# AI AND CYBERSECURITY IN E-COMMERCE: HOW AI INTEGRATION AFFECTS DATA PROTECTION

Emilija Jovanović[1]*,
[0009-0003-7007-6537]

Mladen Veinović[1],
[0000-0001-6136-1895]

Miloš Jovanović[2]
[0009-0008-9032-8195]

[1]Singidunum University, Belgrade, Serbia

[2]Faculty of Mechanical and Civil Engineering in Kraljevo, University of Kragujevac, Kragujevac, Serbia

Abstract:

Every day, artificial intelligence sets significant innovative changes in all fields. Technological innovations introduced by AI have a positive effect on the protection of users in cyber security. Using data analysis, AI can quickly recognize threats and identify signs for early intervention. AI has a crucial role in protecting user accounts, detecting illegal transactions and preventing financial fraud in the sphere of e-commerce.

Despite all the benefits, the use of artificial intelligence also brings problems, such as false positive results resulting from errors of the machines themselves, and high implementation costs. The fact that must not be ignored is that the human factor is still crucial despite everything.

The paper focuses on exploring the application of artificial intelligence in e-commerce cyber security, particularly in the detection of suspicious transactions. An experimental model of Random Forest machine learning algorithms was used to evaluate suspicious transactions in e-commerce. The paper highlights the advantages and challenges of applying AI, emphasizing the importance of integrating intelligent systems and human analysis, which achieves effective and safe protection of the digital space.

Keywords:

E-commerce, AI, Cybersecurity, Data Protection.

## INTRODUCTION

The development of electronic commerce in the first decades of the 21st century brought numerous benefits to both consumers and companies, providing faster and easier shopping, significant improvement of global business and automation of sales processes. However, the development of electronic commerce has been accompanied by an increase in cyberattacks.

Traditional data protection methods, such as encryption and multi-factor authentication, have not been sufficient in recent years to fully protect user data from attacks using automated tools and artificial intelligence. For these reasons, AI is increasingly being used as an important technology in cyber security, enabling faster and easier detection of threats, proposing security measures according to potential threats and improving data protection in real time.

Correspondence:
Emilija Jovanović

e-mail:
ejovanovicrs@gmail.com



DOI: 10.15308/Sinteza-2025-241-246

This paper explores how the application of artificial intelligence can improve cyber security in e-commerce, with a special focus on protecting user data and preventing potential cyberattacks. By analyzing modern AI technologies, we concluded that machine learning algorithms, anomaly detection and user behaviour monitoring identify early threats, automate the response to potential threats and improve security standards.

Also, the paper will address the topic of challenges and limitations of the application of artificial intelligence in cyber security, with special reference to ethical dilemmas, regulatory obstacles and multiple risks. A special emphasis will be on adapting AI technologies to current security frameworks, such as NIST and ISO standards, to ensure more adequate data protection and strengthen user confidence in the electronic trading platforms themselves.

The main task of this paper is to show the advantages and disadvantages of the application of artificial intelligence, as well as to give an insight into possible challenges during the implementation of artificial intelligence in cybersecurity. [1]

## 2. CYBER-SECURITY RISKS IN E-COMMERCE

### 2.1. TRENDS IN CYBER-ATTACKS

The digitalization of business and the increasing number of online transactions have contributed to the increase in the number of cyberattacks. Research has shown that a large number of cyberattacks occurred worldwide in one day, with the majority of them targeting e-commerce platforms, banking systems and financial sectors. Nowadays, innovative methods are used to steal data and financial assets, and the most vulnerable sectors are healthcare, logistics, retail and financial institutions. Companies that do not use advanced data protection methods are in great danger, which is why more and more investments are being made in advanced protection systems to reduce the risk of potential cyberattacks. [2]

### 2.2. TYPES OF CYBERATTACKS

Nowadays, protecting online stores from cyber-attacks is an increasing challenge. Hackers skillfully use various modern methods to compromise the security of data and financial activities.

Phishing is considered one of the most common cyber-attacks. In order to obtain sensitive data, such as passwords, credit card numbers or personal information, attackers use fake e-mail addresses, messages or websites. Mostly, these attacks rely on social momentum, using well-known brands or institutions that have gained user trust and thus encourage them to take action. Innovative forms of phishing, such as spear phishing, use personalized messages to target individuals or organizations in order to carry out a successful attack.

A serious threat is DDoS (Distributed Denial-of-Service) attacks, because the servers are occupied by a large number of requests and thus prevent legitimate users from accessing it. These attacks result in a major financial crash, reduce trust and damage the company's reputation. To carry out this type of attack, botnet networks - networks of compromised computers - are used, which generate a large amount of content and destabilize the system.

Malware, malicious software, violates the protection of user data, redirects transactions or takes over system management. Malicious programs such as viruses, trojans, ransomware and spyware are used to carry out such an attack. They are mostly spread through infected e-mails, fake advertisements or downloaded files. Sensitive information such as phone numbers, credit card numbers and passwords can be compromised through the use of malware, directly compromising the security of both buyers and sellers. [3]

### 2.3. REGULATORY FRAMEWORK: OVERVIEW OF NIST AND ISO DATA PROTECTION STANDARDS

To secure data, organizations apply a regulatory framework for data protection that includes various standards and guidelines. The two most important sets of standards in the field of data protection are NIST (National Institute of Standards and Technology) and ISO (International Organization for Standardization) standards. These standards serve to help when implementing systems for effective data protection as well as systems that provide data security.

NIST is an American agency that develops standards, guidelines, and methods in various fields. These standards are mainly applied to federal information systems in the United States but are also applicable in a wider range of sectors. ISO is an international organization that develops global standards for various industries. The ISO standard is more globally accepted regarding security, but NIST is also used more in technical implementation.

# 3. THE IMPACT OF ARTIFICIAL INTELLIGENCE IN E-COMMERCE CYBER SECURITY

## 3.1. HOW DOES AI HELP DETECT AND PREVENT ATTACKS?

AI (artificial intelligence) is an integral part of detecting and preventing attacks in cyber security today. Artificial intelligence and machine learning are winning techniques as they enable systems to detect threats in real time, respond and also improve security. Traditional security systems use static definitions and signals of attack types, which are often effective against new but standard threats. AI, in this way, enables security tools to learn from huge data sets and identify patterns that indicate threats, long before attacks are actually known.

Real time analysis of large amounts of data is one of the key strengths of artificial intelligence in cybersecurity. In this way, faster detection of threats is possible due to the recognition of unusual activities, such as unusual access to data, variations in network traffic or unusual changes in user behaviour. The ability to stop attacks in their initial stages can greatly reduce the damage that attackers can inflict.

Automated analysis and classification of attacks are enabled by artificial intelligence. This means that the response to potential threats can sometimes be accelerated. In this case, artificial intelligence will monitor the network. When it detects an attack, it will act immediately, however necessary to meet those challenges. This can mean blocking access to the system, separating infected devices from uninfected parts, and redirecting suspicious traffic elsewhere.

Data encryption also benefits from the use of artificial intelligence. The integration of advanced AI algorithms into encryption helps to detect and prevent potential vulnerabilities in data protection systems, so that data is truly protected and attackers cannot find loopholes in existing protection methods.

## 3.2. KEY AI METHODS

### *3.2.1. Anomaly detection*

Anomaly detection in security and protection is where artificial intelligence is particularly useful. By recognizing unusual patterns in the data, it is possible to detect potential threats. Traditional security systems are based on pre-defined correct and known threats, but this is not enough because different attack methods are evolving very quickly.

AI and machine learning can indirectly analyze user behaviour, and identify suspicious activities even through abnormal changes in activity or unusual transactions.

One of how AI contributes to the detection of anomalies is through User Behaviour Analytics (UBA), that is, the analysis of user behaviour. For example, machine learning algorithms can track a user's normal ways of using systems and applications, noting their usual activity patterns. The system can monitor login time, IP address, location and device from which the user connects, as well as typical user operations: creating new files or modifying old ones. When there is a sudden change in this pattern, that is, if any deviation from these habits is observed - for example, when a user logs in from an unknown place at an unusual time one day or suddenly tries to download a very large file - the AI can generate an alert, temporarily lock the account and require additional authentication as necessary. [4]

### *3.2.2. Behavioural authentication*

Biometric authentication is all about analysing and measuring deviations in human behaviour to verify a specific individual. While conventional biometrics are based on something that a user has (fingerprint, iris scan, or facial recognition), behavioural biometrics analyze the way that a user accesses a device. Each individual demonstrates a unique set of behaviour patterns that can be quantified, making them an ideal security instrument. [5]

#### *3.2.2.1. Dynamics of typing on the keyboard*

The typing style of a person can identify them. The AI assesses elements including typing rhythm, keystroke speed and the time between pressing and releasing a key (known as "time of flight"). Every user will have a unique text input pattern and any deviation from the normal one could indicate a breach.

#### *3.2.2.2. Mouse movement and touchpad interaction*

Mouse movements also depend on the way a user moves it, the speed of the movement, how it moves — in a moon or more smooth, even pace — the number of clicks and their precision can prove to be unique elements of your identity. AI can identify these patterns and look for deviations from them to find a possible hacking attempt.

*3.2.2.3. Gait and movement patterns*

Smartphones and wearables utilize sensors to determine how a user moves, regarding stride length, speed of walking, and body posture. These patterns are fairly stable, and deviations from them could be a signal of fraudulent behaviour or that a particular device has been compromised.

*3.2.2.4. Characteristics of speech*

Voice recognition system identifies the user using tonality, intonation, accent and rhythm of speech. This process is commonly used in voice-activated systems, like assistants or banking services, where it will allow the system to recognize its user without additional passwords.

*3.2.2.5. Touch and swipe patterns*

On smartphones and tablets, the way a user touches the screen — pressure strength, swiping speed and scrolling patterns — can provide an added layer of authentication. And that's the reason why it's very hard to fake this data as each user has its own way of interacting with the screen and it makes the system very secure.

By combining these methods, behavioural authentication drastically increases the level of protection and enables early detection of suspicious activities and suppression of unauthorized access. [6]

## 4. EXPERIMENTAL TESTING OF AI MODELS IN THE DETECTION OF SUSPICIOUS TRANSACTIONS IN E-COMMERCE

The experiment was carried out to examine the possibility of applying artificial intelligence in the detection of suspicious transactions in e-commerce, all based on the analysis of significant parameters such as the user's location, device, purchase time and transaction amount.

To experiment, a machine learning model was used that recognizes transactions whether they are suspicious or not. The data is generated based on real scenarios in e-commerce, where different patterns are simulated. The model analyzes four key factors:

1. **User location** - If the user has made several transactions from one location, and a new transaction comes from another (e.g. from another country), this can be an indicator of potential fraud.
2. **The device from which the transaction was made** - A sudden change in the device from which the transaction was mainly made can signal an abused account.
3. **Time of transaction** – Transactions that occur at unusual times of day, such as late at night, can potentially be risky.
4. **Purchase Amount** – Unexpected and significant changes in transaction value may indicate fraudulent activity.

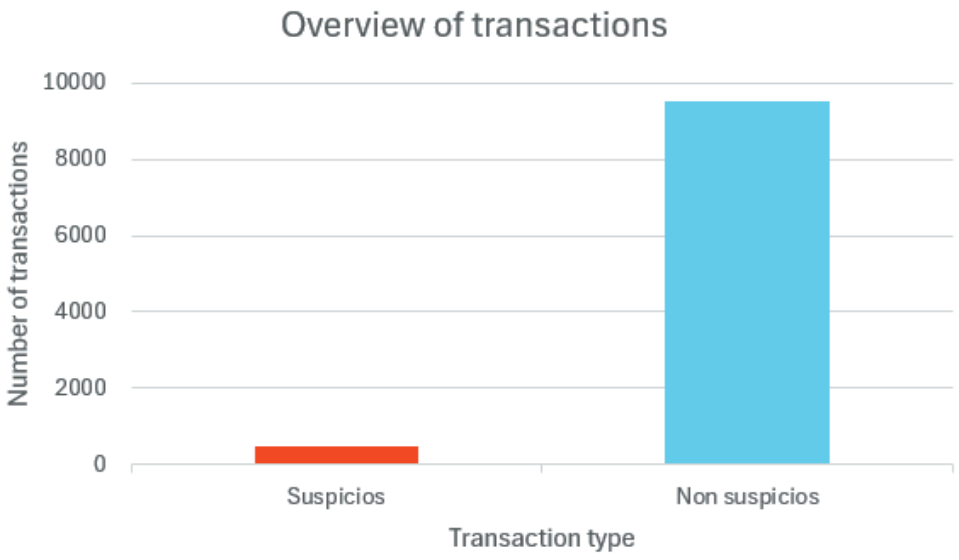


**Figure 1.** Overview of transaction

To recognize transactions as suspicious or not, the Random Forest algorithm was used, which is known for its ability to recognize complex patterns in data. The model was implemented in the Python programming language using the scikit-learn libraries for machine learning and pandas for data processing. A synthetic dataset of 10,000 generated transactions was used to train the model, of which about 5% were identified as potentially suspicious. The dataset was constructed to simulate real-world e-commerce conditions, including deliberately inserted anomalies so that the model could recognize illogicality.

After training, the model was evaluated for accuracy and responsiveness. Figure 1 shows the result visualized through a chart of transactions. This approach enables the automated recognition of potential fraud in real time, contributing to greater platform security and reducing financial risks associated with unauthorized transactions.

## 5. LIMITATIONS AND CHALLENGES OF IMPLEMENTING AI IN CYBERSECURITY

AI has much to offer cybersecurity, but implementing it is far from simple. Beyond technical limitations, organizations may face ethical, legal and operational challenges that can stall the effective integration of AI in data protection.

### 5.1. RESULTS FOR FALSE POSITIVES AND FALSE NEGATIVES

AI systems in cyber security also face the challenge of threat detection accuracy. If AI raises too many false alarms (false positives), security teams will begin to disregard notifications. If the AI fails to detect certain threats (false negatives), attackers can exploit the system with impunity.

### 5.2. LIMITATIONS IN MODEL TRAINING

An AI system's efficacy directly correlates with the quality of the data it is fed. AI can make mistakes if the data provided to it is not suitable or is incomplete, outdated or biased. Furthermore, cyberattacks are continually changing, so models have to be updated and adjusted to new threats in real time.

### 5.3. AI AS A TARGET OF ATTACK

Attackers are increasingly attempting to hack AI systems, to deceive or compromise them. One of the techniques is "data poisoning", where wrong data is introduced into the system, which leads the AI to incorrect conclusions.

### 5.4. HIGH COST

Building AI solutions for cybersecurity needs a massive investment in infrastructure, employee training, and continual model development.

### 5.5. PRIVACY AND REGULATION

AI-based cybersecurity systems typically deal with a large volume of personal and sensitive data, which can, in turn, create privacy and regulatory concerns with laws such as GDPR. A corresponding legal framework is necessary to prevent possible abuses or over-collection of data.

### 5.6. OVERVIEW OF LIMITATIONS AND CHALLENGES

However, while AI will continue to drive a major evolution in the cyber security landscape, human skills cannot be fully replaced as analysis, prioritisation and response to complex threats will always require human decision-making. AI can automatically identify suspicious activity, but human expertise is needed to analyze data, identify new types of attacks and make decisions about how to protect systems.

The downside of AI systems is that they are only as good as the data they are trained on. When the AI encounters threats that were unknown to it during training, it is the human category that can identify the problem and change the security strategy to mitigate this threat.

The human factor proves central to ethical and legal issues in cyber security, as well as technical aspects. Data privacy, regulation and ethical challenges are deeply human decisions that cannot be handed over to algorithms.

To that end, the best way to achieve cybersecurity is not with AI or humans alone, but with both. Coming together, automated analysis with human expertise will enable faster, more accurate and more secure data protection in an increasingly complex digital environment. [7]

## 6. CONCLUSION

This paper shows the importance of artificial intelligence in the field of cyber security. All benefits such as anomaly detection, and behavioural authentication, contribute to a significant improvement in the security of digital systems. Specifically in e-commerce, AI has the ability to analyze massive amounts of data in real time, revealing the potential for an attack.

However, despite all the benefits, the implementation of AI brings security challenges. False results can destroy the systems of certain corporations as well as the artificial intelligence system itself. Also, high costs and legal restrictions hinder widespread implementation, especially in smaller organizations. The lack of experts further complicates the development and maintenance of advanced AI solutions.

A winning combination is artificial intelligence and existing security regulations and practices. In this way, organizations can significantly improve data protection and system resilience. The future of cyber security is reflected in intelligent, adaptive systems that will react promptly and also predict potential attacks. The continued development of artificial intelligence, along with ethical and legal oversight, will enable a safer digital environment.

## REFERENCES

[1] S. S. G. S. M. Ashish Juneja, "Cyber Security and Digital Economy: Opportunities, Growth and Challenges," *Journal of Technology Innovations and Energy*, 2024.

[2] D. R. Gupta, "Cybersecurity Threats in E-Commerce: Trends and Mitigation Strategies," *Journal of Advanced Management Studies,* vol. 1, no. 3, pp. 1-10, 2024.

[3] A. Bendovschi, "Cyber-Attacks – Trends, Patterns and Security Countermeasures," *7th International Conference On Financial Criminology*, pp. 24-31, 2015.

[4] A. J.-A. A. M. N. a. A. M.-N. William Villegas-Ch, "Integrating Explainable Artificial Intelligence in Anomaly Detection for Threat Management in E-Commerce Platforms," *IEEE Access*, vol. 6, 2016.

[5] W. Liang and F. Hamzah, "Behavioral Biometrics and AI for Cloud User Authentication," 2025.

[6] N. Aisyah, R. Hidayat, S. Zulaikha, A. Rizki, Z. B. Yusof and D. P. a. F. Ismail, "E-Commerce Authentication Security with AI: Advanced Biometric and Behavioral Recognition for Secure Access Control," *QuestSquare,* vol. 7, pp. 55-67, 2021.

[7] M. F. Ansari, B. Dash and P. S. a. N. Yathiraju, "The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review," *International Journal of Advanced Research in Computer and Communication Engineering*, 2022.