread phenomenon has emerged – fraud in tourism. Tourism fraud encompasses various deceptive and illegal activities targeting tourists, including fake services, scams, and identity theft. These activities pose significant threats to the financial well-being, personal safety, and overall experience of travelers.

Fraud in tourism takes various forms and exploits the vulnerability and trust of tourists who are often unfamiliar with the destinations they visit. These fraudulent activities range from misrepresentation of accommodations, tour packages, or attractions to fake online reservations and financial transactions. As a result, tourists face the consequences of fraud, which range from minor inconveniences to severe financial losses and concerns for personal safety (Corpuz, Manlutac, De Guzman, & Santos, 2023, p. 154).

Global perspectives on tourism fraud may vary, but common themes and issues are internationally recognized. Tourism fraud refers to various deceptive practices targeting tourists with the aim of unfairly obtaining money or personal data. This can include activities such as fake tours, identity theft, and cybercrime. With the rise of online bookings, the number of fraudulent websites and ads increases, leading to financial losses for tourists (Corpuz, Manlutac, De Guzman, & Santos, 2023, p. 154).

Artificial intelligence (AI) is significantly transforming the tourism industry by enabling personalized experiences, travel optimization, and enhanced customer support. AI algorithms assist in making decisions about destinations, transportation, accommodation, and activities, tailoring offers to the specific needs of tourists. At the same time, the development of digital technologies and the increase in online payments elevate the risk of financial fraud. The use of machine learning, deep learning, and other AI technologies is becoming crucial for recognizing and preventing fraud, thus protecting users and ensuring transaction security. This paper explores the role of AI in e-tourism and emphasizes the importance of AI in preventing fraud in online payments.

THE ROLE OF ARTIFICIAL INTELLIGENCE IN MODERNIZING THE TOURISM INDUSTRY

AI is particularly significant for travel and tourism for several reasons. Tourists face many decisions about their future travels, such as choosing destinations, transportation, accommodation, and activities. These decisions significantly impact their satisfaction during the trip. However, the vast number of available destinations, transportation means, accommodations, and activities creates an almost infinite number of options, requiring some form of assistance. Travel organizations and agents also face the challenge of finding travel packages tailored to the specific needs of users that best suit them. With a nearly unlimited number of potential clients, organizations must perfectly match supply and demand, a complex process suited to AI capabilities (Bulchand-Gidumal, Secin, O'Connor, & Buhalis, 2023, p. 1).

AI is increasingly impacting e-tourism, providing personalized experiences to travelers, faster responses to inquiries, and travel optimization. AI algorithms play a growing role in the development and enhancement of e-tourism. They enable process automation, the analysis of large volumes of data, and the provision of personalized services to tourists. However, while AI brings many advantages, its application also presents challenges, including ethical and security aspects that must be carefully considered (Spalević, Milosavljević, & Marković, 2024, p. 209).

AI is significantly transforming the tourism industry through various aspects (Prahadeeswaran, 2023, p. 12), such as:

Customer support: Chatbots and virtual assistants enable quick responses to inquiries, personalized recommendations, and booking assistance, improving the efficiency and responsiveness of customer support.

Marketing and personalization: AI analyzes large amounts of data to understand traveler preferences, enabling the creation of targeted marketing campaigns and dynamic pricing strategies to optimize revenue.

Demand forecasting: AI algorithms predict demand for tourist destinations, accommodation, and services, helping optimize resources, prices, and inventories.

Sustainable tourism: AI systems help manage energy consumption, and waste management, and promote eco-friendly transportation options, reducing the ecological footprint of tourism.

Smart destinations: AI technologies enable efficient traffic management, crowd control, and information dissemination to visitors, enhancing the visitor experience in real time.

Translation: AI-powered translation tools remove language barriers for international travelers, making tourism more accessible.

Cultural heritage preservation: Aplikacije AI applications like augmented reality (AR) and virtual reality (VR) help preserve and promote cultural landmarks through interactive content.

Crisis management: AI systems monitor weather conditions and natural disasters, helping ensure traveler safety and continuity of tourism operations.

Accessibility: AI improves accessibility for travelers with disabilities through voice-activated services and navigation apps.

Ethical considerations: As AI becomes more prevalent in tourism, it is important to address issues of data privacy, algorithmic bias, and job displacement to ensure fairness and sustainability.

AI continues to reshape the tourism industry, enhancing customer support, personalizing experiences, promoting sustainability, and improving efficiency.

TOURISM AND ONLINE PAYMENTS

Tourism and online payments have become closely linked with the development of digital technology and the growing popularity of travel. Online payments allow tourists to book accommodations, purchase airline tickets, pay for tours and activities, and various services and products during their travels, all via the Internet. This has brought numerous advantages, including greater convenience, speed, and ease in travel planning and booking processes, as well

as a wider choice of offers and destinations available to travelers worldwide. Travelers can explore different options, compare prices, and customize their trips to their needs, all from the comfort of their homes or with the help of a smartphone. However, the increase in online payments in tourism also comes with an increased risk of fraud. Fraudsters may attempt to exploit vulnerabilities in online payment systems to commit fraud, including identity theft, false advertising of tourist offers, or misrepresentation of services.

In recent years, the number of online payments has dramatically increased globally. With the growing popularity of e-commerce, mobile payment apps, and digital wallets, consumers are increasingly using the Internet for their financial transactions. However, along with this rise comes an increased risk of online fraud.

The digital payments market had a global transaction value of $8.35 trillion in 2022 and, according to Statista – Market Insights, is the largest market within FinTech. The digitization of financial services is associated with disruptive changes in the industry concerning the billing process (online purchases) and the payment process at points of sale (offline purchases). Digital payments can therefore be considered the next evolutionary step that enables further financial services and replaces traditional, outdated payment methods (from cash and credit/debit cards to mobile and digital wallets). When it comes to digital payments, China is currently the largest market in the world, with a transaction value of $3.639 trillion in 2022 (Statista, 2023).

According to the National Bank of Serbia, the purchase of goods and services via the Internet is becoming increasingly popular in the Republic of Serbia. In the first quarter of 2023, the number of dinar transactions via the Internet amounted to 8.7 million, representing an increase of 25.76% compared to the same period the previous year. The value of these transactions was 24 billion dinars, an increase of 38.11% compared to the first quarter of 2022. Additionally, in the same period, the number of transactions executed in euros increased by 29.96%, from 1.6 million to 2 million transactions, while their value rose by 36.49%, from 70.4 million euros to 96 million euros. Regarding transactions

executed in US dollars, in the first quarter of 2023, there was an increase in both the number of transactions, by a quarter (from 1.2 to 1.5 million), and their value, by 8% (from $34.2 million to $37 million), compared to the same period the previous year (National Bank of Serbia, 2023).

In 2022, e-commerce merchants worldwide faced various types of fraud, with social engineering tactics such as phishing, pharming, and whaling being the most common (Statista, 2024).

Phishing is a form of social engineering aimed at stealing an individual's personal information. It is usually carried out via fake emails that request the entry of sensitive information on a fraudulent website. These fake sites are designed to look authentic, posing a threat to users both at home and at work. Unlike phishing, which uses email for communication, pharming uses advanced techniques like stealthy DNS servers to manipulate traffic and redirect users to fraudulent websites. Criminals try to alter DNS servers to reroute users to fake locations. Pharming attacks often succeed on unprotected computers. Spear phishing is a form of phishing that targets specific individuals or organizations. Attackers tailor emails and SMS messages to target specific persons. Whaling is a particular form of spear phishing aimed at high-profile individuals such as executives (Issuu, 2021).

Thus, the aforementioned techniques target human errors, attempting to deceive individuals into sharing information or clicking on links that install malicious software on their devices. First-party misuse, such as friend fraud and refund fraud, ranked second, followed by card testing and identity theft. As if that weren't enough, online merchants have identified new fraud trends, including cases where fraudsters provide services that facilitate fraudulent activities for clients. Given that fraudsters are employing increasingly sophisticated strategies, it has become necessary for online merchants to effectively enhance their fraud prevention measures and counterattacks against these threats. A study showed that nearly three-quarters of companies planned to increase their budgets for fraud prevention in 2023. In 2022, tools such as Card Verification Number (CVN) checks and identity verification were the most commonly used for

fraud prevention. However, to strengthen their fraud management strategies and protect their businesses, online merchants are increasingly focusing on improving fraud analytics and the accuracy of automatic detection. Fraud affects the user experience. If merchants witness the financial impact of cybercrime, customers are not far behind them. In recent years, the percentage of online fraud victims who suffered financial losses has consistently remained above 70%. Since websites serve as the main channel for online fraud, this scenario inevitably damages merchants' reputations and undermines consumer trust. In 2022, seven out of ten global e-commerce users expressed a preference for payment methods that do not share their data with merchants, while nearly 60% expressed greater concern about online fraud during payment compared to the previous year. A study published a year earlier indicated that providing fraud protection could encourage the use of e-commerce. In the United States alone, about eight out of ten consumers would shop online more frequently if they were provided protection from these threats (Statista, 2024).

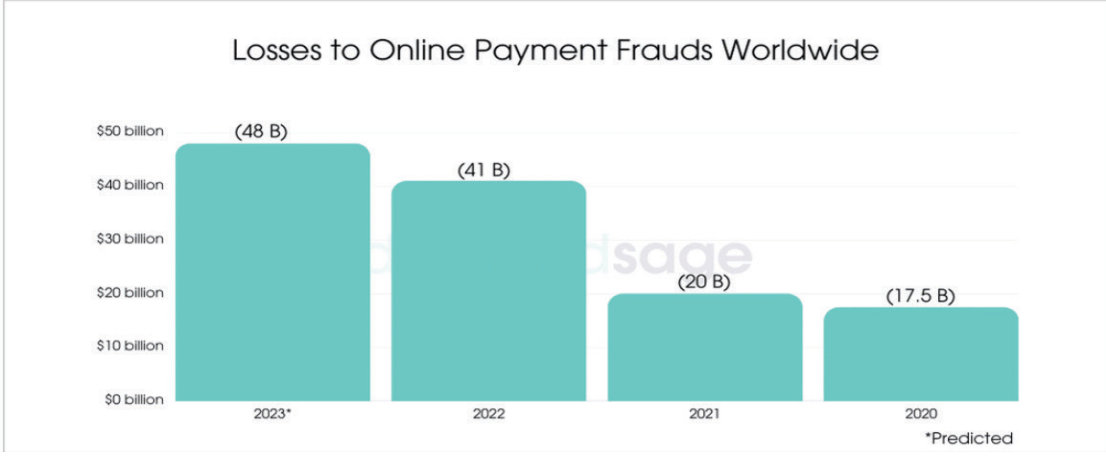

Figure 1. Losses due to online payment fraud worldwide (Ddemandsage, 2023)

Considering the growing popularity of online shopping and the increased number of transactions conducted electronically, the importance of AI in fraud detection is becoming ever more significant. With a greater number

of transactions comes a higher risk of fraud, and traditional fraud detection methods may be insufficiently effective or outdated. Thus, in the digital world, technology connects us and facilitates the exchange of information and services. However, with this progress comes new dangers. Fraud in financial transactions is becoming more frequent, causing significant losses and damage in the service sector. In the e-tourism sector, travelers often make online payments for accommodation, tickets, and other tourist services. Fraudulent activities are not limited to online transactions but can also occur in traditional offline payments. Fortunately, advanced technologies such as machine learning and AI, as well as classification algorithms, can help address these issues (Farzana, Onti, Islam, Islam, and Shatabda, 2023, p. 368).

ARTIFICIAL INTELLIGENCE IN FINANCIAL FRAUD PREVENTION

Many technologies we use in everyday life, from smart assistants (Google Assistant, Siri, etc.) to robotics and from facial recognition systems to autonomous vehicles, are examples of AI (Lu, Li, Chen, Kim, and Serikawa, 2018, p. 368). What makes these technologies AI are the components that comprise them. AI essentially encompasses multidisciplinary technologies, including machine learning, deep learning, computer vision, natural language processing, artificial neural networks, and expert systems (Hangl, Behrens, and Krause, 2022, p. 63).

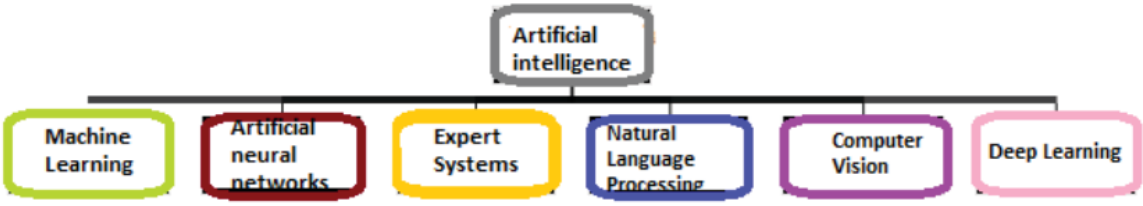

Figure 2. Sub-technologies of artificial intelligence (Hangl, Behrens, and Krause, 2022, p. 63)

Each of these sub-technologies has specific characteristics and applications that significantly contribute to the advancement of AI (Durmaz and Başer, 2023, p. 21).

Machine learning is the foundation of AI and encompasses algorithms that enable computers to learn and improve their performance based on experience. Machine learning is used in various industries for tasks such as fraud detection, credit scoring, recommendation systems, and medical diagnostics. Machine learning algorithms analyze large amounts of data, recognize patterns, and make decisions or predictions without being explicitly programmed for each task. This technology allows computers to become more autonomous and to adapt to new situations and information (Janiesch, Zschech, and Heinrich, 2021).

Deep learning, the most popular subfield of machine learning, uses multilayer neural networks to process complex information such as sound and images. Deep learning enables computers to learn from unlabeled data and extract high-level abstract information from it (Hao, 2019, p. 1).

Artificial neural networks are mathematical models inspired by the structure of the human brain and composed of interconnected artificial neurons that process information. The ambition to create a system that simulates the human brain spurred the initial development of neural networks. In 1943, McCulloch and Pitts attempted to understand how the brain could produce highly complex patterns using interconnected basic cells called neurons. The McCulloch-Pitts neuron model, known as the MCP model, laid the foundation for the later development of artificial neural networks (Voulodimos, Doulamis, Doulamis, and Protopapadakis, 2018, p. 1). These networks are capable of complex tasks such as pattern recognition, data classification, and prediction. Artificial neural networks are particularly useful in areas where traditional statistical techniques are not sufficiently precise, such as modeling financial time series and exchange rate forecasts (Abraham, 2005, p. 901).

Computer vision is the science that studies how machines can "see" using computers and cameras. This technology enables computers to perceive, identify, measure, and track objects in the real world. Computer vision is used in

various applications, from facial recognition systems to automatic classification of microscopic images of cells. For example, the smart store "Amazon Go" uses computer vision technology based on deep learning to track customers and their purchases without the need for cashiers (Lu, 2019, p. 1).

Natural language processing (NLP) involves programming computers to properly process and understand human language. NLP facilitates communication between humans and machines, allowing computers to analyze, understand, and generate human language. Examples of this technology include chatbots that mimic human conversation and respond to customer inquiries. NLP has various applications, including text translation, sentiment analysis, and automatic text generation (Jain, Kulkarni, and Shah, 2018, p. 161).

Expert systems are intelligent computer systems that use expert knowledge to solve problems at a human level. These systems model the ability of humans to solve complex problems using predefined rules and knowledge bases. One of the first expert systems, "Dendral", was developed at Stanford University for chemical analysis of Martian soil. Expert systems are used in medicine, engineering, finance, and many other fields where expert knowledge is needed for decision-making (Lucci and Kopec, 2016, p. 271).

Credit card fraud is an easy and attractive target. E-commerce and many other online sites have increased online payment methods, thereby increasing the risk of online fraud. With the rising fraud rates, researchers have begun to use various machine-learning methods to detect and analyze fraud in online transactions (Dornadula and Geetha, 2019, p. 631). Some of these methods include Decision Tree, Logistic Regression, Random Forest, Ada Boost, XGBoost, Support Vector Machine (SVM), and LightGBM (Lebichot, Paldino, Bontempi, Siblini, He-Guelton, and Oble, 2020, p. 785).

The application of AI and its aforementioned sub-technologies can significantly enhance the tourism industry's ability to detect and prevent fraud, thereby increasing the security and trust of travelers. Here, we will emphasize machine learning and deep learning, which have been the most analyzed in the literature. Machine learning and deep learning algorithms can analyze

large volumes of transactions, reservations, and user behavior data to identify irregularities and anomalies that may indicate fraud. For example, they can detect frequent changes in travel reservations, unusually high expenses, or frequent purchase attempts from different locations, which may indicate suspicious activity.

Deep learning, including algorithms like autoencoders, plays a key role in improving security and trust in the tourism industry. Autoencoders are a special type of neural network used for anomaly detection, including credit card fraud. The main feature of autoencoders is encoding input data into a smaller number of features and then reconstructing them back into output data with the aim of accurately reconstructing the input (Misra, Thakur, Ghosh, and Saha, 2020, p. 254).

The autoencoder process consists of two basic parts (Pumsirirat and Yan, 2018, p. 18):

Encoder: The part of the network that compresses and reduces the dimensionality of the input data into a smaller number of features.

Decoder: The part of the network that reconstructs the original data from the compressed features.

When using the autoencoder model, the backpropagation algorithm is applied for error reconstruction. This algorithm adjusts the network weights to minimize the difference between the actual and reconstructed data.

The process of credit card fraud detection involves the following steps (Pumsirirat and Yan, 2018, p. 18):

Transaction collection: The issuing bank sends transactions to the user's bank with details such as amount, date, time, and location of credit card usage.

Behavior validation: Fraud detection systems use consumer profiles from the database to validate credit card behavior. Autoencoders train models using transaction history data and then use these models to validate new transactions.

Functionality of autoencoders: Autoencoders are designed to efficiently identify patterns and data structures without requiring pre-labeled transactions for training. This approach allows autoencoders to automatically detect

anomalies and irregularities in data, thereby contributing to increased security in the tourism industry.

The advantages of using autoencoders in fraud detection include (Pumsirirat and Yan, 2018, p. 18):

Unsupervised learning capability: Autoencoders do not require labeled data, enabling the use of large amounts of unlabeled data for training.

Efficiency in anomaly detection: Autoencoders are efficient in identifying patterns that deviate from normal behavior, which is crucial for identifying potential fraud.

Adaptability: They can be applied to different datasets and easily adapt to new types of fraud as they emerge.

In the tourism industry, autoencoders represent a key innovation promising to enhance the security and trust of travelers. Their ability to learn from unlabeled data enables the efficient use of a wide range of unlabeled information for training, while providing exceptional efficiency in detecting irregularities. This flexibility allows fraud detection systems to adapt and evolve to confront new challenges in the tourism world. Through such technological advancements, the industry can provide a safer travel experience and ensure that every traveler enjoys their journey without concerns about the security of their transactions.

CONCLUSION

Tourism is a sector that has experienced significant growth and development in recent decades, becoming a vital branch of many countries' economies. However, with this growth, new challenges have arisen, with one of the most significant being fraud in tourism. Fraudulent activities, especially in online payments, pose a serious threat to both financial stability and the reputation of the tourism industry.

In this context, the application of artificial intelligence has proven to be a crucial strategy for combating fraud and improving the security of online transactions. Through various techniques such as machine learning, deep learning,

and artificial neural networks, artificial intelligence can identify irregularities, recognize patterns, and automatically respond to potential fraudulent activities. Among all these techniques, deep learning stands out as one of the key technologies in combating fraud in the tourism industry, as it can analyze complex datasets and identify hidden patterns. This type of artificial intelligence enables systems to autonomously recognize the characteristics of fraudulent activities and adapt to new threats without the need for explicit programming.

The application of deep learning enables tourism companies to effectively detect suspicious activities and prevent financial losses, while also enhancing the traveler experience. This technology allows real-time monitoring of transactions and rapid response to potential threats, ensuring the security and reliability of tourism services for all users.

Artificial intelligence plays a crucial role in detecting fraud in tourism and improving the security of online payments, while also contributing to the modernization and efficiency of the tourism industry. With proper implementation and management, artificial intelligence can be a powerful force guiding tourism towards a more sustainable and secure future.

REFERENCES

1. Abraham, A. (2005). Handbook of Measuring System Design. 129 Artificial Neural Networks, Part 8. Elements: B – Signal Conditioning. John Wiley & Sons, Ltd. 901–908.
2. Bulchand-Gidumal, J., Secin, E. W., O'Connor, P., & Buhalis, D. (2023). Artificial intelligence's impact on hospitality and tourism marketing: exploring key themes and addressing challenges. Current Issues in Tourism, 1–18.
3. Corpuz, R. R. N., Manlutac, A. C., De Guzman, S. M. R., & Santos, C. J. P. (2023). Mitigating Tourism Fraud In Northern And Central Luzon: Understanding Factors Affecting Domestic Tourists And Enhancing

Trust In Destination Experiences. EPRA International Journal of Multidisciplinary Research (IJMR), 9(11), 154–168.

4. Ddemandsage. (2023). 59 eCommerce Fraud Statistics For 2024 (Latest Data). Retrieved from https://www.demandsage.com/ecommerce-fraud-statistics/
5. Dornadula, V. N., & Geetha, S. (2019). Credit Card Fraud Detection using Machine Learning Algorithms. Procedia Computer Science, 165, 631–641.
6. Durmaz, Y., & Başer, M. Y. (2023). A Systematic Literature Review on Artificial Intelligence Applications in Tourism Marketing. International Journal of Research in Business Studies and Management, 10(1), 21–30.
7. Farzana, N., Onti, Y. L. H., Islam, T., Islam, M., & Shatabda, S. (2023). Fraud Detection Analysis of Revenue and Trip Transaction. 1–8.
8. Hangl, J., Behrens, V. J., & Krause, S. (2022). Barriers, Drivers, and Social Considerations for AI Adoption in Supply Chain Management: A Tertiary Study. Logistics, 6(3), 63.
9. Hao, Z. (2019). Deep learning review and discussion of its future development. MATEC Web of Conferences, 277, 02035: 1–7.
10. Issuu. (2021). Phishing, pharming, whaling? Common data attacks and how to prevent them. Retrieved from https://issuu.com/castillians/docs/castille_newsletter_march_2021/s/12015870#google_vignette
11. Jain, A., Kulkarni, G., & Shah, V. (2018). Natural Language Processing. International Journal of Computer Sciences and Engineering, 6(1), 161–167.
12. Janiesch, C., Zschech, P., & Heinrich, K. (2021). Machine learning and deep learning. Electronic Markets.
13. Lebichot, B., Paldino, G. M., Bontempi, G., Siblini, W., He-Guelton, L., & Oble, F. (2020). Incremental learning strategies for credit cards fraud detection: Extended abstract. International Conference on Data Science and Advanced Analytics, 785–786.

14. Lu, H., Li, Y., Chen, M., Kim, H., & Serikawa, S. (2018). Brain Intelligence: Go beyond artificial intelligence. Mobile Networks and Applications, 23(2), 368–375.
15. Lu, Y. (2019). Artificial intelligence: a survey on evolution, models, applications and future trends. Journal of Management Analytics, 6(1), 1–29.
16. Lucci, S., & Kopec, D. (2016). Artificial Intelligence in the 21st Century, A Living Introduction. (2nd ed.). Mercury Learning and Information, 271–272.
17. Misra, S., Thakur, S., Ghosh, M., & Saha, S. K. (2020). An Autoencoder Based Model for Detecting Fraudulent Credit Card Transaction. Procedia Computer Science, 167, 254–262.
18. Narodna banka Srbije. (2023). Saopštenje o podacima u vezi s pružanjem platnih usluga i izdavanjem elektronskog novca u prvom tromesečju 2023. godine. Retrieved from https://www.nbs.rs/sr/scripts/showcontent/index.html?id=18941
19. Nedelea, A., & Bălan, A. (2010). E-tourism and Tourism Services Consumer Protection. Amfiteatru Economic, 12(28), 492–503.
20. Prahadeeswaran, R. (2023). A Comprehensive Review: The Convergence of Artificial Intelligence and Tourism. International Journal for Multidimensional Research Perspectives, 1(2), 12–24.
21. Pumsirirat, A., & Yan, L. (2018). Credit Card Fraud Detection using Deep Learning based on Auto-Encoder and Restricted Boltzmann. International Journal of Advanced Computer Science and Applications, 9(1), 1–25.
22. Spalević, Ž., Milosavljević, B., & Marković, S. (2024). Legal Basis of Educational Processes of Artificial Intelligence Algorithms in E-tourism. International Journal of Cognitive Research in Science, Engineering and Education, 12(1), 209–217.
23. Statista. (2023). Top 100 companies: Online Payment. Preuzeto sa https://www.statista.com/study/140117/top-100-companies-online-payment/

24. Statista. (2024). E-commerce fraud - statistics & facts. Preuzeto sa https://www.statista.com/topics/9240/e-commerce-fraud/#topicOverview
25. Voulodimos, A., Doulamis, N., Doulamis, A., & Protopapadakis, E. (2018). Deep Learning for Computer Vision: A Brief Review. Computational Intelligence and Neuroscience, 7068349, 1–13.