Journal homepage: https://devma.com.ua/en

DEVELOPMENT MANAGEMENT

UDC 004.4'2:004.8
DOI: 10.57111/devt/4.2023.53

Vol. 22, No. 4. 2023

Hybrid approaches to machine learning in software development: Applying artificial intelligence to automate and improve processes

Oleksii Zarichuk*

Computer and Information Systems Manager
LLC Fides
02000, 11A E. Sverstyuk Str., Kyiv, Ukraine
https://orcid.org/0009-0009-0771-8465

Abstract. The study on hybrid machine learning approaches is relevant because these approaches have great potential to improve predictive accuracy and software automation, and their use is becoming more widespread. The purpose of this study was to provide recommendations for the use of hybrid machine learning methods and analyse the areas of application of artificial intelligence, which is used to automate and improve processes. Problems related to hybrid approaches to machine learning were identified using the analytical method. The use of the statistical method allowed assessing the development of stability and performance of hybrid machine learning approaches. Features and differences of machine learning in the field of software development are noted. Errors and reasons that are made when improving development processes are analysed. It is established that a comprehensive analysis of the functioning of artificial intelligence is important to assess its effectiveness, development, and complexity of work in automation and improvement of development. The issues of evaluating the work of this type of approach, the expediency of their use, limitations in the process, and the impact of restrictions on the result are considered. It is determined that the use of artificial intelligence in the process of automation and improvement of development processes will improve the quality of resource optimisation. The study offers recommendations that will contribute to the effective regulation of this issue. The practical value of the study lies in the possibility of applying the results obtained to eliminate errors in the development and improvement of hybrid approaches, investigating the reliability of using artificial intelligence, considering various factors that serve as the basis for recommendations on appropriate use

Keywords: predictive accuracy; resource optimisation; information protection; reduced development time; cybersecurity

Article's History: Received: 11.05.2023; Revised: 12.10.2023; Accepted: 29.11.2023

INTRODUCTION

Hybrid approaches to machine learning in software development involve combining different machine learning methods and techniques to solve specific software development tasks. Hybrid models can use controlled (such as classification and regression) and uncontrolled learning methods (such as clustering and anomaly analysis) together to analyse and process data in software development. This is useful for detecting errors in code or analysing event logs. Hybrid approaches can use neural networks to analyse structured data and natural language processing to understand text. As V. Kochkodan *et al.* (2023) state, an important aspect of information security and cybersecurity is the development of specialised software that detects potential threats and automatically responds or notifies users. Such software can be used to detect and prevent various cyber threats and security incidents. The improvement of artificial intelligence arises from the need to solve problems related to errors that occur at the stages of software development and operation. These problems arise in connection with the need to define and optimise indicators at the stages of system design, operation, and development. Artificial intelligence has the ability to analyse large amounts of data, including event logs, network traffic, and user activity, and detect unusual and suspicious actions or events that may be threat indicators. According to T. Yarovoy (2023), artificial intelligence is rapidly developing, its application in the public sector has great potential to change how society is managed. It can analyse large

Suggested Citation:
Zarichuk, O. (2023). Hybrid approaches to machine learning in software development: Applying artificial intelligence to automate and improve processes. *Development Management,* 22(4), 53-60. doi: 10.57111/devt/4.2023.53.

*Corresponding author

amounts of data and extract information that is useful for government services.

In this area, it is necessary to introduce effective hybrid approaches and invest in research and development of technologies for more efficient operation of artificial intelligence. According to O. Smyrnov & A. Borysenko (2023), different software can combine and analyse different data sources to identify complex patterns and relationships that indicate potential threats. It can detect anomalies in system parameters, user behaviour, and network traffic, and the detected abnormal changes can indicate potential threats. It is important to implement policies aimed at developing threat detection software. This technology is often integrated with other security systems, such as firewalls and identification systems, to automatically respond to detected threats. According to D.M. Byelov & M.V. Bielova (2023), artificial intelligence can automatically analyse large amounts of data from various sources and help governments make informed decisions in areas as diverse as agriculture, health, education, and transportation. It also suggests that artificial intelligence can use data analysis and machine learning to create personalised programmes and services for citizens that meet their specific needs and requests. K. Nazarova *et al*. (2023) noted that some systems use machine learning and artificial intelligence techniques to improve threat detection and reduce the number of false positives. According to I. Ivanova *et al*. (2023), artificial intelligence can create chatbots and automated response systems that can interact with citizens, provide information, and solve standard questions. As a result of historical data, the software can develop models to predict future threats and risks.

Despite substantial scientific achievements on this issue and its examination in various fields, the issue of applying hybrid approaches to machine learning has not been considered in detail, and some of the studies do not provide enough recommendations. The purpose of this study was to perform an objective analysis and consider recommendations for identifying problems and errors in the process of improving the efficiency of artificial intelligence machine learning using hybrid approaches.

MATERIALS AND METHODS

At the beginning of the study, its main theoretical base was prepared, which included various literature sources on the analysis of which the basis for further drawing conclusions was laid. The use of the analytical research method allowed identifying problems associated with using hybrid approaches to machine learning, which are used in the processes of improving the efficiency of software development. Using the statistical method, an analysis of the investigation of artificial intelligence was conducted, which in turn helps to understand the number and causes of errors in improving artificial intelligence, which is the basis for the sustainable development of automation systems and improving software development processes. The analytical method also examined opportunities for improving the operation of data processing mechanisms, prospects for using these programmes and developing the sustainability and productivity of hybrid machine learning approaches.

Using the method of analysis, the examined issue was divided into smaller components, which helped to conduct a detailed analysis of the role and essence of hybrid approaches at different levels of machine learning development in the field of software; identify the advantages and disadvantages of their application; analyse the impact of the functioning of artificial intelligence systems on the material and technological support of developing countries; consider the areas of using artificial intelligence and its contribution in various fields of life. Through the structural and functional method, trends, factors, and models aimed at improving artificial intelligence were considered, and effective solutions to problems related to errors in development, improving the maintenance of software and its components were identified and analysed; the method allowed further analysing the methods for improving and innovating mechanisms to reduce inaccuracies in their functioning and optimising indicators at the development stages. Using the deduction method, the features of the functioning of complex automation in artificial intelligence in the processing, solution, and neutralisation of cyber threats were considered by highlighting the characteristics of these threats necessary for a complete analysis of the work and solving the problems of this process, in particular, the introduction of error-solving mechanisms.

By applying the synthesis method, various aspects of the subject considered before were formed and examined as one set, which helped to consider the obtained indicators of theoretical analysis and practical experience to identify recommendations aimed at solving problems and achieving progressive growth of the process. The synthesis allowed paying attention to improving the quality of software mechanism development, reducing errors, presenting predictive models, and designing solutions for artificial intelligence. The functional analysis method provided an opportunity to consider in more detail the concept of "using hybrid approaches to machine learning in the field of software development and using artificial intelligence to automate and improve development processes". This method allowed characterising the features and principles of software functioning and the process of improving development, analysing the complexity of mechanisms in the processes of detecting and solving cyber threats and their impact on the satisfaction and requirements of certain users.

RESULTS

Progressive development of automation and hybrid machine learning approaches is necessary to ensure reliable processing and optimisation of information and effective operation of artificial intelligence mechanisms in various areas of the software industry. Special attention should be paid to improving their mechanisms, in particular, precise design and modelling, since these approaches are widely used in software development processes, which will contribute to increasing the production potential of artificial intelligence. The introduction of intrusion detection systems based on artificial intelligence and machine learning allows using resources more efficiently, optimising solutions in many sectors, such as healthcare and education, and has a substantial impact on public safety. Intrusion detection systems based on artificial intelligence can help governments more effectively allocate limited cybersecurity resources: they can prioritise and focus on the most important aspects of protection (Baduge *et al*., 2022). It is important to solve the problem that occurs when developing, improving, and modelling software mechanisms.

Some errors directly impact improving the potential of artificial intelligence, the reliability of service delivery, and the security of information processing. Attention should be paid to the effectiveness of mechanisms in developing countries and the further development of hybrid software approaches. Anomaly-based systems use machine learning techniques to build models of normal network behaviour, anomalies that deviate from this norm are observed and identified as potential threats. Detecting intrusions into critical infrastructure, such as energy systems, transport networks, and telecommunications systems, can help ensure public safety and protect against cyber-attacks that can have serious consequences for society (Ramachandran *et al.*, 2022). In the field of software and artificial intelligence, it is necessary to analyse and identify the root causes of errors in information processing, and further solving these problems is aimed at improving the quality of information storage services. The use of artificial intelligence and machine learning can help intrusion detection systems more effectively detect new and modern attacks and reduce the number of false positives.

Intrusion detection systems can be used to analyse and optimise healthcare processes. For example, they can help identify possible leaks in medical records and improve the safety of medical equipment. Artificial intelligence can analyse medical data and patient records to predict the spread of diseases and the need for medical care. Hybrid approaches can use information from a variety of sources, such as clinical data, images, and genetic data, to diagnose and even make recommendations for the treatment of diseases. Hybrid recommendation systems can combine collaborative filtering techniques with content-based approaches to provide more accurate recommendations to users. In other industries, such as the financial and manufacturing sectors, intrusion detection systems can help reduce losses from cyber-attacks and data leaks. Intrusion detection systems can ensure the safety and privacy of patients and students and improve the quality of services provided. The use of artificial intelligence and machine learning in Intrusion detection systems can play an important role in ensuring cybersecurity and optimising decision-making in many areas of life and has great potential to improve society's standard of living (Rajagopal *et al.*, 2022). The development of new methods to solve the problems of eliminating errors in developing, designing, and improving software to increase the capacity of mechanisms for intrusion detection systems in many areas has great progress and prospects. Machine learning algorithms can be used to generate code based on specifications or code samples automatically – this can substantially speed up the development process.

However, the use of artificial intelligence in cybersecurity and other areas can also involve risks that need to be carefully evaluated. Hackers can use machine learning algorithms to break into systems, bypass security, or create new types of attacks (Beerbaum, 2022). If modern electronics and computerised data processing of intrusion detection systems are used to improve software and artificial intelligence, which are the basis for the development of many areas, this will help to substantially increase the capabilities of these processes and mechanisms and increase the demand for their use in many areas. Rule-based systems use a set of rules that define acceptable and unacceptable behaviour on the network. The activity can be identified as suspicious or abnormal if it does not meet these standards. The use of artificial intelligence may require access to large amounts of data, including the personal data of users, which requires care to ensure the confidentiality of such data and compliance with the requirements for their protection (Javaid *et al.*, 2022). The challenges of effectively managing technological hybrid approaches to software mechanisms and their problems with the application and development of innovative parts and devices for use are becoming increasingly practical.

Statistical methods use statistical indicators (mean, variance, deviation from the mean) to detect abnormal traffic values. Machine learning techniques use machine learning algorithms such as neural networks, decision trees, classifiers, and clustering to build models of normal traffic. Anomalies are defined as deviations from these patterns. The use of artificial intelligence can sometimes raise ethical issues, especially in certain contexts, such as facial recognition, medical decision-making, and criminal justice, so it is important to consider issues of fairness, bias, and responsibility (Lareyre *et al.*, 2023). In this complex process, reviewing the causes of errors in the improvement, automation, and optimisation of artificial intelligence, which increases the potential for automation and improvement of software development processes, and their solution becomes particularly important since the development of this process and their mechanisms in the world is one of the most pressing problems of our time. Threshold methods detect anomalies, if traffic metrics exceed these thresholds, this can be considered an anomaly. In turn, signature systems are effective at detecting known attacks but are not able to respond to new attacks. Rule-based systems can be configured to detect specific anomalies, but they may not be able to handle complex scenarios.

Machine learning models can make errors, including false positives (false attack alerts) and false negatives (failure to detect real attacks), which can lead to data loss or an overload of security administrators (Celik *et al.*, 2022). Often, the processing and execution of proper processes in a system of software mechanisms has certain errors that degrade the effectiveness of these processes for use in the field of information technology. The behaviour of attackers in computer networks often differs from that of ordinary users, and these differences can be detected by analysing their digital traces and network activity. Intrusion detection systems and anomaly detection systems are used to detect these differences. It is important to ensure transparency in how artificial intelligence systems make decisions and how they affect people's lives, and organisations should be held accountable for the consequences of using artificial intelligence.

The communication capabilities of the internet are taking on new forms due to modern technologies, and communication technologies based on instant messengers and chatbots have become especially relevant. Chatbots are widely used in various business sectors to automate communication with customers and perform analytical tasks: chatbots can learn from user responses or have a pre-programmed set of templates. They can be used both for personal use and for doing business: to start using a chatbot, you can add it to the general group for all colleagues, start a dialogue in private messages, or take out a subscription (Povolotsky, 2019). Chatbots are a modern solution for simplifying communication between clients and the institution, providing quick answers to user questions.

The problem of eliminating errors in software improvement, automation, and optimisation is not fully solved. Neural networks can be trained to analyse network traffic and detect anomalies that indicate possible attacks or unusual activity. Anomalies that are difficult to detect by conventional methods can also be detected. The volume of data in the public sector is huge, and its processing and analysis require powerful tools and technologies, including systems for storing and processing large amounts of data. The public sector uses data analytics to make decisions in areas such as health, education, and the economy, and data analysis helps identify trends, plan resources, and improve programmes and services.

Software mechanisms and their components are often used because of their efficiency and low cost of operation, and there is currently increased interest in this process in many countries to increase information technology capacity. Neural networks can be trained to recognise attack signatures, including known types of attacks such as Structured Query Language Injection or Distributed Denial of Service attacks – they can even recognise modified or variant signatures. Data analysis using artificial intelligence and machine learning can cover complex relationships and patterns that would go unnoticed in human analysis and can be used to predict events, classify data, and automate routine tasks. Neural networks can analyse the behaviour of users and systems and detect abnormal behaviour, they learn from normal behaviour and warn about deviations from normal patterns. Neural networks filter out noise and reduce the number of false positives, helping to detect only truly substantial anomalies and threats; they can learn from new threats and adapt to changing attack methods. Data processing and analysis involve substantial privacy and security issues. The public sector must comply with relevant standards and regulations regarding personal data protection and information security.

The public sector can promote the availability of data to the public and researchers to encourage innovation and the development of data-based applications, the legal framework and rules for data collection, processing and storage in the public sector are important for ensuring the rights and privacy of citizens. The main advantages of intrusion detection systems that use neural networks and other artificial intelligence methods are their high learning rate and adaptability to new types of attacks. Neural networks can learn large amounts of data in a relatively short period of time and thus detect new attacks and anomalies that were previously unknown, and rapid training allows the system to adapt to changing threats. Artificial intelligence is useful in analysing large amounts of public data, helping to make informed decisions in various sectors: it can process and analyse large amounts of data much faster than humans and identify complex patterns, trends, and connections that go unnoticed by conventional analysis methods.

Neural network training can be automated, allowing the system to update its models based on new data without substantial human intervention. Neural networks are suitable for detecting anomalies because they can detect changes in the data structure, even if they are not typical for attacks. Systems that use reinforcement learning techniques can improve their strategies in real time based on the results of detecting and responding to attacks. Artificial intelligence can help government agencies identify areas where they can use resources more efficiently, optimise processes, and reduce costs. It can track and analyse public opinion based on social media and other sources, which can help governments understand public sentiment and respond quickly to it.

Artificial intelligence can use data from weather stations and satellite observations to predict weather conditions and help take appropriate measures in the event of dangerous weather events. In public administration and finance, artificial intelligence can analyse economic indicators, financial markets, and microeconomic trends to predict economic events and make monetary policy decisions. It can be used to analyse large amounts of data stored in various government agencies, allowing governments to make better-informed decisions in areas such as the economy, health, and education. Hybrid methods can also be used to analyse large amounts of data, where data processing at a preliminary stage (for example, using noise reduction methods) is combined with deep learning to identify complex dependencies. In business, it can analyse data on supply and demand, consumer trends, price dynamics, and other factors to predict demand for goods or services, which helps companies optimise production and inventory. In transport systems, artificial intelligence can be used to predict the intensity and regulation of traffic, optimise routes to improve transport efficiency. Artificial intelligence is used to analyse environmental data to predict natural disasters, pollution, and other environmental problems. Artificial intelligence political systems can analyse social and political trends to predict election results and public reactions to government decisions.

The emphasis on building hybrid systems that combine neural networks with other machine learning methods is of great importance in modern research and development because hybrid systems have the advantages of both approaches and can help in solving complex problems. Hybrid systems can solve multiple tasks simultaneously or sequentially, which is why building hybrid systems is an active area of research in the field of machine learning and artificial intelligence. This is because these systems can achieve excellent results in a variety of complementary areas, such as intrusion detection, pattern recognition, and decision-making. Hybrid systems can combine expert knowledge with data-driven learning. For example, decisions can be made by combining rules and neural networks developed by experts. Many countries have made substantial progress in developing the design and modelling of hybrid approaches to improving software mechanisms. Hybrid systems adapt and can change components according to the task and situation: these systems can be designed to ensure stability and speed of task execution. When improving software mechanisms and automating and optimising them for better passage of complex technological operations, process models should adequately describe the essence of the work, be simple and easy to implement.

In achieving optimal performance of software mechanisms and increasing the potential of the information technology sector, personnel qualifications and timely diagnostics of the neural network are of great importance. Hybrid approaches in computer science and machine translation have made substantial strides and are key to achieving high quality and productivity. In the field of machine translation, hybrid approaches are used that combine statistical methods and deep learning methods, for example, deep learning models such as Neural Machine Translation. Recurrent neural networks or transformers can be combined with statistical machine translation techniques to improve translation accuracy. The introduction of artificial intelligence in public administration is becoming more widespread and has great potential to improve the quality and efficiency of public administration. It can be argued that artificial intelligence can be useful for automating and improving software development processes at various stages. The various areas of its use are summarised in Table 1.

Table 1. Promising areas of artificial intelligence application

Field	Application method
Public sector	Decision-making analytics for all other areas, secure storage of personal data of citizens, efficient use of available resources, cost reduction
Healthcare	Accounting of medical documentation, analysis of the condition of technical equipment, forecasting the course of the disease
Business	Communication with clients and colleagues, maintaining financial documentation, optimising the production of goods, and providing various services
Cybersecurity	Automatic notification about threats, blocking attacks, scanning the network or software to identify weaknesses
Infrastructure and environment	Analysis of air pollution, forecasting of environmental hazards, regulation of traffic

Source: compiled by the author

Therefore, hybrid machine learning methods can be applied in a large number of tasks where different approaches need to be combined to achieve better results. Developing hybrid models can require substantial effort during the data preparation and parameter configuration stages. However, the properly selected and developed hybrid approach can bring substantial advantages in complex machine learning tasks. For optimal use of hybrid approaches, it is recommended to conduct the following actions. Before considering a hybrid approach, it is important to understand the problem in detail, determine why hybridisation is necessary, and which approaches or models can be combined to achieve better results. In addition, it is necessary to consider what components will be included in the hybrid system: it can be a combination of classical machine learning models, deep learning, rule systems, or other methods. It is necessary to build a hybrid model that combines the selected methods, this may include a set of models combined by, for example, multiclass classification, or a sequential approach where the output of one method is used as input for another. It is important to configure the parameters of each method and the hybrid model in general, for which, using cross-validation and optimising the parameters to improve performance is recommended. Data preparation for a hybrid approach should include cleaning, anomaly removal, scaling, and feature selection, but different methods may require different types of data preparation. Different metrics and criteria are often used to evaluate the performance of a hybrid model, so it is important to understand that it solves the problem correctly and is not retrained. After implementing the hybrid model, it is crucial to monitor its performance and results and make adjustments to the hybrid approach if necessary. Hybrid machine learning techniques can be a powerful tool for solving complex problems but also require careful preparation and configuration. Keeping detailed documentation about hybrid models, their parameters, and results is recommended, which will help save settings and make further support more efficient. A balanced approach and a thorough study of the specific task are key success factors.

DISCUSSION

Hybrid approaches to machine learning in software development are important in the modern world. These approaches combine machine learning techniques and methods with other approaches, such as conventional programming, expert systems, natural language processing, computer vision, optimisation, data mining, etc., to achieve improved process improvement and automation results. Many researchers focus their attention both on the examination of this issue and the improvement of artificial intelligence itself and the use of hybrid approaches in working with it. Hybrid machine learning methods allow using the strengths of different approaches and algorithms to achieve more accurate and efficient solutions to complex problems. Hybrid methods that combine expert rules with analysis of large amounts of data can be used to detect threats and cyber-attacks. Hybrid approaches can combine structured data and deep link training to create more complete knowledge graphs. It is important to consider the choice of specific methods, and their combination will depend on the specific task and available data.

Based on the results of the recent study by M.H.A. Banna *et al*. (2023) in Natural Language Processing, hybrid approaches combine rules and statistics. For example, entity recognition systems can use rules to define named entities and statistical methods to determine the context and relationships between them. In computer vision, hybrid approaches can combine deep learning and structural analysis for object recognition in complex contexts. It is necessary to improve the quality of various methods and approaches to enhance software mechanisms of the information technology sector, for the effective operation of the entire mechanism through the use of new methods. It is necessary to improve the quality of the automation and optimisation of these systems, especially neural networks to begin the process of improving these systems. After analysing the mechanism of artificial intelligence, the researcher established that for the successful implementation of artificial intelligence, it is necessary to have stable fundamental knowledge that allows you to understand the physical principles and determine the optimal number of processes, which is important for effective improvement of software mechanisms, to increase the potential of the information technology sector in many countries under appropriate conditions.

Turning to the definition by M.H. Jarrahi *et al*. (2023), artificial intelligence can help automate citizen registration and service processes using chatbots, virtual assistants, and other technologies to reduce administrative burden and increase the availability of services. Artificial intelligence can use data analytics to predict a city's population and resource requirements. This can help optimise budget allocations and plan infrastructure development. This confirms the fact that this study coincides with modern trends in the field of design and modelling of methods for improving artificial intelligence mechanisms. In the modern world, great attention is paid to considering all factors that affect the quality of these processes to increase the potential of the information and technology sector. However, this study did not consider that an important property of artificial intelligence is its use to automate procurement processes and control costs, reducing corruption in government procurement.

Researchers A. Talukder *et al*. (2023) determined that the development of hardware and software tools for unauthorised access requires constant adaptation of technical data protection tools. As cybercriminals are constantly looking for new methods of attacks and vulnerabilities, it is important to maintain a high level of cybersecurity. It is important to regularly update software and operating systems and install official patches that fix the identified vulnerabilities, preventing attackers from exploiting the vulnerabilities. For more correct operation of cybersecurity applications and software mechanisms, it is necessary to constantly check the entire neural network, so the potential of the information technology sector in countries will reach high values in a short time. There are differences with this study in that the author overlooked the importance of the features of using this type of hybrid approach to machine learning, timely examination of data and possible causes of problems with the mechanisms of this software for further promising development of the use of artificial intelligence mechanisms to increase the prospects of the information technology field.

Researcher J.P. Bharadiya (2023) notes that intrusion detection systems are an important component of cybersecurity, helping to detect anomalies and potential threats in computer networks and systems. Signature-based intrusion detection systems analyse network traffic and system logs for known attack signatures. When they detect a situation that matches the signature, they notify the administrator or perform other predefined actions. This approach is effective for detecting known threats, but not for new attacks. The results of this study of the characteristics of intrusion detection systems were analysed and more accurately considered. It can be supplemented by the fact that increasing the potential of the information technology industry directly depends on the improvement and innovation of software and providing high-quality service to the mechanisms of this artificial intelligence.

I. Arpaci & M. Bahari (2023) showed that the use of machine learning algorithms can affect a number of areas, such as combating fraud and corruption in social security systems, planning transport networks, optimising routes, automating document processing, and interacting with citizens. Machine learning algorithms can analyse large amounts of data to identify anomalies and patterns that signal potential fraud and corruption. For example, they may detect abnormal patterns in social security applications and financial transactions. Machine learning can analyse traffic data, passenger traffic, and road conditions to optimise transport networks and develop efficient routes. It was not specified or considered in the paper by I. Arpaci & M. Bahari (2023) that natural language processing algorithms can automate the processing of documents delivered to organisations by identifying key information and classifying documents. Notably, this is due to the fact that the use of chatbots and virtual assistants based on machine learning has increased substantially in recent years, and this can facilitate the interaction of citizens with government agencies, so there is a difference between this study and that by the authors. As noted by S.S. Ray *et al*. (2023), anomaly detection systems model the normal behaviour of a network or system and look for any abnormal changes or deviations from this norm. They use statistical methods and machine learning to identify potential threats, even if these threats are not known in advance, and are also useful for detecting new attacks and out-of-the-box scenarios.

It should also be attributed to the results of the study that intrusion detection systems are an important element in protecting users' and businesses' information, as they help to respond to potential threats in a timely manner and reduce the risk of loss of confidential information and other cyber events. It is necessary to consider two aspects to improve the design and modelling of methods for improving software mechanisms and to reduce errors in automation and optimisation during complex technological processes: increasing funding and improving the skills of developers, and the introduction of new technologies. The main goal of these measures is to improve the quality and efficiency of the process of improving artificial intelligence mechanisms and reduce the risk of errors.

CONCLUSIONS

The study confirmed that the decision to use hybrid approaches in machine learning should be justified from a scientific and practical standpoint. The results show that the main purpose of intrusion detection systems is to identify and filter potentially malicious requests or attacks in computer networks and systems. Many technological adaptations need to be made for certain areas. In this paper, recommendations for eliminating errors in the processes of designing and implementing mechanisms of hybrid approaches and analysing their functioning were considered, technological processes during the operation of software and errors and problems made during the functioning of artificial intelligence processes were analysed. Implementing effective tools will solve these problems and prevent mistakes. Hybrid approaches were considered to improve the software. The analysis shows that hybrid models that combine deep learning with classical image processing or natural language processing techniques will help improve object recognition accuracy in images or text comprehension. It was considered that it is possible to improve the efficiency of artificial intelligence and software mechanisms in the information technology field through the introduction of hybrid methods.

The study analysed aspects of improving software mechanisms, ways to improve the processes of artificial intelligence, and identifying methods for eliminating errors in the process of improving software efficiency, which will contribute to improving the potential, competitiveness, and quality in the information technology field. The study provides recommendations for the successful use of hybrid machine learning methods in software development. It is required to configure the parameters of each method and hybrid model using cross-validation and prepare the data by performing cleaning, scaling, and feature selection, considering the requirements of different methods. It is also necessary to carefully examine the metrics and criteria for evaluating the performance of a hybrid model and avoid improper retraining. It is essential to provide detailed documentation on the parameters of hybrid models. These recommendations can help achieve successful results when applying hybrid machine learning methods. Future research will focus on creating and implementing innovative intrusion detection systems to advance the information technology sector.

ACKNOWLEDGEMENTS

None.

CONFLICT OF INTEREST

None.

REFERENCES

[1] Arpaci, I., & Bahari, M. (2023). Investigating the role of psychological needs in predicting the educational sustainability of Metaverse using a deep learning-based hybrid SEM-ANN technique. *Interactive Learning Environments*. doi: 10.1080/10494820.2022.2164313.

[2] Baduge, S.K., Thilakarathna, S., Perera, J.S., Arashpour, M., Sharafi, P., Teodosio, B., Shringi, A., & Mendis, P. (2022). Artificial intelligence and smart vision for building and construction 4.0: Machine and deep learning methods and applications. *Automation in Construction*, 141, article number 104440. doi: 10.1016/j.autcon.2022.104440.

[3] Banna, M.H.A., Ghosh, T., Nahian, M.J.A., Kaiser, M.S., Mahmud, M., Taher, K.A., Hossain, M.S., & Andersson, K. (2023). A hybrid deep learning model to predict the impact of COVID-19 on mental health from social media big data. *IEEE Access*, 11, 77009-77022. doi: 10.1109/ACCESS.2023.3293857.

[4] Beerbaum, D.O. (2022). Artificial intelligence ethics taxonomy-robotic process automation (RPA) as business case. *SSRN*. doi: 10.2139/ssrn.4165048.

[5] Bharadiya, J.P. (2023). Machine learning and AI in business intelligence: Trends and opportunities. *International Journal of Computer (IJC)*, 48(1), 123-134.

[6] Byelov, D.M., & Bielova, M.V. (2023). Artificial intelligence in judicial proceedings and court decisions, potential and risks. *Scientific Bulletin of the Uzhhorod National University*, 2(78), 315-320. doi: 10.24144/2307-3322.2023.78.2.50.

[7] Celik, I., Dindar, M., Muukkonen, H., & Järvelä, S. (2022). The promises and challenges of artificial intelligence for teachers: A systematic review of research. *TechTrends*, 66, 616-630. doi: 10.1007/s11528-022-00715-y.

[8] Ivanova, I., Borovyk, T., Zalozna, T., & Rudenko, A. (2023). Use of artificial intelligence for marketing. *Marketing and Digital Technologies*, 7(2), 32-42. doi: 10.15276/mdt.7.2.2023.3.

[9] Jarrahi, M.H., Askay, D., Eshraghi, A., & Smith, P. (2023). Artificial intelligence and knowledge management: A partnership between human and AI. *Business Horizons*, 66(1), 87-99. doi: 10.1016/j.bushor.2022.03.002.

[10] Javaid, M., Haleem, A., Singh, R.P., & Suman, R. (2022). Artificial intelligence applications for industry 4.0: A literature-based study. *Journal of Industrial Integration and Management*, 7(1), 83-111. doi: 10.1142/S2424862221300040.

[11] Kochkodan, V., Petryna, M., & Stankovska, I. (2023). Application of machine learning and artificial intelligence in oilfield development. *Scientific Bulletin of Ivano-Frankivsk National Technical University of Oil and Gas*, 1(27), 16-26. doi: 10.31471/2409-0948-2023-1(27)-16-26.

[12] Lareyre, F., Behrendt, C.-A., Chaudhuri, A., Lee, R., Carrier, M., Adam, C., Duy Lê, C., & Raffort, J. (2023). Applications of artificial intelligence for patients with peripheral artery disease. *Journal of Vascular Surgery*, 77(2), 650-658. doi: 10.1016/j.jvs.2022.07.160.

[13] Nazarova, K., Parasii-Verhunenko, I., & Ostapets, A. (2023). Risk classification of IT industry companies. *Bulletin of the Kyiv National University of Trade and Economics*, 150(4), 120-137. doi: 10.31617/1.2023(150)08.

[14] Povolotskyi, B. (2019). *Mobile application with Telegram-bot of the Konotop Industrial Pedagogical Professional College of Sumy State University*. (Master thesis, Sumy State University, Sumy, Ukraine).

[15] Rajagopal, B.R., Anjanadevi, B., Tahreem, M., Kumar, S., Debnath, M., & Tongkachok, K. (2022). Comparative analysis of blockchain technology and artificial intelligence and its impact on open issues of automation in workplace. In *2022 2nd international conference on advance computing and innovative technologies in engineering (ICACITE)* (pp. 288-292). Greater Noida: IEEE. doi: 10.1109/ICACITE53722.2022.9823792.

[16] Ramachandran, K.K., Mary, A.A.S., Hawladar, S., Asokk, D., Bhaskar, B., & Pitroda, J.R. (2022). Machine learning and role of artificial intelligence in optimizing work performance and employee behavior. *Materials Today: Proceedings*, 51(8), 2327-2331. doi: 10.1016/j.matpr.2021.11.544.

[17] Ray, S.S., Verma, R.K., Singh, A., Ganesapillai, M., & Kwon, Y.N. (2023). A holistic review on how artificial intelligence has redefined water treatment and seawater desalination processes. *Desalination*, 546, article number 116221. doi: 10.1016/j.desal.2022.116221.

[18] Smyrnov, O., & Borysenko, A. (2023). Trend in software-defined vehicles. *Bulletin of Mechanical Engineering and Transport*, 17(1), 163-169. doi: 10.31649/2413-4503-2023-17-1-163-169.

[19] Talukder, A., Hasan, K.F., Islam, M., Uddin, A., Akhter, A., Yousuf, M.A., Alhabri, F., & Moni, M.A. (2023). A dependable hybrid machine learning model for network intrusion detection. *Journal of Information Security and Applications*, 72, article number 103405. doi: 10.1016/j.jisa.2022.103405.

[20] Yarovoy, T. (2023). Opportunities and risks of the use of artificial intelligence in public administration. *Economic Synergy*, 2, 36-47. doi: 10.53920/ES-2023-2-3.

Гібридні підходи до машинного навчання в галузі розроблення ПЗ: Застосування штучного інтелекту для автоматизації та поліпшення процесів

Олексій Геннадійович Зарічук

Менеджер комп'ютерних та інформаційних систем
ТОВ «Фідес»
02000, вул. Є. Сверстюка, 11А, м. Київ, Україна
https://orcid.org/0009-0009-0771-8465

Анотація. Дослідження гібридних підходів машинного навчання є актуальним, адже дані підходи мають великий потенціал у підвищенні прогностичної точності та автоматизації програмного забезпечення, а їх використання стає все більш поширеним. Метою цієї роботи було надання рекомендацій для застосування гібридних методів машинного навчання, а також аналіз сфер застосування штучного інтелекту, який використовується для автоматизації та покращення процесів. За допомогою аналітичного методу було виявлено та визначено проблеми, пов'язані із використанням гібридних підходів до машинного навчання. Застосування статистичного методу дозволило оцінити розвиток стійкості і продуктивності гібридних підходів машинного навчання. Відзначено особливості та відмінності машинного навчання в галузі розроблення програмного забезпечення. Проаналізовано помилки та причини, які допускаються при покращенні процесів розроблення. Встановлено, що важливе значення має всебічний аналіз функціонування штучного інтелекту з метою оцінки його ефективності, розвитку та ускладнення роботи при автоматизації та поліпшенні розроблення. Розглянуто питання оцінки роботи даного типу підходів, доцільність їх використання, обмеження у процесі, вплив обмежень на результат. Визначено, що використання штучного інтелекту у процесі автоматизації та поліпшенні процесів розроблення забезпечить підвищення якості оптимізації ресурсів. В дослідженні запропоновано рекомендації, які сприятимуть ефективному регулювання даного питання. Практична цінність роботи полягає у можливості застосування отриманих результатів для усунення помилок у розробці та вдосконаленні гібридних підходів, вивченні надійності застосування штучного інтелекту з урахуванням різних факторів, які служать основою для рекомендацій щодо доцільного використання

Ключові слова: прогностична точність; оптимізація ресурсів; захист інформації; скорочення часу розробки; кібербезпека