ISSN 0861 - 6604
ISSN 2534 - 8396

BUSINESS management

PUBLISHED BY
D. A. TSENOV ACADEMY
OF ECONOMICS - SVISHTOV

1/2026

BUSINESS management 1/2026

Editorial board:

Prof. Krasimir Shishmanov, Phd - Editor in Chief, Tsenov Academy of Economics, Svishtov, Bulgaria
Assoc. Prof. Marin Marinov, PhD – Co-editor in Chief, Tsenov Academy of Economics, Svishtov, Bulgaria
Prof. Mariana Petrova, PhD - Managing Editor Tsenov Academy of Economics, Svishtov, Bulgaria
Assoc. Prof. Aleksandar Ganchev, Phd - Tsenov Academy of Economics, Svishtov Bulgaria
Assoc. Prof. Irena Emilova, Phd - Tsenov Academy of Economics, Svishtov Bulgaria
Assoc. Prof. Ivan Marchevski, Phd - Tsenov Academy of Economics, Svishtov, Bulgaria
Assoc. Prof. Simeonka Petrova, Phd - Tsenov Academy of Economics, Svishtov Bulgaria
Assoc. Prof. Taner Ismailov, Phd - Tsenov Academy of Economics, Svishtov, Bulgaria

International editorial board:

Olena Sushchenko, Prof., DSc (Ukraine)
Dariusz Nowak, Prof., PhD (Poland)
Nurlan Kurmanov, Prof., PhD (Kazakhstan)
Ryszard Pukala, Prof., PhD (Poland)
Yoto Yotov, Prof., PhD (USA)
Badri Gechbaia, Prof., PhD (Georgia)
Mahmut Kadir Isguven, Assoc. Prof., PhD (Turkey)
Stefan-Alexandru Ionescu, Assoc. Prof., PhD, (Romania)

Proofreader: Elka Uzunova
Technical Secretary: Zhivka Tananeeva
Web Manager: Martin Aleksandrov

The printing of the issue 1-2026 is funded with a grand from the Scientific Research Fund, Contract KP-06-NP7/18/05.12.2025 by the competition "Bulgarian Scientific Periodicals - 2026".
The Scientific Research Fund is not responsible for the content of the materials.

Submitted for publishinq on 18.03.2026, published on 20.03.2026,
format 70x100/16, total print 80

© D. A. Tsenov Academy of Economics, Svishtov,
2 Emanuil Chakarov Str, telephone number: +359 631 66298
© Tsenov Academic Publishing House, Svishtov, 11A Tsanko Tserkovski Str

BUSINESS management

D. A. Tsenov Academy of Economics, Svishtov

Year XXXVI * Book 1, 2026

CONTENTS

A DUAL-LAYER HYBRID SECURITY FRAMEWORK: ANALYZING DIGITAL MODELS TO ENHANCE CYBERSECURITY MANAGEMENT FOR START-UPS AND SMES

Julia Yereshko[1],
Petyo Bozhinov[2],
Iryna Udovychenko[3],
Nomeda Dobrovolskienė[4],
Oksana Tsimoshynska[5]

Abstract: The rapid evolution of generative AI is transforming cybersecurity practices by providing advanced capabilities for threat detection and response. For start-ups and SMEs, these technologies offer a cost-effective way to defend against sophisticated online threats without the need for massive capital investment. While AI facilitates the identification of anomalies and malicious behavior, it also introduces new risks, such as deepfakes, zero-day exploits, and the potential for attackers to manipulate AI models themselves. The study examines the impact of large language models and artificial intelligence on the software and architecture of cybersecurity systems. The main types of attacks on artificial intelligence systems and the changes in the software development paradigm that result from them are being considered. To address the evolving threat landscape, this study proposes a Dual-Layer Hybrid

[1] National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine, e-mail: julia.jereshko@gmail.com, ORCID: 0000-0002-9161-8820

[2] D. A. Tsenov Academy of Economics, Svishtov, Bulgaria, e-mail: petyo.bozhinov@gmail.com, ORCID: 0009-0003-2784-9311

[3] Sumy Regional Institute of Postgraduate Pedagogical Education, Sumy, Ukraine, e-mail: hafran@ukr.net, ORCID: 0000-0002-1980-5402

[4]Vilnius Gediminas Technical University, Vilnius, Lithuania, e-mail: nomeda.dobrovolskiene@vilniustech.lt, ORCID: 0000-0002-1606-9980

[5] Interregional Academy of Personnel Management, Kyiv, Ukraine, e-mail: ovmichailenko@ukr.net, ORCID: 0000-0002-2277-3317

Security Framework that integrates high-speed algorithmic detection with cognitive analysis. We present an algorithm for building a security system using LLM models. We also propose a software application tailored explicitly for the comprehensive analysis of network traffic while detecting cybersecurity incidents using Python and the Pandas library. Furthermore, it leverages artificial intelligence to provide a comprehensive approach to detecting and mitigating cybersecurity threats. This will enable start-ups and small businesses to manage their cybersecurity in-house.

Keywords: Cybersecurity, AI, LLM, Smart Analytics, Hybrid Security Architecture, Start-ups, SMEs

JEL: M15, L26, O32

DOI: https://doi.org/10.58861/tae.bm.2026.1.03

Introduction

Generative artificial intelligence (AI) technologies, particularly generative pre-trained transformers (GPT, Gemini, etc.), are changing the field of security. AI provides advanced capabilities for detecting, preventing, and responding to threats, which significantly improves cybersecurity practices. This gives companies the ability to defend against more sophisticated online threats and is especially crucial for start-ups and newly established businesses, which may lack the financial resources to make substantial cybersecurity investments and are often required to cut costs.

This is also linked to the widespread development of innovation in enterprises (especially start-ups) implementing new technologies (Pukala, 2016). It should also be emphasised that innovative enterprises are very important for the country's economy and are its driving force (Ishchuk et al., 2021) as well as for the sector in which they operate (Pukala & Petrova, 2019).

Moreover, as the renewable energy sector continues to expand, the supporting infrastructure has become a prime target for cyberattacks. This is due to the increasing interconnectivity of technologies and systems within the energy sector, making them more susceptible to cyber threats. Attackers are exploiting vulnerabilities in smart grids, solar and wind farms, and other renewable energy facilities, posing significant risks to the stability and security of our energy supply.

DNV (2023) highlighted in "Energy Cyber Priority: Closing the Gap Between Awareness and Action" the increasing awareness of cybersecurity threats within the energy industry. The report points out that companies are

ramping up their investments to address these threats, driven by factors such as heightened geopolitical tensions, emerging compliance requirements, and the rapid adoption of digitally connected infrastructure.

There is a pressing need to place a stronger focus on securing safety-critical systems in light of these developments. Moreover, as cybersecurity's role in enabling digital transformation and the energy transition becomes more recognized, DNV (2023) emphasizes the importance of delving into the state of cybersecurity within the energy sector. This involves understanding the evolving landscape of cyber threats and the measures being taken to mitigate risks and ensure the resilience of critical energy infrastructure.

Artificial intelligence systems are able to sift through huge amounts of data and identify trends that may be signs of online threats. Anomalies, malicious behaviour, and well-known attack patterns can be detected using trained machine-learning models. Because of this, security services can detect and eliminate threats in advance.

However, it is important to note that artificial intelligence in cybersecurity does not come without challenges. Attackers can also potentially exploit AI systems to their advantage or avoid detection through anti-AI techniques. Artificial intelligence use can lead to cybersecurity issues in several ways, namely (Yermachenko et al., 2023):

• Emerging new types of cyber threats: Hackers can use artificial intelligence to create more sophisticated cyberattacks (or cyberattacks of entirely new types), such as creating fake content (e.g., deepfakes), bypassing technical security measures (e.g., voice biometrics) or exploiting vulnerabilities (e.g., zero-day exploits).

• Compromise of artificial intelligence systems: Artificial intelligence systems themselves may be vulnerable to cyber-attacks by tampering with their data, algorithms, or results. This can bias AI systems, which in turn can cause errors.

• Ethical and social issues: artificial intelligence systems may violate ethical and social issues related to cybersecurity, such as the privacy of private information, transparency, and reliability of data.

• Justice, human dignity, etc.: These issues can affect and/or violate the safety and well-being of individuals and society.

The research addresses these vulnerabilities by proposing a bifurcated framework where machine learning detection and Large Language Model interpretation operate as a single, cohesive unit.

AI-based programs differ from classical programs since they integrate the large language models (LLMs) and their key components, such as training data, models, policies, questions, and actions. While the functional components of classical applications (interface, backend, infrastructure, database, and standard functions) remain an integral part of AI-based applications, they will be modified.

1. Architecture of AI-based software

1.1. Background

Noever (2023) carried out an in-depth comparative analysis to evaluate the performance of state-of-the-art artificial intelligence-based systems, such as machine learning and deep learning algorithms, in comparison with a range of traditional static analysers. Including data flow analysis and abstract interpretation, for the purpose of detecting and rectifying various types of software vulnerabilities such as buffer overflows, SQL injection, and cross-site scripting. GPT4, in particular, has proven to be very effective, especially in terms of its capability to provide detailed explanations of vulnerabilities in code and to offer effective solutions to patch these vulnerabilities. The success of prediction can be significantly increased by integrating advanced natural language processing models with traditional static code analysis techniques. This integration allows for the thorough identification and elimination of security vulnerabilities within software systems, thereby improving the overall reliability and security of the predictive models. By leveraging the strengths of both paradigms, organizations can effectively fortify their systems against potential security threats and ensure the robustness of their predictive capabilities.

Koch (2023) demonstrated that GPT-3 outperformed a state-of-the-art static code analyzer in predicting security vulnerabilities. This highlights the potential of advanced language models such as GPT-3 in the cybersecurity and code analysis fields.

Bakhshandeh et al. (2023) found that the utilization of artificial intelligence significantly enhanced the capability of developers to identify and localize vulnerable code. This was particularly evident when artificial intelligence was combined with static analyzers, resulting in more accurate and efficient detection of vulnerabilities within the codebase.

Kalinin (2024) concluded that the rapid pace of global digital transformation significantly impacts the economic security of enterprises. The high level of openness exhibited by companies is identified as a contributing factor to the emergence of diverse threats and risks that directly affect their operational activities (Demianchuk et al., 2021; Lelyk et al., 2022; Kaminsky et al., 2023).

Therefore, it is important to study the problems associated with the risks of digital transformation and AI development (Popova et al., 2024; Popova et al., 2023; Popova & Petrova, 2024; Tairov et al., 2024; Popov et al., 2024).

1.2. Benchmarking the Circuit-Based and Artificial Intelligence Architecture

Software applications based on schemes (circuit-based) have a clear and rigid structure. Inputs and outputs must be explicitly established, routed, and maintained. Any deviation from this structure leads to errors, and adding new features requires a linear effort on the part of the organization's developers.

The new software will be based on intelligence. Such programs are based on natural language, in which requests are sent to a system that actually understands what the person is asking. Adding new features to such a program would be as simple as asking different questions and/or providing different commands. Comprehension-based applications adapt to the questions that are asked of them. To add new functionality, you ask different questions and ask for different actions on the results.

The new AI-based software architecture is expected to be much more elegant and based on AI systems, including a four-component structure: state, policy, question, and action. In essence, this is a transition from circuit-based application architecture to an intelligence-based architecture (Table 1).

Table 1
Circuit-Based Architecture vs Artificial Intelligence Architecture

Structure elements	Circuit-Based	AI-Based
input	Rigid – programme runs must be explicitly coded by the development team using explicit queries against a structured database.	Unlimited – programs run using natural language, so there is no need to explicitly code new requests to the server when other questions need to be asked.
data	Structured – data repositories have well-defined schemas that require specific ways of adding, retrieving, changing, and deleting data.	Dynamics – system's backend is a set of models that understand the world and your business. To upgrade the data repositories, get bigger/better data and save your models.
output	Stativity – program output returns the specific information requested by the specific query. To do something else, one needs to write separate code for it.	Flexibility – the output of the program is as flexible as the questions asked of the models. And questions and answers can be directly related to actions.
action	Isolation – actions are separated from query results. For example, after querying a database for housing prices, one or more additional steps must be taken to make them useful.	Coherence – actions can be linked to an outcome because models understand how they are related. This means that there is no need to create explicit bridges from each result to new actions.
understanding	Missing – the program does not understand the data, the queries being made against it, or the result it returned. It is a simple mechanism for storing and retrieving data.	Deep – models understand the data they are dealing with, which means that improving the models simultaneously improves most aspects of the application.
flexibility	Linear - to add more features to a program, you need to explicitly expand the number of encoded inputs, the number of output operations, the data structure, or all together.	Explicit – the main concepts: 1) ensuring the quality and freshness of the models; 2) ensuring the correctness of the questions.

1.3. Attacks on Artificial Intelligence Systems

In LangChain, agents are intelligent entities designed to achieve specific objectives. They are equipped with a variety of tools and resources that enable them to carry out their tasks effectively. Each agent operates with a clear purpose, utilizing its capabilities to navigate challenges and implement solutions efficiently.

A coordinated attack on the agents would have serious repercussions for entrepreneurs, potentially disrupting their operations and hindering business growth. For AI agents to be effective, they must be empowered with two key capabilities (Bondarenko et al., 2022):

1) They should possess extensive knowledge about the relevant objects, including highly personal and sensitive information.

2) They need the ability to act like the user in various tasks, such as sending money, posting on social networks, writing letters, and sending messages. An attacker who gains this knowledge and access will hence gain significant leverage over the target (Figure 1).

Tools refer to the resources available to Agents for performing their tasks. These tools can include web search capabilities, document scanning and analysis software, plagiarism detection systems, and other similar resources.

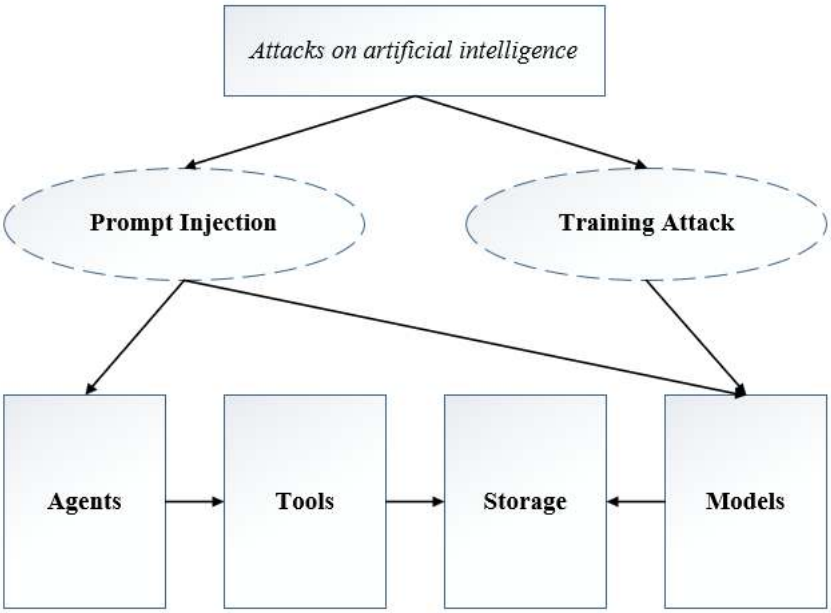

Figure 1. Attacks on artificial intelligence systems

Models are essential components of AI security, serving as the foundational frameworks that enable effective machine learning applications. In recent years, numerous business applications have adopted these advanced techniques, enhancing their operational efficiency and decision-making processes. By leveraging sophisticated algorithms and data analysis, organizations can better detect potential security threats, optimize resources, and improve overall performance.

Attacks on artificial intelligence systems are designed to manipulate models in such a way that they begin to exhibit undesirable behaviors. The goal is to undermine their reliability, making them less trustworthy in their outputs. Additionally, these attacks can result in models generating content that is more toxic and biased, further distorting their intended purpose and functionality.

Table 2
Basic types of attacks on artificial intelligence systems

Components of AI systems	Attack types
Agents	• alter the agent's routing • send commands to unknownsystems
Tools	• execute arbitrary commands • go through injection on connected tool systems • code execution in the agent's system
Data repositories	• attack embedded databases • extract confidential data • change the data, which leads to fake results of the models
Models	• bypassing the protection model • make the model exhibit bias • extraction of data of other users and/or server data • forcing the model to exhibit intolerant behavior • poison the results of other users • violate the trust/reliability of the model • access to unpublished models

The inherent redundancy of the Dual-Layer Hybrid Security Framework addresses these vulnerabilities by ensuring that Layer 1 detection results are validated against Layer 2 policy and context, thereby reducing the success rate of model manipulation and poisoned outputs.

AI implementation is associated with several challenges, including data preparation, model building, scalability, and ethical issues. Companies need a systematic methodology to leverage several core business and technology capabilities to implement AI and machine learning technologies in the enterprise.

The traditional approach to automating the detection of malicious code involves using static analysis tools such as SonarQube, CodeQL, Snyk, and Coverity. These tools can be used at any time but are typically used to scan code for vulnerabilities after the code freeze phase and before the formal release processes are complete. They work by parsing the

source code into an abstract syntax tree or control flow graph that shows how the code is organized and how all the components (classes, functions, variables, etc.) are related to each other. Rule-based analysis and pattern matching are then used to identify a wide range of problems.

Static analysis tools can be integrated with IDEs and CICD systems throughout the development cycle, and many offer customizable configuration, query, and reporting options.

Static code analysis takes input and asks two things: What's wrong? How to fix it? Analyse this approach from the point of view of software transformation under the influence of artificial intelligence, presented in Figure 2.

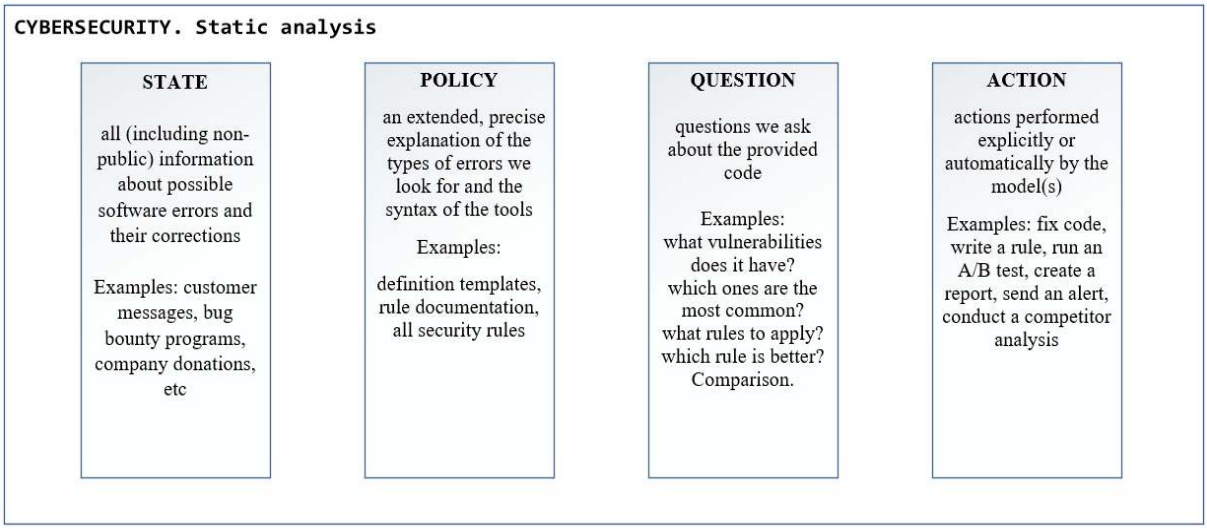

Figure 2. Static analysis in LLM-based applications

Artificial intelligence will transform all existing software into one that is based on understanding. Once it is sufficiently exposed to the problem through one's "state" and understands what one is trying to do through one's "policy", it can do much more than just find code problems and fix them.

It will be able to perform the following actions: find the problem; show how to fix it in any language (coding or human); write an instruction that will avoid these mistakes; write a rule in the tool's technology that would detect this; will provide you with a fixed code; and make sure the code works. This cognitive ability is achieved through the integration of the dual-layer approach, which enables the system to interpret errors within a specific organizational context rather than merely identify them.

In addition, it is possible to build multiple versions of a cyber defence system to see how each version will respond to the most common attacks and then make recommendations based on those results.

2. Building a Security System

2.1. Algorithm for Building a Security System Using LLM Models

The proposed Dual-Layer Hybrid Security Framework operationalizes the transition from circuit-based to intelligence-based architectures. This framework bifurcates security operations into two specialized tiers. Layer 1 serves as the detection engine, utilizing a Random Forest algorithm to provide high-speed, real-time anomaly detection within network traffic. Layer 2 acts as the interpretation engine, where a Large Language Model ingests the alerts from the primary layer to generate human-readable incident summaries, map threats to specific security policies, and provide actionable remediation steps.

1. Choose a base model. Start with the latest general GPT model from OpenAI or alternatives like Gemini from Google and Meta. Many companies are anticipated to implement advanced language models, which may be designated as OpenAI GPT-4. It has an impressive breadth of knowledge across various fields, including security protocols, biotechnological advancements, project management strategies, effective planning, meeting facilitation, budget management, incident response tactics, and audit preparedness. This expertise positions it as a crucial resource for companies looking to navigate complex challenges and ensure operational efficiency. However, to fully leverage its capabilities, organizations need to provide a more personalized context that aligns with their specific industry needs and operational goals. This tailored approach will allow companies to maximize the potential benefits of GPT-4's insights and recommendations.

2. Develop a custom machine learning model that leverages company-specific data relevant to GPT-4 queries. This data set should encompass a variety of sources, including the status section, telemetry information, company context details, firewall logs, financial documents, chat conversations, email communications, and transcripts from meetings.

Make sure to thoroughly train the model on this diverse dataset to enhance its accuracy and relevance.

3. Train your policy model. A separate model is meticulously crafted to ensure alignment with your company's mission and objectives. This model takes into account the challenges you face and integrates your strategic business priorities (Klochan et al., 2021), creating a cohesive framework that supports your organization's vision and enhances overall effectiveness. We use the guidance we get from people to drive part of the action architecture. Artificial intelligence will do this with the help of rules formed in the policy model.

4. Instruct the system to execute the following action: the models have now been merged. We have integrated GPT-4 with both our state model and policy model. This powerful combination allows them to analyze and interpret our behavior and preferences in ways that often surpass our own understanding. Together, they create a comprehensive picture of who we are, delving into the nuances of our thoughts and actions with remarkable insight.

2.2. Model task

We are developing a comprehensive software application designed for network traffic analysis and anomaly detection, leveraging advanced artificial intelligence techniques. The following software application demonstrates the practical execution of Layer 1 within the proposed framework, focusing on the technical requirements for robust, automated detection of suspicious traffic patterns. It will utilize synthetic data to train the model, ensuring it can accurately identify unusual patterns and potential threats within network traffic. By simulating various traffic scenarios, we aim to enhance the model's robustness and effectiveness in real-time monitoring and security assessment. This project will provide critical insights into network behavior, helping organizations proactively address anomalies and safeguard their digital infrastructure. All information transmitted over the Internet is divided into smaller units known as packets. Each packet contains a specific set of data that is addressed to a designated destination, much like how physical mail is sent to a particular address.

1. Installing and importing libraries. The code is shown in Fig. 3:

```python
import pandas as pd
import numpy as np
from sklearn.model_selection import train_test_split
from sklearn.ensemble import RandomForestClassifier
import gradio as gr
import warnings
warnings.filterwarnings('ignore')
```

Figure 3. Linking libraries

2. Creating a training data set. A software module is being developed to create a data set that represents a given network. This module will feature several key functions, including:

- ‘packet_size’: This function will determine the size of individual packets as they travel through the network, providing insights into traffic patterns.

- ‘duration’: This function will measure the time it takes for packets to traverse the network, helping to identify latency issues.

- ‘protocol_type’: This function will categorize the protocols used within the network, allowing for analysis of traffic types and their respective behaviors.

- ‘number_of_packets’: This function will count the total packets transmitted, enabling an understanding of network load and performance.

- ‘port_number’: This function will identify the specific ports in use, facilitating the analysis of communication endpoints and potential vulnerabilities.

Together, these functions will create a detailed representation of network activity, supporting performance analysis and optimization efforts. The values for these functions will be randomly generated using the NumPy library. The target variable ‘traffic_type’ indicates "normal" or "suspicious" traffic. The goal is to train a model for smart data analysis. The code is shown in Fig. 4:

```python
# Simulated dataset
np.random.seed(0)
n = 100
features = ['packet_size', 'duration', 'protocol_type', 'num_packets', 'port_number']
target = 'traffic_type'
# Protocol
protocols = ['TCP', 'UDP', 'ICMP']
# Generate random data
df = pd.DataFrame({
    'packet_size': np.random.randint(100, 1500, n),
    'duration': np.random.uniform(0, 120, n),
    'protocol_type': np.random.choice(protocols, n),
    'num_packets': np.random.randint(1, 100, n),
    'port_number': np.random.randint(1, 65535, n),
    'traffic_type': np.random.choice(['normal', 'suspicious'], n)
})
```

Figure 4. Creating a training data set

3. Creating a model. The code converts the DataFrame column named "protocol_type" into a numeric format, then splits the data into separate sets of functions and targets, and subsets for training and testing. Based on the input training data, the RandomForestClassifier model is trained. The code defines a prediction function that takes network traffic characteristics as input and converts them into the expected format and uses an already trained model to predict and determine the type of traffic ("normal" or "suspicious"), as shown in Fig. 5.

```
# Encoding data
df['protocol_type'] = df['protocol_type'].astype('category').cat.codes

# Split the data
X = df[features]
y = df[target]
X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.2, random_state=42)

# Train a simple model
model = RandomForestClassifier()
model.fit(X_train, y_train)

# Define the prediction function
def predict(packet_size, duration, protocol_type, num_packets, port_number):
    input_data = pd.DataFrame({
        'packet_size': [packet_size],
        'duration': [duration],
        'protocol_type': [protocols.index(protocol_type)],
        'num_packets': [num_packets],
        'port_number': [port_number]
    })
    prediction = model.predict(input_data)[0]
    return prediction
```

Figure 5. Data transformation and traffic forecasting

We anticipate that the proposed software application will be effective for monitoring and diagnosing network issues, and it may be enhanced with a graphical interface in the future.

Conclusions

Incorporating artificial intelligence (AI) alongside large language models (LLM) demands a comprehensive analysis of the system's architecture, as well as the implementation of robust security measures to mitigate potential challenges. It may also be worth exploring the concept of LLM pen-testing, where security professionals test applications to discover vulnerabilities against their LLM models.

Integrating AI-powered applications into cybersecurity is a significant shift that has the potential to revolutionize the industry in the foreseeable future. By leveraging AI, cybersecurity systems can better detect and respond to advanced threats, predict potential vulnerabilities, and adapt to

evolving attack techniques. This integration also enables the automation of routine tasks, allowing cybersecurity professionals to focus on more complex and strategic initiatives.

Using the Dual-Layer Hybrid Security Framework, SMEs can achieve robust cybersecurity by combining the efficiency of high-speed statistical models with the contextual depth of Large Language Models, thereby enhancing their overall security posture and staying ahead of sophisticated cyber threats. It becomes obvious that AI-powered applications offer ample opportunities for threat detection, risk assessment, and general intelligence enhancement. However, they also have potential cybersecurity issues that need to be addressed.

References

Bakhshandeh, A., Keramatfar, A., Norouzi, A., & Chekidehkhoun, M. M. (2023). Using ChatGPT as a static application security testing tool. (arXiv:2308.14434). DOI: 10.48550/arXiv.2308.14434

Bondarenko, S., Bratko, A., Antonov, V., Kolisnichenko, R., Hubanov, O., & Mysyk, A. (2022). Improving the state system of strategic planning of national security in the context of informatization of society. *Journal of Information Technology Management*, 14, pp.1-24. DOI: 10.22059/jitm.2022.88861

Demianchuk, M., Koval, V., Hordopolov, V., Kozlovtseva, V., & Atstaja, D. (2021). Ensuring sustainable development of enterprises in the conditions of digital transformations. *E3S Web of Conferences, 280, Article 02002*. DOI: 10.1051/e3sconf/202128002002

DNV. (2023). *Energy cyber priority 2023: Closing the gap between awareness and action*. Available online: https://www.dnv.com/cybersecurity/cyber-insights/energy-cyber-priority-2023/

Dikhaminjia, I., Tireuov, K., Qajaia, T., & Khussainova, Z. (2025). Research of some factors affecting discrimination in the organization and its impact on conflict situations. *Business Management*, 2025(2), pp. 47–63. DOI: 10.58861/tae.bm.2025.2.03

Ishchuk S., Sozanskyy L., Pukala, R. (2021). Optimisation of structural parameters of the industry by the criterion of product innovation, *Engineering Management in Production and Services*, Vol. 13, Issue 3, Bialystok 2021, pp. 7 – 24, DOI: 10.2478/emj-2021-0018

Kalinin, O. (2024). Investment Security in the Development of the Digital Economy. *Economics Ecology Socium*, 8(2), pp.73–84. DOI: 10.61954/2616-7107/2024.8.2-6

Kaminsky, O., Koval, V., Yereshko, J., Vdovenko, N., Bocharov, M., & Kazancoglu, Y. (2023). *Evaluating the effectiveness of enterprises' digital transformation by fuzzy logic. In Advances in Soft Computing Applications* (pp. 75–90). River Publishers.

Kazbekova D, Petrova M, Sushchenko O, Belgibayeva A, & Mitkov M. (2024). Mechanisms of Stimulation of Small- and Medium-Sized Entrepreneurship: The Experience of Kazakhstan. *Journal of Risk and Financial Management*. 17(7):257. DOI: 10.3390/jrfm17070257

Klochan, V., Piliaiev, I., Sydorenko, T., Khomutenko, V., Solomko, A., & Tkachuk, A. (2021). Digital platforms as a tool for the transformation of strategic consulting in public administration. *Journal of Information Technology Management*, 13. DOI: 10.22059/JITM.2021.80736

Koch, C. (2023*). I used GPT-3 to find 213 security vulnerabilities in a single codebase. Better Programming*. Available online: https://betterprogramming.pub

Lelyk, L., Olikhovskyi, V., Mahas, N., & Olikhovska, M. (2022). An integrated analysis of enterprise economy security. *Decision Science Letters,* 11(3), pp.299–310. DOI: 10.5267/j.dsl.2022.2.003

Noever, D. (2023). Can large language models find and fix vulnerable software? (arXiv:2308.10345). arXiv. DOI: 10.48550/arXiv.2308.10345

Ozkan-Ozay, M., E. Akin, O. Aslan, S. Kosunalp, T. Iliev, I., & Stoyanov, I. Beloev (2024). A Comprehensive Survey: Evaluating the Efficiency of Artificial Intelligence and Machine Learning Techniques on Cyber Security Solutions *IEEE Access*, 12, pp.12229-12256, DOI:10.1109/ACCESS.2024.3355547

Popov, O., Choch, V., Iatsyshyn, A., Kovach, V., Semenets-Orlova, I., & Iatsyshyn, A. (2024). Artificial intelligence application in remote UAV methods. In V. Babak & A. Zaporozhets (Eds.), Systems, Decision and Control in Energy VI (Vol. 561, pp. 1–13). Springer, Cham. DOI: 10.1007/978-3-031-61011-0_1

Popova, P., Popov, V., Marinova, K., Petrova, M. & K. Shishmanov. (2024). The Digital Platform — new opportunities and implementation strategy. 1*6th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, Iasi, Romania, 2024, pp. 1-9, DOI: 10.1109/ECAI61503.2024.10607401

Popova, P., Popov, V., Marinova, K., &Petrova, M. (2023). The Role of Digital Platforms and Big Data Analytics as a Base for Digital Service Innovation. *2023 4th International Conference on Communications, Information, Electronic and Energy Systems (CIEES)*, Plovdiv, Bulgaria, 2023, pp. 1-8, DOI: 10.1109/CIEES58940.2023.10378780

Popova, P., & Petrova, M. (2024). The Role of AI for Smart Environments based on Big Data and IoT Applications," *2024 5th International Conference on Communications, Information, Electronic and Energy Systems (CIEES)*, Veliko Tarnovo, Bulgaria, 2024, pp. 1-8, DOI: 10.1109/CIEES62939.2024.10811252

Pukala R. (2016). Use of neural networks in risk assessment and optimization of insurance cover in innovative enterprises, *Engineering Management in Production and Services*, 8 (3), Bialystok 2016, pp. 43 – 56, https://doi.org/10.1515/emj-2016-0023.

Pukala R., & Petrova M. (2019). Application of the AHP method to select an optimal source of financing innovation in the mining sector, *E3S Web of Conf.,* 105, 04034, DOI:10.1051/e3sconf/201910504034

Tairov, I., Stefanova, N., Aleksandrova, A., & Aleksandrov, M. (2024). Review of AI-Driven Solutions in Business Value and Operational Efficiency. *Economics Ecology Socium*, 8(3), 55–66. DOI: 10.61954/2616-7107/2024.8.3-5

Yermachenko, V., Bondarenko, D., Akimova, L., Karpa, M., Akimov, O., & Kalashnyk, N. (2023). Theory and practice of public management of smart infrastructure in the conditions of the digital society' development: Socio-economic aspects. *Economic Affairs* (New Delhi), 68(1), pp. 617-633. DOI: 10.46852/0424-2513.1.2023.29