STATE UNIVERSITY OF INFORMATION AND COMMUNICATION TECHNOLOGIES

ABSTRACTS OF REPORTS OF THE INTERNATIONAL SCIENTIFIC AND PRA CTICAL CONFERENCE DIGITAL TRANSFORMATION: STRENGTHENING THE CYBERSECURITY CAPACITIES IN THE MODERN WORLD

4-5 November

Krakow 2025

ISBN 978-617-8580-10-0
UDC 004.056.5:004.9]:001.891.3

Digital Transformation: Strengthening the Cybersecurity Capacities in the Modern World : abstr. of rep. of the Intern. Sci. and Practical Conf., (Krakow, 4-5 November 2025) / Ministry of Education and Science of Ukraine, State University of Information and Communication Technologies / eds.: V. Shulha (ed.) [et al.]. Kyiv : Pro Format, 2025. 76 p.

This volume contains the abstracts of reports presented at the International Scientific and Practical Conference “Digital Transformation: Strengthening the Cybersecurity Capacities in the Modern World”, devoted to current issues of digital transformation, cybersecurity, and software engineering in the context of modern hybrid threats.

The proceedings reflect the results of scientific research in the fields of information security, artificial intelligence in cybersecurity, detection and prevention of cyberattacks, cloud security, Internet of Things, cryptographic methods, radio-electronic systems, information warfare, social engineering, DevSecOps practices, as well as cybersecurity of critical infrastructure and on-board equipment.

The presented abstracts address modern mathematical models, methods, and algorithms for cybersecurity assessment, intelligent approaches to threat detection, machine learning and explainable artificial intelligence, Zero Trust architectures, and practical aspects of implementing secure digital technologies in governmental, educational, and corporate environments.

The proceedings are intended for researchers, academic staff, PhD students, higher education students, cybersecurity and information technology professionals, as well as all those interested in issues of digital transformation and information security.

CONFERENCE ORGANIZERS

- State University of Information and Communication Technologies (Ukraine).
- University of the National Education Commission in Krakow (Poland).
- Science, Entrepreneurship, Technology University.

CHAIRMEN OF THE PROGRAMME COMMITTEE

- Mr. Jaroslaw Ponder, Head of the ITU Office for Europe.
- Prof. Piotr Borek, Rector, University of the National Education Commission, Krakow.
- Prof. Volodymyr Shulha, Rector, State University of Information and Communication Technologies.

MEMBERS OF THE PROGRAMME COMMITTEE

- Prof. Olga Wasiuta, University of the National Education Commission, Krakow.
- Prof. Oleksandr Korchenko, State University of Information and Communication Technologies.
- Prof. Serhii Semenov, University of the National Education Commission, Krakow.

CONTENTS

TECHNIQUES FOR IDENTIFYING ANONYMOUS USERS IN CRITICAL INFRASTRUCTURE

Ivan Azarov[1], Oleksandr Korchenko[2], Anna Korchenko[3], Ihor Ivanchenko[4] and Illia Azarov[5]
[1,2,4] *State University of Information and Communication Technologies, Solomianska 7, 03110 Kyiv, Ukraine*
[3] *Dnipro University of Technology, Avenue 19, 49005 Dnipro, Ukraine,*
[5] *National Aviation University, Liubomyra Huzara Avenue 1, 03058 Kyiv, Ukraine*

Abstract

This research is dedicated to the analysis of modern techniques for the identification of anonymous users in the context of protecting critical infrastructure facilities. Popular techniques of active and passive methods for generating user digital fingerprints are analyzed, their essence and characteristics are described, and the key advantages and disadvantages of their application for user identification are determined. It has been determined that the optimal criteria for identifying anonymous users are not the collection of a unique fingerprint, but rather the verification of functionality and availability and the identification of spoofed or masked functions to ensure the cyber defense of critical infrastructure information resources (CIIR).

Keywords

Anonymous user identification, cyber defense of critical infrastructure, browser fingerprinting

Introduction

The number of digital technologies grows daily, leading to the emergence of new cyber threats. There is a pressing need to improve techniques for detecting anonymous users, as malicious actors frequently exploit anonymity to carry out cyberattacks. Identifying anonymous users allows for the prevention and minimization of cyber incidents, thereby safeguarding critical state infrastructure through the monitoring and restriction of actions by unauthorized persons.

Therefore, the objective is to determine the optimal criteria/attributes by analyzing modern techniques for identifying anonymous users to improve the level of cybersecurity for digital objects of critical infrastructure.

Below, we examine modern technologies for extracting unique characteristics of user devices and browsers that remain stable even in incognito mode.

Theoretical foundations for the development of techniques for identifying anonymous users.

In the current conditions of the continuous evolution of cyberattack techniques, the use of traditional static methods of user identification is insufficient. The formation of a digital fingerprint is based on the principle of variable combinations of unique browser attributes, operating system (OS) settings, and user device characteristics [1].

A comprehensive analysis of modern user identification techniques allows for their detailed examination, determination of advantages and disadvantages, and drawing certain conclusions regarding their application for identifying anonymous users in countering cyber threats to critical infrastructures.

Active browser fingerprinting techniques:

The main feature of obtaining a user fingerprint using active techniques consists in the targeted active scanning and computation on the user's browser side to obtain informative results regarding the individually-variable functional capabilities of the device's software and hardware. Active techniques can be classified into the following identification categories: Software and hardware includes : ECMAScript objects, Graphic identification characterized by: Canvas, WebGL, WebGPU, Emoji, and Font identifier fingerprints, Audio identification based on : the Web Audio API, Browser features include: CSS properties, Browser storage contains attributes: Cookies, LocalStorage, SessionStorage, IndexedDB, Network identification includes : Fetch API, WebSockets, WebRTC, Service Workers, Browser extensions and User behavior [2].

Passive techniques for obtaining a device's digital fingerprint:

The use of these device-fingerprinting techniques enables passive analysis of information about baseline configurations, software-hardware usage patterns of the user, and connection behavior with server infrastructure, without requiring active computation on the client side. The methods examine TLS/SSL handshakes, TCP/IP stack characteristics, and HTTP/2 frame patterns, which reveal the use of a particular type or version of the user's software-hardware stack. This approach remains effective even when active techniques are disabled on the client side and allows detection of anonymization tools. For critical infrastructure, protocol fingerprinting provides a basic level of visibility at the network layer, enabling the identification of automation tools with high accuracy [3,4].

Based on the conducted research, a comparative table (Table 1) has been constructed.

Table 1. Comparative table of user digital fingerprinting methods.

Method name	Type	Attribute category	Stability	Uniqueness	Resistance to masking	Anonymity detection	Automation and bot detection
ECMAScript objects	Active	Software and hardware	High	Medium	Low	High	High
Canvas	Active	Graphic	Medium	Medium	Low	Low	Medium
WebGL	Active	Graphic	Medium	Medium	Low	Low	High
WebGPU	Active	Graphic	Medium	High	Medium	Low	High
Emoji	Active	Graphic	High	Low	Low	Low	Low
Font finder	Active	Graphic	Low	Medium	Low	Low	Medium
Web Audio API	Active	Audio	Medium	High	Medium	Low	Medium
CSS	Active	Browser feature	High	Low	High	Low	Low
Cookies	Active	Browser storage	High	Low	High	High	High
LocalStorage	Active	Browser storage	High	Low	High	High	High
SessionStorage	Active	Browser storage	High	Low	High	High	High
IndexedDB	Active	Browser storage	High	Low	High	High	High
Fetch API	Active	Network	Medium	Low	Medium	Low	Low
WebSockets	Active	Network	Medium	Low	Medium	High	High
WebRTC	Active	Network	Medium	High	Low	High	High
Service Worker	Active	Network	Medium	Low	Low	High	High
Browser Extensions	Active	Extension	Low	High	High	High	High
Behavior	Active	Behavioral	Low	High	Low	High	High
HTTP/S / HTTP/2	Passive	Protocols	Medium	Medium	Low	High	High
TCP/IP	Passive	Protocols	Medium	Medium	Low	High	High
TLS/SSL	Passive	Protocols	Medium	Low	Low	Medium	Medium

Conclusions

Based on a comprehensive analysis of existing active and passive browser and user device fingerprinting techniques for detecting anonymous users, an optimal solution has been determined based on the defined criteria: Stability, Uniqueness, Resistance to masking, Anonymity detection, and Automation and bot detection. This solution relies on a combination of techniques: (ECMAScript objects, browser storage, browser extensions, and the Service Worker API) for identifying the browser and its mode, WebRTC for detecting network masking, and user behavioral characteristics, which will allow for the prevention of potential cyber threats directed against the state's critical infrastructure.

References

[1] Kumar, V., & Paul, K. (2023). Device fingerprinting for cyber-physical systems: A survey. ACM Computing Surveys, 55(14s), 1-41.

[2] Zhang, D., Zhang, J., Bu, Y., Chen, B., Sun, C., & Wang, T. (2022). A survey of browser fingerprint research and application. Wireless Communications and Mobile Computing, 2022(1), 3363335.

[3] Laperdrix, P., Bielova, N., Baudry, B., & Avoine, G. (2020). Browser fingerprinting: A survey. ACM Transactions on the Web (TWEB), 14(2), 1-33.

[4] Li, S., & Cao, Y. (2020, October). Who touched my browser fingerprint a large-scale measurement study and classification of fingerprint dynamics. In Proceedings of the ACM Internet Measurement Conference (pp. 370-385).

ALGORITHMIC SOFTWARE FOR CYBERSECURITY POSTURE EVALUATION OF CLOUD SERVICES

Volodymyr Shulha[1], Yevheniia Ivanchenko[2], Ihor Ivanchenko[3], Yevhenii Pedchenko[4] and Maryna Pedchenko[5]
[1,2,3,4,5] *State University of Information and Communication Technologies, Solomianska 7, 03110 Kyiv, Ukraine*

Abstract

This article provides a detailed description of the need to conduct an evaluation of the cybersecurity posture of cloud services, as well as the consequences of insufficient protection. In addition, a brief description of the mathematical model and method for evaluating the cybersecurity posture of cloud services is presented. A structural model of the system for evaluating the cybersecurity posture of cloud services, developed on the basis of the model and method, is also introduced. Furthermore, building upon the developed mathematical model and method, as well as the structural model of the system, a detailed description of the developed algorithmic software for evaluating the cybersecurity posture of cloud services is provided. This software outlines the stages of execution and the modules for evaluating cloud services, along with a visual representation of the sequential algorithms of the network application.

Keywords

cybersecurity, information security, assessment, mathematical model, mathematical method, structural model, algorithm, audit, CSP, Cloud Service Provider, IaaS, PaaS, CaaS, FaaS, SaaS, cloud assessment

Introduction

Cloud services have become a foundational component of modern business operations because they make it easier to scale computing resources and accelerate service development. At the same time, the benefits of cloud adoption can quickly turn into major risks when organizations misconfigure cloud settings or grant excessive access rights on the server side: such weaknesses may lead to confidential data leakage and disruptions in business continuity.

A key argument is that cyber incidents in globally known companies repeatedly demonstrate how cloud security gaps materialize into real-world damage. Examples: Capital One (2019) where attackers gained temporary accounts and access to AWS-based resources due to misconfigurations in a Web Application Firewall; Snowflake (2024) where the absence of Multi-Factor Authentication enabled large-scale customer account breaches through password guessing; Microsoft (2023) where overly permissive SAS token settings exposed around 38 TB of data from Azure storage; and Toyota (2023) where cloud misconfigurations led to public exposure of customer data.

The purpose of the research is developing algorithmic software for evaluating the cybersecurity posture of cloud services used by information infrastructure objects.

This article explain that the algorithmic software is grounded in previously developed components: a mathematical model, a mathematical method, and a structural model of an evaluation system, which together should form a basis for creating network software that helps auditors assess cloud security configurations and identify areas that require improvement [1].

Mathematical model for evaluating the cybersecurity posture of cloud services.

Mathematical model that evaluates cloud services across a set of parameters which include question sets, answer options, and recommendations. The model is intended to be applicable to major cloud service models such as IaaS, CaaS, PaaS, FaaS, and SaaS, and its generalized component is denoted as CSP (Cloud Service Provider).

The model consists of 11 parameters (modules), each targeting a specific security dimension of cloud service use and management. In summary, these modules include: General Points (identifying the type/name of the cloud service and checking cooperation with aggressor countries), Network, Storage, Server, Virtualization, Operating System, Container Technology, Runtime (including logging, anomaly/vulnerability detection, and service operability checks), Application, Data (data processing methods and their operational impact), and a Recommendations module that produces guidance based on auditor responses.

The mathematical model for evaluating the cybersecurity posture of cloud services of information infrastructure objects has the following generalized form, which is presented in Formula 1:

$$\boldsymbol{CSP} = \left\{ \bigcup_{i=1}^{n} \boldsymbol{CSP}_i \right\} = \left\{ \boldsymbol{CSP}_1, \boldsymbol{CSP}_2, \boldsymbol{CSP}_3, \ldots, \boldsymbol{CSP}_7, \ldots, \boldsymbol{CSP}_{11} \right\} = \left\{ \boldsymbol{GP, N, S, SR, V, OS, CT, R, A, D, RE} \right\}, \quad (1)$$

where $\boldsymbol{CSP}_i \subseteq \boldsymbol{CSP}$ $(i = \overline{1,n})$ – a key component of the tuple model of characteristics, representing the i-th identifier of the cloud service evaluation parameter, where n – is their total number [2].

Mathematical method for evaluating the cybersecurity posture of cloud services.

A mathematical method that enables calculation of all 11 parameters, with the final assessment depending both on the auditor's responses and the specifics of the evaluated cloud service. A 0–5 scoring scale is used, where 0 represents the lowest score and 5 the highest.

The method is implemented through 11 evaluation stages. The stages begin with collecting general information about the cloud service and its cooperation with aggressor countries, then continue through assessing security levels for network, storage, server, virtualization, operating system, container management, business continuity/runtime, application management, and data processing/management, and finally conclude with defining criteria for calculating the total points based on the auditor's responses [3].

Structural model for evaluating the cybersecurity posture of cloud services.

Building on the model and method, a structural model of the evaluation system that includes both databases and functional modules was developed. The system maintains an evaluation results database and multiple question databases aligned with the assessment modules (general, network, storage, server, virtualization, operating system, containerization, business continuity, applications, data processing). It also includes databases for recommendations and reference values, and contains functional modules for evaluation initialization, data acquisition, module-by-module evaluation, storing results, and visualizing results.

This structural model is positioned as the "system backbone" that supports consistent execution of the method and provides the persistence needed for reusing results, comparing evaluations, and generating reports [4].

Network application concept and algorithmic software

A central practical contribution of the article is the conceptual scheme of a secure network application that auditors can use. The workflow described begins when an auditor opens a browser, navigates to the web application, and enters credentials. The credentials are verified against hash values stored in the database; if correct, the auditor receives a one-time session token valid only for the current session, granting access to the application. After authorization, the auditor can review existing evaluations or conduct a new evaluation across the main cloud service modules, and all responses and results are stored in the database for later review and reporting [5].

The reporting capability is emphasized: the auditor can generate a final report containing per-module/parameter details, the total score achieved, and recommendations regarding further cloud service use. The report also includes recommendations for each answered question, such as best practices for using specific service functionalities or alternatives when required functionalities are missing.

On top of the conceptual network application scheme, was developed "algorithmic software" composed of several complementary blocks. These blocks represent the sequential logic of the application and the auditor's actions: "Auditor Authorization," "Conducting a New Evaluation," "Selection of an Evaluation" for managing completed assessments, and "Report Generation" for producing and presenting results and recommendations. The article notes that the authorization flow includes credential entry, token generation, and server-side verification, while the evaluation flow includes selecting parameters according to the chosen cloud service type [1].

Conclusions

The research presented the mathematical model, method, and structural model for evaluating cloud service cybersecurity posture, and that these elements formed the basis for developing algorithmic software. This algorithmic foundation enables the creation of network software that provides auditors with a prepared platform for fast and high-quality audits of cloud services used by client companies, delivering clear recommendations to remediate vulnerabilities before a cyber incident occurs. The expected benefit is a reduction of reputational and financial losses and an overall improvement of the cybersecurity level of cloud services used by businesses.

References

[1] Pedchenko Y. Methods and models of assessing the state of cybersecurity of cloud services of information infrastructure objects : dissertation of PhD in Cybersecurity. Kyiv, 2025. 254 p.

[2] Ivanchenko I., Pedchenko Y. Secure web application model for cybersecurity assessment of cloud service providers. Scientific Notes of the State University of Information and Communication Technology. Kyiv, 2024. No. 2. 116-134 p. DOI: https://doi.org/10.31673/2518-7678.2024.025842

[3] Pedchenko Y., Ivanchenko I. The method of assessing the cyber security of cloud services of information infrastructure objects. Modern Information Security. 2024. No. 3. 75-84 pp. DOI: https://doi.org/10.31673/2409-7292.2024.030008.

[4] Ivanchenko I., Pedchenko Y. Structural model of the cybersecurity assessment system of cloud services of information infrastructure objects. Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique». 2024. Vol. 1, No. 25. 505-515 pp. DOI: https://doi.org/10.28925/2663-4023.2024.25.505515.

[5] Korchenko O., Ivanchenko Y., Ivanchenko I., Pedchenko Y., Petrovska M. The system of secured user's credentials transfer. CPITS-II 2024: Cybersecurity Providing in Information and Telecommunication Systems II 2024. 2024. Vol. 3826. 168-173 pp. URL: https://ceur-ws.org/Vol-3826/short3.pdf.

THREATS TO A DIGITAL LEARNING SPACE

Serhii Zybin[1,2], Olha Suprun[2], Oleksandr Piroh[3]
[1] *State University of Information and Communication Technologies, Solomianska 7, 03110 Kyiv, Ukraine*
[2] *Taras Shevchenko National University of Kyiv, Bohdana Havrylyshyna 24, 04116 Kyiv, Ukraine*
[3] *Zhytomyr Polytechnic State University, Chudnivska 103, 10005 Zhytomyr, Ukraine*

Abstract
The purpose of the article is to analyze the main cybersecurity threats on higher education in Ukraine. For this purpose, a cross-sectional survey study was chosen. The primary tool in the study was a cross-sectional questionnaire.

Keywords
cybersecurity, cyber threat, cyber hygiene, national strategy, technology

Introduction

The main research problem is the growing vulnerability of Ukrainian higher education to cyber threats. The focus of this article is to provide a detailed analysis of the leading cyber threats affecting higher education and assess the effectiveness of existing protection measures.

Results and Discussion

The results show that digital technologies have increased dramatically in the Ukrainian higher education system in recent years. Accordingly, only 7% of respondents have not faced cyber threats while studying or teaching. The most common cybersecurity threat is viruses and malware (identified by 39.4%). Hacking of university platform accounts (26.8%), phishing (14.1%), and personal information leakage (12.7%) are also common. At the same time, most respondents rarely face cyber threats, with only 7% experiencing them constantly during their studies or teaching.

The analysis of the responses showed that universities where teachers participated in digital competence training or received cybersecurity training had significantly fewer cases of cyberattacks. In addition, professors with high cybersecurity knowledge actively teach students the key basics of online protection. This also reduces the risk of incidents.

Conclusions

Consequently, the most common threats to a secure digital learning space are viruses and malware, hacking of university platform accounts, phishing attacks, and personal data leakage. The surveyed participants in the educational process have an average awareness of ensuring an adequate digital space, indicating the need to improve cybersecurity protection policies. The respondents' answers pointed to the importance of optimising the cybersecurity space by integrating a two-factor authentication system for students and teachers, implementing system audits, more expansive use of automated threat detection systems, and using encryption to protect data. At the same time, the findings showed that training staff and students to detect phishing attacks and other types of social engineering is a vital protection aspect. The study proved the need to introduce mandatory digital literacy and cyber awareness training and tests. These measures should be implemented to improve cybersecurity in Ukrainian universities.

METHOD OF SEARCHING DIGITAL ILLEGAL MEANS OBTAINING INFORMATION BASED ON CLUSTER ANALYSIS

Oleksandr Laptiev1, Andrii Sobchuk[2], Tetiana Laptieva [3],, and Sergey Laptiev[4],
1 Taras Shevchenko National University of Kyiv, Volodymyrska Str., 60, Kyiv, 01033, Ukraine
2 State University of Information and Communication Technologies, Solomyanska Str., 7, Kyiv, 03110, Ukraine
3*National Technical University «Kharkiv Polytechnic Institute»,2, Kyrpychova str., 61002, Kharkiv, Ukraine 4State University «KYIV Aviation institute», 1, Liubomyra Huzara ave., 03058, Kyiv, Ukraine*

Abstract

The article explores a multipositional digital eavesdropping device detection method based on clustering, showing current techniques are ineffective amid legal signals in multi-agent environments. A bee colony algorithm with direct agent communication improves clustering reliability by 6–12% over k-means.

Keywords
Information protection, inbound device, multi-agent system, clusterization, cybersecurity.

Introduction

Modern covert surveillance tech, especially advanced GSM bugs with LPI and frequency-hopping, thrives in today's congested RF spectrum. Legitimate emissions from Wi-Fi, Bluetooth, cellular systems, and other devices mimic spy transmitters, complicating detection. Effective TSCM now requires agile, sensitive systems with advanced algorithms to distinguish malicious signals from dense, benign RF noise.

Purpose of the study

This study proposes a multi-position, multi-agent clustering method based on artificial bee colony optimization with direct communication to reliably detect covert bugs in congested RF environments, overcoming classical clustering limits and enabling real-time, unsupervised discrimination of LPI transmitters masked by legitimate signals like GSM or Wi-Fi.

Presenting main material

The work of the multiagent optimization method with direct communication between agents to perform clustering can be represented as the following algorithm: 1. Forming a search space with *m* cells. Cells are formed by dividing the radio frequency range into separate clusters corresponding to a certain type of radio transmitter (legal and illegal). Because agents are physically located at different points in space, the overall picture they will perceive will be somewhat different.

Agents that inform other agents about the cell to which the object is distributed include the following agents:

1. Agents whose object is not further than the center of the cell $\Delta\left(D_n\left(C^l, o_r^l\right) < \Delta\right)$, provided that there are 3 or more objects in the cell. It is chosen experimentally and depends on the specific practical task. Half of such agents are randomly selected and they inform other agents about the corresponding cell.

2. Agents whose object belongs to a cell in which the object is unique $\left|o^l\right| = 1$. Half of such agents are also randomly selected to inform about the objects being distributed.

All agents that are not included in the group of agents that perform information are automatically included in the group of agents that analyze information from other agents.

After dividing into groups for each agent that analyzes the information, the distance between the object that it distributes and between the objects that distribute agents belonging to the informing group of agents is calculated. If the minimum of the resulting differences is less than ΔD, then the object that distributes the informed agent is duplicated in the cell with the object that distributes the corresponding informing agent.

11. Natural selection. Since one object can be in several cells at the same time, you need to select and leave each object in only one cell. To do this, you must perform the selection procedure. It is proposed to perform a rigid selection, according to which for each object it is necessary to take into account how close it is to each of the centers of the cells $D\left(C^l, o_r^l\right)$, weighted by the normalized distance for the current cell. Therefore, it is necessary to leave the object in the cell in which the given weighted distance is the smallest

$$q = \arg\min_l \left[D\left(C^l, o_r^l\right) \cdot \left(1 - D\left(C^l, o_r^l\right)\right) \right], \forall l = \overline{1, m}, \quad (5)$$

where q is the cell in which you want to leave the object o_r .

12. *t: = t + 1* - go to the next iteration.

13. If *t <tmax*, then perform the transition to step 3, otherwise - go to step 14.

14. Calculate the end centers of clusters. Each individual cell is considered a cluster. Based on the objects in the cells, calculate the centers of the clusters:

$$x_i^c = \frac{1}{N^c} \cdot \sum_{j \in O^c} x_i^j \quad . \tag{6}$$

15. The end.

In developing this method, some features are taken into account that provide a match for the optimal solution:

1. Direct communication between agents is ensured by the exchange of information between agents, through which some agents can obtain information about search areas in which they were not and from which they are far away. Thus, a better study of the search space is achieved, which has a positive effect on the convergence to the optimal solution.

2. The introduction of the natural selection procedure allows to exclude objects from clusters for which the location conditions are unsatisfactory. To do this, a measure is introduced that characterizes the conditions of the object in the cluster, as the distance of the object to the center of the cluster, weighted by the normalized distance, taking into account both the absolute value of the distance and the relative impact of the object as a whole.

3. To better study the search space, it is suggested to perform step 6 several times, which will allow each agent to study the area in which he is in more detail.

To compare the accuracy of clustering, 150 experiments were performed, during which the electronic situation in the middle and around the room was recorded by two parameters (operating frequency and signal strength), after which

the results were processed by the known k-means method and the proposed multi-agent method. In general, the method of k-means gives from 12 to 18% of errors in the classification of signal samples, while the multi-agent method 6 - 8%. Thus, multi-agent clustering using direct communication between agents proves greater efficiency compared to classical methods. Another positive point is the lack of need for a priori assumptions about the number and nature of clusters.

Conclusion

To counter advanced digital eavesdropping devices that mimic legal signals, this work proposes a multi-position, multi-agent detection system using an artificial bee colony algorithm with direct agent communication. Unlike classical clustering—limited by needing predefined cluster counts and high interactivity—this approach enables real-time, unsupervised recognition of illicit RF emissions. Agents spatially scan the spectrum, share findings, and collaboratively classify signals, improving clustering reliability by 6–12% over traditional methods.

References

[1] Barabash O., Sobchuk V., Sobchuk A., Musienko A., Laptiev O.. Algorithms for synthesis of functionally stable wireless sensor network // Advanced Information Systems. 2025. V. 9, № 1. pp. 70–79. DOI: https://doi.org/10.20998/2522-9052.2025.1.08.

[2] Petrivskyi V., Shevchenko V., Yevseiev S., Milov O., Laptiev O., Bychkov O., Fedoriienko V., Tkachenko M., Kurchenko O., Opirsky I.. Development of a modification of the method for constructing energy-efficient sensor networks using static and dynamic sensors // Eastern-European Journal of Enterprise Technologies. 2022. V. 1, № 9 (115). pp. 15–23. DOI: https://doi.org/10.15587/1729-4061.2022.252988.

IMPLEMENTING DEVSECOPS PRACTICES IN WEB DEVELOPMENT USING GULP AND ESLINT

Oleh Bondarenko[1], Artem Antonenko[2], Nataliia Lashchevska[3]
[1] *Higher Education Institution "Academician Yuriy Bugay International Scientific and Technical University", Kyiv, Ukraine*
[2] *National University of Life and Environmental Sciences of Ukraine, Heroes of Defense St. 15, .03041 Kyiv, Ukraine*
[3] *State University of Information and Communication Technologies, Solomianska 7, 03110 Kyiv, Ukraine*

Abstract
Modern web development requires integrating security early in the lifecycle ("shift-left"). This paper demonstrates implementing DevSecOps practices by integrating Static Application Security Testing (SAST) into a Gulp-based build pipeline. The objective is to automatically detect and block vulnerable JavaScript patterns. Using the gulp-eslint-new plugin and ESLint configured with security rules like no-eval, the system analyzes code during the build process. The pipeline is engineered to halt execution immediately upon detecting specific threats, preventing vulnerable code from reaching production. Experimental results confirm that the automated pipeline successfully identifies and blocks dangerous constructs. This approach provides a lightweight, effective first line of defense against common OWASP Top Ten vulnerabilities without requiring complex external infrastructure.

Keywords
DevSecOps, SAST, Gulp, ESLint, build automation, web security

Introduction

Modern web development demands rapid delivery cycles, yet security risks remain a critical concern. Vulnerabilities such as Cross-Site Scripting (XSS) consistently appear in industry reports, often stemming from unsafe coding practices. Traditional manual security reviews are insufficient for high-speed CI/CD environments. To address this, the industry is adopting DevSecOps strategies, specifically the "shift-left" principle, which moves security checks to the earliest stages of the lifecycle. Automated build tools like Gulp provide an ideal platform for this integration. This paper aims to demonstrate a practical method for embedding Static Application Security Testing (SAST) directly into Gulp pipelines using ESLint. This ensures that dangerous JavaScript patterns are automatically detected and blocked before code reaches the repository.

Configuration and Methodology

The foundation of this research relies on the widespread ESLint utility, adapted here for security auditing rather than just code style. The methodology follows the "white-box" testing approach. To detect vulnerabilities such as Remote Code Execution (RCE) or XSS vectors, specific security-focused rules were explicitly enabled in the configuration. Key rules include no-eval, which prohibits the use of the eval() function, and no-implied-eval, which prevents passing strings to setTimeout or setInterval. These patterns are identified by OWASP as significant risks [1], [2]. This configuration transforms the standard linter into a specialized SAST tool capable of identifying high-risk constructs at the syntax level.

Pipeline Integration

The core implementation involves modifying the Gulp build process to enforce a "fail-fast" policy. The gulp-eslint-new plugin was utilized to integrate ESLint into the pipeline [3]. A dedicated Gulp task, scriptLint, was created to process JavaScript files before transpilation or minification. The critical component of this integration is the eslint.failAfterError() method. Unlike standard logging, this method monitors the stream for error-level issues and throws a Gulp exception if any are found, immediately halting the build process. This mechanism ensures that no artifact containing detected vulnerabilities can be generated or deployed.

Experimental Results

To validate the system, a test environment was set up containing a JavaScript file with intentional vulnerabilities: a direct eval() call and a string-based setTimeout(). Upon executing the Gulp build command, the pipeline triggered the scriptLint task. The system successfully identified the dangerous patterns, outputting precise error messages to the console (Fig. 1). Crucially, the build process was automatically terminated, preventing the creation of the final distribution files. This experiment confirms that the proposed architectural approach effectively blocks insecure code execution and aligns with Node.js security best practices [4], serving as a reliable automated gatekeeper.

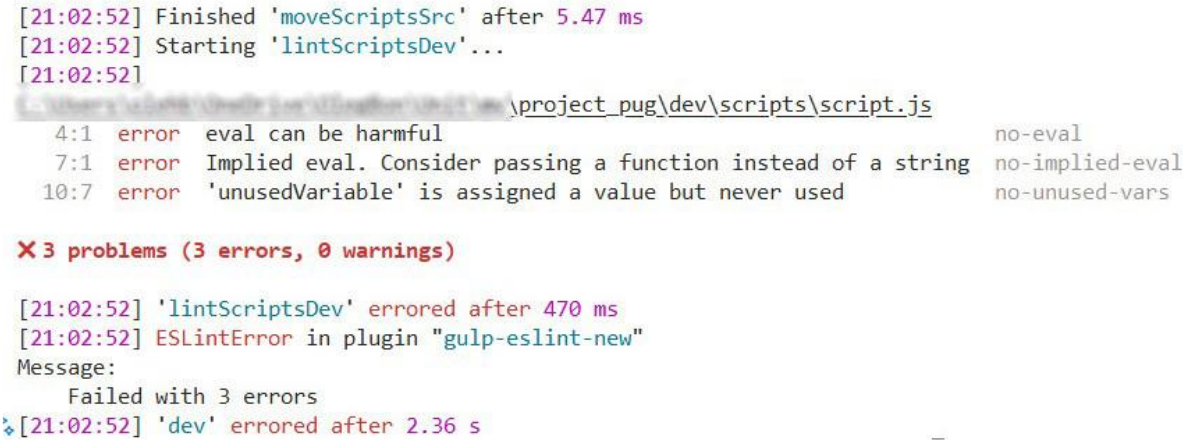

Figure 1. Result of executing the Gulp dev script with errors

Conclusions

The study confirms the effectiveness of integrating SAST tools into automated Gulp pipelines for front-end development. By configuring ESLint with security-focused rules and utilizing specific Gulp plugins, we created a system that automatically identifies and halts builds containing vulnerable JavaScript constructs. The experiment demonstrated that the pipeline successfully blocks high-risk patterns, preventing them from entering production. This approach validates that lightweight tools can serve as a robust first line of defense against common vulnerabilities, offering an accessible implementation of DevSecOps practices that aligns with modern security guidelines.

References

[1] OWASP Foundation. (2024). OWASP Top Ten. URL: https://owasp.org/www-project-top-ten/
[2] OWASP Foundation. (2025). Static Code Analysis. OWASP Community Pages. URL: https://owasp.org/www-community/controls/Static_Code_Analysis
[3] npm. (2025). gulp-eslint-new. URL: https://www.npmjs.com/package/gulp-eslint-new
[4] Node.js. (2025). Security Best Practices. URL: https://nodejs.org/en/docs/guides/security

METHOD FOR ENHANCING THE DETECTION SYSTEM OF DANGEROUS RADIO SIGNALS

Ivan Parkhomenko 1,†, Mykola Brailovskyi 2† ,Oleksandr Toroshanko 3,†Volodymyr Rovda4,† and Yuliia Khokhlachova 5,†

1,2,3 Taras Shevchenko National University of Kyiv, Volodymyrska Str., 60, Kyiv, 01033, Ukraine
4 State University of Information and Communication Technologies, 7, Solomyanska Str., Kyiv, Ukraine, 03110
5State University of Commerce and Economics / Kyiv National University of Commerce and Economics,19, Kyoto str., Kyiv, 02156, Ukraine

Abstract

This work boosts noise immunity in digital radio detection using linear/quadratic low-pass filters, achieving 23% SNR improvement via coherent signal accumulation and incoherent noise suppression, with applications in secure comms and electronic warfare.

Keywords

Noise immunity, digital radio signal, low-pass filtering, coherent summation, signal-to-noise ratio (SNR), covert communication, likelihood density estimation.

Introduction

Radio interference—any unwanted EM disturbance—degrades signal detection and parameter estimation. Noise immunity, defined as a system's ability to maintain performance amid interference, is critical in digital radio due to its "cliff effect." Enhancing it requires understanding interference statistics, spectral properties, and mitigation via filtering, diversity, or AI-driven techniques—especially in contested EM environments.

Purpose of the study

The primary objective of this research is to develop and validate a method for enhancing the noise immunity of automated systems designed for the detection and recognition of digital radio signals, particularly those employed in covert (silent) information reception. The study specifically investigates the efficacy of low-pass filtering techniques—both linear and quadratic in their response characteristics—in discriminating useful signal components from background interference through coherent and incoherent summation mechanisms. By analyzing statistical and spectral properties of filtered signals under varying correlation conditions, the work aims to quantify the achievable improvement in system robustness and to establish a theoretical and experimental basis for optimizing filter design in electromagnetically contested environments.

Presentation of main material

Almost all methods of noise immunity receive signals based on the principle of signal averaging and interference. This principle is that the summation process is performed. Moreover, the useful signal is summed up coherently, and the noise signal is incoherent. For the purpose of averaging the useful signal and interference, linear systems of two types are used: narrow band filters and low frequency filters. It is possible to optimize low pass filters or narrow band filters.

To consider the issue of interference filtering, let us assume that the narrowband filter itself does not distort the signal that has passed through it. An ideal bandpass filter is a filter with an amplitude-frequency response of the type:

$$K(\omega)=\begin{cases}1 \quad якщо \quad \omega_0-\dfrac{\Delta\omega}{2}\le|\omega|\le\omega_0+\dfrac{\Delta\omega}{2}\\ 0 \quad якщо \quad \left]-\infty,\omega_0-\dfrac{\Delta\omega}{2}\right[U\left]\omega_0+\dfrac{\Delta\omega}{2},\infty\right[\end{cases}, \tag{1}$$

The frequency response of the expression for (1) is the impulse transition characteristic, which will be determined by the expression:

$$h_\delta(t)=\frac{\Delta\omega}{\pi}\cdot\frac{\sin\dfrac{\Delta\omega t}{2}}{\dfrac{\Delta\omega t}{2}}\cos\omega_0 t, \tag{2}$$

Given that the digital signal is not a clear pulse [7-10], it is possible to calculate the envelope voltage at the output of an ideal filter when exposed to a rectangular pulse of duration:

$$x(t)=\begin{cases}X_m\cos\omega_0 t \quad якщо \quad 0\le t\le T\\ 0 \quad якщо \quad \left]-\infty,0\right[U\left]T,\infty\right[\end{cases}, \tag{3}$$

Using the envelope voltage theorem of the narrowband filter, we write the expression for the envelope voltage at the output of the filter:

$$Y_m(t) = \frac{1}{2\pi} \int_{-\infty}^{\infty} K_{fn}(j\omega) S_{X_m}(j\omega) e^{j\omega t} dt \quad , \tag{4}$$

$$K_{fn}(j\omega) = \begin{cases} 1 \quad якщо \quad -\frac{\Delta\omega}{2} \le |\omega| \le \frac{\Delta\omega}{2} \\ 0 \quad якщо \quad]-\infty, \frac{\Delta\omega}{2}[\; U \;]\frac{\Delta\omega}{2}, \infty[\end{cases} \tag{5}$$

Substituting expression (5) into expression (4), we get the expression:

$$Y_m(t) = \frac{X_m}{2\pi}\left(Si(\Delta\omega t) - Si(\Delta\omega(t-T))\right) \quad , \tag{6}$$

In fig. 1 dependency graphs of the duration of the influencing rectangular pulse (blue color - pulse duration T = 1, red color - T = 10, green color - T = 15 and black color - T = 20) on the frequency range (filter bandwidth).

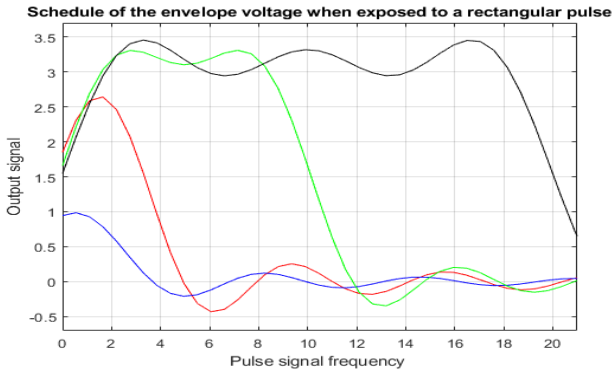

Fig. 1: Graph of the envelope voltage when exposed to a rectangular pulse signal

Conclusion

This work shows that narrowband low-pass filtering boosts noise immunity in digital radio detection by 23%, leveraging coherent signal vs. incoherent noise accumulation. Validated via statistical analysis and 2D likelihood estimation, it enhances robustness in contested EM environments—key for secure comms and electronic warfare.

References

[1] Lukova-Chuiko, N., Herasymenko, O., Toliupa, S., Laptieva, T., Laptiev, O. The method detection of radio signals by estimating the parameters signals of eversible Gaussian propagation. 2021 IEEE 3rd International Conference on Advanced Trends in Information Theory, ATIT 2021 – Proceedings. 2021. pp. 67–70.

[2] Laptiev O., Tkachev V., Maystrov O., Krasikov O., Open'ko P., Khoroshko V., Parkhuts L.. The method of spectral analysis of the determination of random digital signals. International Journal of Communication Networks and Information Security (IJCNIS). 2021. Vol 13, No 2, August pp.271-277. DOI: https://doi.org/10.54039/ijcnis.v13i2.5008

CONCISE ARCHITECTURE OF DUAL-CHANNEL RADIO SYSTEMS WITH A UNIFIED CRYPTOGRAPHIC CORE

Serhii Holdobin[1], Vitalii Hrunovych[2]
[1,2] *National Academy of the Security Service of Ukraine, Mykhaylo Maksymovycha 22, 03022 Kyiv, Ukraine*

Abstract
This paper presents a compact dual-purpose radio architecture that integrates two RF modules with a single cryptographic core. The proposed approach improves bandwidth utilization, reduces latency, and lowers power consumption compared to traditional dual-core designs. Shared synchronization, adaptive phase control, and centralized cryptographic processing enable secure and energy-efficient operation. Experimental validation confirms high synchronization accuracy, low error rates, and improved system stability, making the architecture suitable for military, special-purpose, and IoT communication systems.

Keywords
Dual-channel radio systems; dual RF modules; unified cryptographic core; secure radio architecture; synchronization; resource integration; FPGA-based implementation; low-latency communication; energy-efficient radio systems; multi-band communicationsg

Introduction

Modern communication systems increasingly require simultaneous multi-band operation combined with strong cryptographic protection. Dual-channel radio platforms are widely used in military, special-purpose, and advanced civilian networks to support these demands [1], [3]. However, such systems face challenges related to synchronization accuracy, mutual interference, and coordination of processing resources. Independent RF architectures offer implementation simplicity but suffer from reduced coherence and efficiency, while integrated designs provide higher robustness at the cost of increased architectural complexity [3], [4].

Therefore, the objective is to determine the optimal architectural and operational criteria by analyzing modern approaches to integrating dual RF modules with a unified cryptographic core in order to improve the efficiency, security, and energy performance of dual-purpose radio systems.

Below, we examine contemporary techniques for synchronization, centralized cryptographic processing, and coordinated resource management that ensure stable and secure operation of multi-channel radio architectures under varying operational conditions.

Integrated Dual-RF System Architecture

The proposed architecture integrates two RF modules within a single computing framework controlled by shared synchronization and data paths. The system is structured into three logical layers: a hardware layer for signal transmission and reception, a system layer responsible for synchronization and multiplexing, and a security layer that hosts the cryptographic core [5], [7]. Adaptive synchronization mechanisms and centralized resource management ensure coherent operation and reduced energy consumption.

Unified Cryptographic Core and Coordination:

A single cryptographic core is employed to perform encryption, authentication, and key management for both RF channels. Hardware-accelerated cryptographic processing enables low-latency operation while maintaining strong security properties [2], [4]. Centralized cryptographic control prevents cross-channel inconsistencies and improves synchronization stability compared to systems using separate cryptographic cores [5].

Experimental Evaluation and Optimization:

The architecture was evaluated through simulation and experimental validation using FPGA-based platforms with two independent RF modules. Performance metrics included throughput, transmission delay, synchronization accuracy, and power consumption [6]. Results demonstrated improved bandwidth utilization, reduced latency, and near-perfect synchronization when using a unified cryptographic core. Architectural optimization through adaptive resource allocation further reduced power consumption and improved system stability [7].

Conclusions

The study confirms that integrating two RF modules with a single cryptographic core significantly improves the efficiency of dual-purpose radio systems. Centralized synchronization and unified security processing reduce delay and energy consumption without compromising robustness or security [1], [5].

The proposed architecture provides a scalable and practical foundation for secure multi-band communication systems in military, special-purpose, and IoT applications.

References

[1] Smith, J. Dual-Radio Integration Techniques for Modern Communication Systems. IEEE Communications Magazine, Vol. 60, No. 4, 2022, pp. 54–67.
[2] Brown, T. Cryptographic Cores in Embedded Systems: Design and Performance. Springer, Berlin, 2021.
[3] Lee, K. Secure Multi-Frequency Radios for Tactical Networks. ACM Transactions on Embedded Systems, Vol. 21, No. 2, 2023, pp. 112–125.
[4] Lin, C. Dual-Channel Synchronization Algorithms for RF Systems. IEEE Transactions on Wireless Communications, 2023, pp. 2845–2858.
[5] Silva, F. Integration of Multi-Frequency Radios with Shared Cryptographic Logic. IEEE Systems Journal, Vol. 17, 2024, pp. 2234–2248.
[6] Chen, X. Experimental Benchmarking of Secure Dual-Radio Modules. IEEE Transactions on Wireless Communications, Vol. 23, No. 4, 2024, pp. 1810–1824.
[7] Chen, L. Architectural Optimization in Multi-RF Secure Systems. IEEE Transactions on Vehicular Technology, Vol. 74, No. 2, 2024, pp. 332–345.

ANALYSIS OF METHODS FOR DETECTING BOT ACTIVITY ON THE INTERNET

Illia Azarov[2], Ivan Azarov[1]
[1] *State University of Information and Communication Technologies, Solomianska 7, 03110 Kyiv, Ukraine*
[2] *National Aviation University, Liubomyra Huzara Avenue 1, 03058 Kyiv, Ukraine*

Abstract
The paper presents a study on automated bot identification methods in social networks. An approach for bot detection based on ensemble learning has been developed. A detailed mathematical analysis of LSTM, BERT, Random Forest, and SVM algorithms was conducted, and their performance evaluation criteria (Accuracy, Recall, F1-score) are provided. Experimental results show that the proposed approach achieves high classification accuracy by combining text and metadata analysis.

Keywords
Information security, bot detection, machine learning, AI, NLP, ensemble methods, social networks.

Introduction

Relevance of the Research Topic.

The contemporary information landscape has evolved into an arena of hybrid warfare, where automated agents (bots) are deployed to destabilize society, disseminate disinformation, and manipulate public opinion. A particular threat is posed by next-generation intelligent bots that utilize Large Language Models (LLMs) to generate content, rendering their behavior nearly indistinguishable from that of humans. Traditional defensive methods are losing effectiveness, necessitating the development of adaptive AI-based systems. The aim of this work is to enhance information security by examining existing algorithms for bot activity detection.

The objective of the study is to analyze methods for identifying bot activity on the Internet and evaluate them based on a set of criteria to formulate an optimal solution for countering cyber threats through the application of an adaptive ensemble approach.

Object of research: The process of bot functioning within the internet environment, specifically in news comment sections.

Subject of research: Technologies and methods for bot detection based on behavioral and content analysis.

Scope of work: The study involves the systematization and comprehensive analysis of modern bot detection methods that combine machine learning, linguistic, and behavioral analysis. This is aimed at formulating an optimal solution to counter malicious activity and improve systems for protecting the information space from the harmful influence of bots.

Scientific Novelty: Unlike existing solutions that often rely on a monolithic architecture, the proposed microservice-based method utilizes dynamic result weighting (Weighted Soft Voting). In this approach, the contribution of each classifier depends on the type of input data (text or metadata), enabling the effective detection of hybrid attacks.

Description of research methods and algorithms.

To ensure maximum detection accuracy, four diverse algorithms were utilized and investigated in this study.

1. Recurrent Neural Network (LSTM + GloVe)

The LSTM (Long Short-Term Memory) architecture was selected for the deep analysis of word sequences in comments. Unlike classical RNNs, LSTM effectively solves the vanishing gradient problem, allowing the model to retain the context of long sentences in memory. The input text is vectorized using pre-trained GloVe embeddings, which enables the network to analyze semantic coherence and detect patterns of automated text generation.

2. Transformer Model (BERT)

The BERT (Bidirectional Encoder Representations from Transformers) model was employed for the most in-depth contextual analysis. Thanks to the Self-Attention mechanism, BERT analyzes each word within the context of the entire sentence simultaneously (bidirectionally), rather than sequentially. This

allows for the detection of hidden sarcasm, irony, and complex manipulative structures often used by advanced bots.

3. Random Forest

An ensemble classical machine learning algorithm based on constructing a multitude of decision trees. In the developed system, it is primarily responsible for processing tabular metadata (non-textual features). Parameters such as account age, follower/following ratio, publication frequency, and activity timestamps are analyzed.

4. Support Vector Machine (SVM)

SVM was used as a reliable linear classifier for working with high-dimensional vectors obtained via the TF-IDF method. The algorithm seeks an optimal hyperplane in a multidimensional space that separates the "bot" and "human" classes with the maximum margin. This method is particularly effective for short, concise texts and spam messages.

Table 1. Bot Classification Matrix: types, subtypes, function examples, characteristic platforms, automation level, and coordination level [1-2]

Bot Type	**Subtypes**	**Function Examples**	**Characteristic Platforms**	**Automation Level**	**Coordination Level**
Social Bots	Content-based; Behavior-based; cyborgs	Narrative amplification, commenting, reposting, formation of fake connections	Twitter/X, Telegram, Facebook, Instagram	From partial to full	From individual to coordinated networks
News Bots	Clickbait; propaganda; "junk news"	Mass dissemination of news content, clickbait, consistency of multimodal elements	News sites, social networks	Predominantly full	Network campaigns with coordinated reposts
Spam Bots	Form spam; phishing; email harvesting; fake followers	Spam distribution, email harvesting, metric inflation, carding	Web forms, social networks, forums	Full	Often part of a botnet
Troll Bots	State-sponsored; political	Propaganda, polarization, coordinated discussions	Social networks	Human-operated	High (campaigns)
Other (infrastructural)	Botnets; scrapers; crawlers; downloader bots; ticket bots	DDoS, data scraping, indexing, ticket sales manipulation	Web, API, ticketing	Full	Often large-scale networks

Comparative performance analysis:

Standard binary classification performance metrics were used to objectively evaluate the quality of the implemented models. The evaluation was based on a confusion matrix, taking into account True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN) outcomes.

This study conducted an in-depth analysis of four diverse machine learning and deep learning algorithms. The following criteria were used for an objective evaluation of their performance:

1. Accuracy:

Indicates the overall percentage of correct system predictions. It is calculated using the formula:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

While this is a fundamental metric, it may be insufficient when dealing with imbalanced classes.

2. Recall:

Reflects the model's ability to detect the «bot» class. In the context of information security, this is a critical parameter, as missing a bot is more dangerous than an erroneous block (false positive).

$$\mathrm{Re}\,call = \frac{TP}{TP + FN}$$

3. F1-score:

Represents the harmonic mean of Precision and Recall. It allows for the evaluation of the model's balance.

$$F1 = 2 \times \frac{\mathrm{Pr}ecision \times \mathrm{Re}call}{\mathrm{Pr}ecision + \mathrm{Re}call}$$

The results of the comparative analysis are presented in the table below. [2]

Table 2. Comparative analysis of machine learning methods performance

Method	**Accuracy**	**Precision**	**Recall**	**F1-Score**	**Training Time**
LSTM + GloVe	92.5%	89.3%	94.1%	91.6%	High
Random Forest + TF-IDF	89.8%	86.7%	91.2%	88.9%	Medium
SVM + RBF	88.4%	85.1%	90.5%	87.7%	Medium
BERT	94.2%	91.8%	95.3%	93.5%	High

BERT shows superior performance but necessitates substantial computational resources. LSTM+GloVe offers a favorable balance between accuracy and efficiency, whereas Random Forest proves optimal for rapid deployment with satisfactory accuracy. The ensemble approach maximized the F1-score, ensuring an optimal trade-off between threat detection and the minimization of false positives.

Conclusions:

1. The conducted analysis demonstrates that none of the considered methods, when used individually, constitutes a universal solution for the task of bot detection in social networks. There is a clear correlation: methods with high accuracy and context understanding (BERT, LSTM) require significant resources and have low processing speeds, while fast methods (Random Forest, SVM) lose accuracy when analyzing complex content.
   - BERT leads in quality (Accuracy 94.2%), but its real-time application for processing millions of comments is economically unfeasible due to high resource demands.
   - Random Forest processes profile metadata perfectly but is powerless against bots with "well-developed" accounts that post toxic comments.
   - SVM and LSTM occupy intermediate positions, possessing their own specific limitations.
2. Based on this, it is concluded that the most effective solution is the use of a combined method. Such an approach allows for mitigating the drawbacks of individual algorithms by integrating their advantages:
   - Using Random Forest at the first stage for rapid filtering based on metadata.
   - Deploying BERT or LSTM only for the analysis of suspicious texts that have passed the initial screening.
3. It is the ensemble architecture that ensures a synergistic effect, maximizing the overall system accuracy and F1-score while optimizing the load on computational resources. This is supported by the necessity to balance threat detection with the minimization of false positives under real-world operating conditions.

References

[1] Latah, M. (2020). Detection of malicious social bots: A survey and a refined taxonomy. *Expert Systems with Applications*, *151*, 113383.

[2] Ng, L. H. X., & Carley, K. M. (2024). Assembling a multi-platform ensemble social bot detector with applications to us 2020 elections. Social Network Analysis and Mining, 14(1), 45.

[3] Hays, C., Schutzman, Z., Raghavan, M., Walk, E., & Zimmer, P. (2023, April). Simplistic collection and labeling practices limit the utility of benchmark datasets for twitter bot detection. In Proceedings of the ACM web conference 2023 (pp. 3660-3669).

[4] Кіфорчук, К. О. (2019). Ідентифікація Twitter ботів засобами машинного навчання.

CYBERSECURITY RISK MODELING USING ARTIFICIAL INTELLIGENCE

Farah Abdulrazzaq Mahmood[1], Ahmed Bahaa al-Abbasy[2], Viktoriia Trofymchuk[3]
[1,2]AL-RAFIDAIN UNIVERSITY
[3] KYIV, UKRAINE

Abstract

The increasing sophistication of cyber threats requires adaptive and predictive cybersecurity risk models. Traditional approaches based on static rules and historical data are insufficient for anticipating emerging attacks. Artificial intelligence (AI) enables dynamic cybersecurity risk modeling through pattern recognition, anomaly detection, and predictive analytics. This study examines AI-based risk modeling for threat prediction and mitigation in complex networks and critical infrastructure, including the identification of anonymous users using active and passive digital fingerprinting techniques. The results indicate that effective risk assessment relies on verifying functionality, availability, and detecting spoofed or masked functions rather than collecting a single unique identifier. Challenges related to data quality, adversarial AI, and explainability are also addressed.

1. Introduction

Cybersecurity threats have evolved into highly targeted and adaptive campaigns, exposing the limits of static and reactive defense models. Risk modeling is essential for estimating the likelihood and impact of cyber incidents, but conventional approaches struggle to keep pace with rapidly changing attack vectors. The growth of digital technologies has also increased threats that exploit anonymity, making anonymous user identification important for protecting critical infrastructure by monitoring and restricting unauthorized actions. Artificial intelligence (AI) strengthens cybersecurity risk modeling through data-driven prediction, vulnerability prioritization, and support for proactive prevention and real-time mitigation.

2. Foundations of Cybersecurity Risk Modeling

Traditional cybersecurity risk models, such as the NIST Cybersecurity Framework and ISO/IEC 27005, define risk as a function of threat, vulnerability, and impact, relying on historical data, expert judgment, and static probabilities. However, these approaches lack adaptability to rapidly evolving attack techniques, including zero-day exploits, adversarial tactics, and dynamic infrastructures such as cloud and IoT environments. Similarly, traditional static methods of user identification are insufficient in modern threat landscapes where anonymity is actively exploited. Contemporary risk modeling increasingly relies on the analysis of variable combinations of browser attributes, operating system settings, and device characteristics to support the identification of anonymous users. Artificial intelligence enhances these foundations by incorporating real-time telemetry, behavioral analysis, and predictive modeling for more effective cybersecurity risk assessment in critical infrastructures.

3. Artificial Intelligence in Cybersecurity Risk Modeling

Artificial intelligence enhances cybersecurity risk modeling through machine learning, deep learning, and reinforcement learning techniques. Supervised and unsupervised ML methods support traffic classification and anomaly detection, while deep learning architectures improve feature extraction for complex threats such as malware and advanced persistent attacks. Reinforcement learning enables adaptive defense strategies by optimizing security controls in dynamic environments. Hybrid AI models combine multiple approaches to provide context-aware risk assessment, integrating technical vulnerabilities with broader impact considerations. Within this framework, active browser fingerprinting techniques use targeted client-side analysis of software, hardware, network, and behavioral attributes to support the identification of anonymous users as part of AI-driven cybersecurity risk modeling.

4. Applications of AI-Driven Risk Modeling

4.1 Threat Prediction

AI models analyze system logs, network traffic, and threat intelligence to predict potential cyberattacks and support early warning.

4.2 Intrusion Detection and Response

AI-based intrusion detection systems identify anomalies in real time and assist in adaptive mitigation.

4.3 Vulnerability Prioritization

AI supports risk-based prioritization of vulnerabilities by considering exploit likelihood and impact.

4.4 Cyber Risk Quantification

AI enables quantitative assessment of cyber risks by combining technical indicators with impact evaluation.

4.5 Passive Device Fingerprinting

Passive fingerprinting techniques analyze network and protocol characteristics to identify anonymization and automation tools without client-side interaction.

5. Challenges and Limitations

AI-based cybersecurity risk modeling faces several challenges, including limited availability of high-quality and diverse data, vulnerability of models to adversarial attacks, and insufficient explainability of complex algorithms. Scalability remains an issue when processing large volumes of real-time data, while effective human–AI collaboration is necessary to avoid overreliance on automated predictions.

6. Future Directions

Future research focuses on federated learning to enable collaborative defense while preserving data privacy, graph neural networks for modeling complex attack dependencies, and integration of AI-driven risk modeling with zero-trust architectures. Additionally, the combination of AI techniques with post-quantum cryptography is expected to improve resilience against emerging quantum-enabled cyber threats.

The following figure presents detection accuracy and risk mitigation efficiency for selected artificial intelligence approaches used in cybersecurity risk modeling.

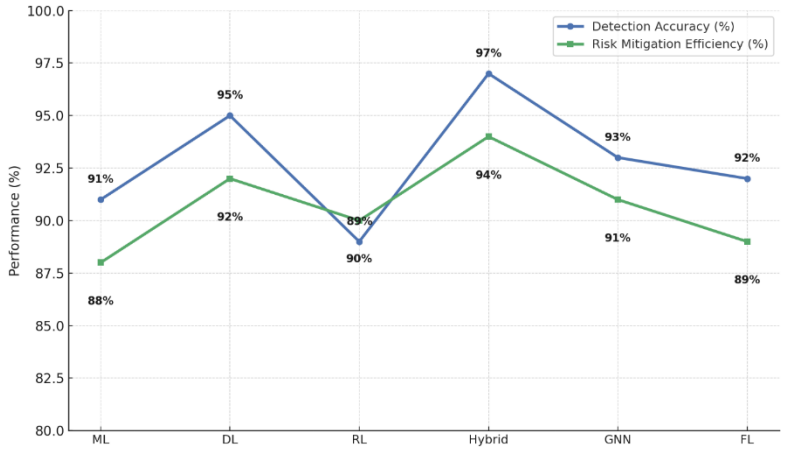

Figure 1. Comparative Analysis of AI-Based Cyber Risk Modeling Performance

7. Conclusion

AI-driven cybersecurity risk modeling enables a transition from reactive to proactive defense by improving threat prediction, vulnerability prioritization, and mitigation. The combined use of AI techniques and active and passive user fingerprinting supports effective identification of anonymous users and enhances the resilience of critical infrastructure despite existing challenges related to explainability and adversarial threats.

References

[1] NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity.

[2] Sommer, R., & Paxson, V. (2010). "Outside the Closed World: On Using ML for Network Intrusion Detection." IEEE S&P Symposium.

[3] Chandola, V., Banerjee, A., & Kumar, V. (2009). "Anomaly Detection: A Survey." ACM Computing Surveys, 41(3), 1–58.

[4] Kim, J., Kim, H., & Kim, Y. (2020). "Deep Learning in Intrusion Detection." IEEE Access, 8, 8395–8405.

[5] Taddeo, M., & Floridi, L. (2018). "How AI Can Be a Force for Good in Cybersecurity." Science & Engineering Ethics, 24(3), 851–869.

[6] Liu, Y., et al. (2018). "Predicting Cyber Attacks with Threat Intelligence." IEEE Transactions on Information Forensics and Security, 13(11), 2856–2871.

[7] Almukaynizi, M., et al. (2020). "AI-Driven Vulnerability Prioritization." Computers & Security, 94, 101832.

METHODOLOGICAL FRAMEWORK OF AI-BASED INTRUSION DETECTION ANALYSIS

Serhii Bulba[1], Oleksandr Symonenko[2]
[1] *State University of Trade and Economics, Kioto 19, Kyiv, 02156, Ukraine*
[2]*Kruty Heroes Military Institute of Telecommunications and Information Technologies, Ukraine*

Abstract
The proposed framework is grounded in the transition from static intrusion detection mechanisms to adaptive, learning-driven models capable of real-time analysis. It examines supervised, unsupervised, and deep learning paradigms, including artificial neural networks, convolutional and recurrent neural networks, and reinforcement learning, as core methodological components. The study also addresses theoretical aspects such as pattern recognition, anomaly detection, scalability, and adaptability, along with considerations of explainable and federated learning. A practical evaluation is conducted using a labeled dataset of approximately 10,000 network traffic records with 28 descriptive features to validate the framework. Experimental results demonstrate that supervised ensemble models, particularly Gradient Boosting and Random Forest, achieve high accuracy and robustness, confirming the effectiveness of the proposed methodological framework for AI-based intrusion detection analysis.

Keywords
Supervised, unsupervised, and deep learning; machine learning (ML); Logistic Regression; Random Forest; SVM (RBF); Decision Tree (CART); KNN (K=5); Gradient Boosting; network traffic

Introduction

AI-based scanning for intrusion detection has become a critical component of modern cybersecurity systems. By leveraging machine learning techniques, these systems continuously scan network traffic and system activity to detect abnormal and malicious behavior in real time. Supervised learning models trained on real-world datasets enable accurate identification of known intrusion patterns and attack signatures. Artificial neural networks improve detection capabilities by modeling complex relationships within large volumes of traffic data. Deep learning approaches, such as convolutional and recurrent neural networks, further enhance real-time scanning by capturing both spatial and temporal characteristics of intrusions as they occur. Overall, AI-based intrusion detection scanning provides a proactive, adaptive, and resilient framework for identifying threats and strengthening system security.

Theoretical foundations of AI-based intrusion detection analysis

The theoretical foundations of AI-based intrusion detection analysis are grounded in the transition from static security mechanisms to adaptive, learning-driven models. Machine learning theory underpins modern intrusion detection systems by enabling pattern recognition, anomaly detection, and continuous model improvement through supervised and unsupervised learning. Deep learning architectures, such as convolutional, recurrent, and long short-term memory networks, provide the theoretical basis for modeling spatial and temporal dependencies in complex network traffic. Reinforcement learning further extends this foundation by introducing adaptive decision-making, allowing intrusion detection systems to adjust their responses to evolving threat environments dynamically. Additionally, the integration of explainable AI and federated learning addresses theoretical challenges related to transparency, scalability, and privacy, reinforcing the robustness of AI-based intrusion detection frameworks.

ML techniques for intrusion detection: practical experiment and results

AI-based intrusion detection analysis is built on supervised, unsupervised, and deep learning paradigms. Among these, supervised learning is the most widely used due to the availability of labeled network traffic data. Supervised classification models enable intrusion detection systems to reliably differentiate between normal and malicious network behavior. Logistic regression is commonly applied as a probabilistic method for classifying network observations into benign or intrusive categories.

The analysis is based on a dataset of approximately 10,000 network traffic records designed to reflect realistic operating environments. These records include explicit labels that indicate intrusion attempts, supporting effective model training and evaluation. A total of 28 features were used, capturing traffic intensity metrics, behavioral indicators of anomalous activity, and contextual metadata.

Performance evaluation of various machine learning models demonstrates the effectiveness of AI-based intrusion detection techniques. Gradient Boosting and Random Forest achieved the highest

accuracy, with rates of 95.2% and 94.1%, respectively. These models also showed strong precision, recall, F1-score, and AUC values, confirming their robustness and reliability in intrusion detection tasks.

Conclusions

AI-based intrusion detection analysis represents a significant advancement in modern cybersecurity by enabling proactive, adaptive, and data-driven threat detection. Theoretical foundations rooted in machine learning, deep learning, and reinforcement learning support the transition from static defense mechanisms to intelligent systems capable of continuous learning and real-time response. Practical experimentation confirms that supervised learning models, particularly ensemble methods such as Gradient Boosting and Random Forest, achieve high accuracy and reliability when applied to labeled network traffic data. The effective use of diverse traffic, behavioral, and contextual features further enhances detection performance. Overall, the integration of robust theoretical models with experimentally validated machine learning techniques demonstrates the effectiveness and scalability of AI-based intrusion detection systems in addressing evolving cyber threats.

References

[1] Gutierrez Garcia J. L., Sánchez DelaCruz E., Pozos Parra M. d. P. A Review of Intrusion Detection Systems Using Machine Learning: Attacks, Algorithms and Challenges. Advances in Information and Communication, FICC 2023 (Vol 2), pp. 59–78. URL: https://www.researchgate.net/publication/368921304_A_Review_of_Intrusion_Detection_Systems_Using_Machine_Learning_Attacks_Algorithms_and_Challenges

[2] Khanza A., Yulian F.D., Khairunnisa N., Yusuf N.A., Nuche A. Evaluating the effectiveness of machine learning in cyber threat detection. Journal of Computer Science and Technology Application, 8(2), (2024) 45-59. URL: https://journal.corisinta.org/corisinta/article/view/47

[3] Martínez Medina J., Hernández Torres J. A., Vega González A. Machine learning based network intrusion detection for big and heterogeneous data environments. Journal of Big Data, 11:45 (2024). URL: https://journalofbigdata.springeropen.com/articles/10.1186/s40537-024-00886

[4] Samed A., Seref S. Explainable artificial intelligence models in intrusion detection systems. Engineering Applications of Artificial Intelligence, (2025). 110-145. URL: https://www.sciencedirect.com/science/article/abs/pii/S0952197625001459

[5] Xu Z., Wu Y., Wang S., Gao J., Qiu T., Wang Z., Wan H., Zhao X. Deep Learning based Intrusion Detection Systems: A Survey. ArXiv preprint, (2025). URL: https://arxiv.org/abs/2504.07839

CHALLENGES AND OPPOTUNITIES FOR SECURE COMPUTING IN CLOUD ENVIRONMENTS

Ashwaq Amorad Muhee[1], Teba Mohammed Qasim[2], Genadiy Zhyrov[3]
[1,2]*AL-RAFIDAIN UNIVERSITY, Iraq*
[3] *TARAS SHEVCHENKO NATIONAL UNIVERSITY OF KYIV, Ukraine*

Abstract

Quantum computing poses an unprecedented threat to modern cryptography. Algorithms such as RSA, ECC, and Diffie–Hellman—which secure the vast majority of cloud communications—are vulnerable to Shor's algorithm, capable of breaking public-key cryptosystems in polynomial time. The emergence of post-quantum cryptography (PQC) offers a promising avenue to safeguard cloud environments against quantum-capable adversaries. This article explores the challenges and opportunities of deploying PQC in cloud infrastructures. The article concludes that PQC adoption in cloud environments is both a necessity and an opportunity to redefine the future of secure computing.

Introduction

Cloud computing underpins global digital infrastructures, enabling distributed storage, computation, and services at scale. Security in these environments relies heavily on asymmetric cryptography for authentication, key exchange, and digital signatures. However, the rapid progress of quantum computing threatens to render current cryptographic schemes obsolete. Post-quantum cryptography (PQC) aims to provide cryptographic primitives resilient to quantum attacks while maintaining efficiency and interoperability in classical computing environments.

Foundations of Post-Quantum Cryptography.

Quantum Threats to Classical Cryptography: Shor's Algorithm (1994) enables efficient factorization of large integers and computation of discrete logarithms, breaking RSA and ECC [1]; Grover's Algorithm weakens symmetric cryptography, requiring doubled key lengths for AES and SHA-based systems [2].

PQC Families: The main candidate families for PQC include: Lattice-based cryptography (e.g., Kyber, Dilithium) – strong security, scalable, chosen by NIST for standardization [3]; Code-based cryptography (e.g., McEliece) – proven long-term security but large key size; Multivariate cryptography – fast signature schemes but less mature; Hash-based cryptography (e.g., XMSS) – quantum-resistant but with stateful management; Isogeny-based cryptography – compact key sizes but under cryptanalytic scrutiny [4].

Cloud Environments and Cryptographic Vulnerabilities:

Cloud environments amplify cryptographic challenges due to: Multi-tenancy: shared infrastructures increase exposure to breaches; Dynamic workloads: frequent key generation, distribution, and revocation; Long-term data storage: "harvest now, decrypt later" attacks allow adversaries to store encrypted data until quantum capabilities emerge [5]; APIs and orchestration layers: vulnerable points for man-in-the-middle (MITM) and side-channel attacks.

Challenges of PQC Deployment in Cloud Environments:

PQC algorithm require larger key sizes and more computational resources. For instance, Kyber-1024 has key sizes exceeding 1KB, compared to ~256-bit ECC [6]. Cloud providers must maintain interoperability between PQC and legacy cryptography during the transition phase. Hybrid protocols combining classical and post-quantum algorithms are emerging but add complexity [5]. The NIST PQC standardization project (round 3 results announced in 2022) selected Kyber (encryption) and Dilithium (signatures) as primary standards [8]. However, global adoption requires alignment with ISO, IETF, and national policies. Side-channel attacks on PQC implementations remain a concern. Ensuring constant-time execution and secure key management in cloud hardware (e.g., HSMs, TPMs) is critical .

Opportunities for Secure Computing:

Adopting PQC ensures long-term confidentiality for sensitive workloads such as healthcare, finance, and government operations hosted in the cloud. PQC can enhance zero-trust architectures by providing quantum-safe identity verification, authentication, and micro-segmentation in distributed cloud systems. Machine learning can optimize PQC key distribution and anomaly detection, improving resilience against both classical and quantum adversaries. PQC strengthens confidential computing and federated AI training in the cloud, ensuring security in collaborative environments.

Future Directions

Hardware Acceleration: Development of PQC-ready chips (Intel, IBM, Google) for efficiency.

Cloud Provider Adoption: Major providers (AWS, Microsoft Azure, Google Cloud) are experimenting with PQC in TLS handshakes.

Quantum-Safe Standards: Broader integration of PQC into TLS 1.3, VPNs, and blockchain systems.

Conclusions

Post-Quantum Cryptography represents both a challenge and an opportunity for cloud security. While PQC introduces performance, migration, and implementation complexities, it is indispensable in ensuring quantum-resilient infrastructures. For cloud environments—where scalability, interoperability, and long-term data protection are critical—the transition to PQC must be accelerated. By combining PQC with zero-trust frameworks, AI-driven key management, and hardware optimization, the future of secure computing in the cloud can remain resilient against quantum-capable adversaries.

References

[1] Shor, P. W. (1994). "Algorithms for Quantum Computation: Discrete Logarithms and Factoring." Proceedings of FOCS.

[2] Grover, L. (1996). "A Fast Quantum Mechanical Algorithm for Database Search." STOC Proceedings.

[3] NIST. (2022). Post-Quantum Cryptography Standardization Project, Round 3 Results.

[4] Biasse, J. F., & Song, F. (2016). "Efficient Quantum Algorithms for Computing Class Groups and Solving the Principal Ideal Problem in Arbitrary Degree Number Fields." Proceedings of SODA.

[5] Mosca, M. (2018). "Cybersecurity in an Era with Quantum Computers." Philosophical Transactions of the Royal Society A, 376(2133).

IMPROVING ADAPTIVE PROTECTION IN COMPUTER NETWORKS BASED ON MACHINE LEARNING

Zaihab Shakir Amory[1*], Saba Omar Ghanem[2], Hennadii Mohylnyi[3]
[1,2] AL-RAFIDAIN UNIVERSITY, Iraq
[3*] *Taras Shevchenko National University, 1 Gogol Square, the City of Starobilsk, Luhansk Region, Ukraine*

Abstract

Intrusion Detection Systems (IDS) play an important role in ensuring computer network security. Traditional signature-based detection methods show limited effectiveness against zero-day attacks and sophisticated threats. Machine learning enables adaptive, data-driven intrusion detection by identifying anomalous patterns in network traffic. This paper examines ML-based IDS architectures, including supervised, unsupervised, and deep learning approaches, and discusses key challenges related to scalability, feature selection, and robustness. Emerging trends such as explainable artificial intelligence and integration with zero-trust architectures are also considered.

Introduction

The increasing complexity and diversity of cyberattacks necessitate advanced intrusion detection mechanisms. Traditional IDS based on static rules and signatures are insufficient against modern threats such as polymorphic malware and zero-day attacks. Machine learning–based IDS provide adaptive and scalable detection by learning patterns of normal and malicious behavior from data.

This research focuses on analyzing how machine learning contributes to improved intrusion detection by evaluating IDS architectures, learning paradigms, and contemporary technological challenges.

Evolution of Intrusion Detection

2.1 From Signature-Based to Anomaly-Based

Early IDS (e.g., Snort, Bro/Zeek) relied on signature-based detection of known attacks, which is ineffective against zero-day threats. ML-based IDS adopt anomaly detection to identify deviations from normal network behavior, providing improved adaptability [2].

2.2 Data-Driven Security

The increasing availability of large-scale security data enables ML models to detect subtle attack patterns. Distributed computing technologies support the scalability of ML-based IDS in enterprise and cloud environments [3].

Machine Learning Approaches in IDS

3.1 Supervised Learning

Supervised learning employs algorithms such as SVMs, Random Forests, and neural networks to classify traffic based on labeled datasets (e.g., KDD'99, NSL-KDD, CICIDS2017)[4]. Despite their high accuracy, the effectiveness of these methods may decrease in real-world environments with highly variable network activity.

3.2 Unsupervised and Semi-Supervised Learning

For scenarios with limited labeled data, clustering (k-means, DBSCAN) and autoencoders enable anomaly detection by identifying outliers in traffic [5]. Semi-supervised models leverage partially labeled data to improve detection performance [6].

3.3 Deep Learning

Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Transformers enable advanced feature extraction from raw traffic, improving detection of stealthy attacks [7]. However, they require substantial computational resources and raise interpretability concerns.

Adaptive Defense and Real-Time Intrusion Detection

4.1 Dynamic Threat Landscapes

Adversaries employ techniques such as polymorphism, obfuscation, and adversarial ML attacks to evade detection. ML-driven IDS must adapt in real-time, incorporating continuous learning pipelines [8].

4.2 Integration with Security Orchestration

By embedding ML-driven IDS into Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) systems, organizations achieve coordinated defense strategies [9].

4.3 Explainable AI (XAI)

Interpretability is crucial in IDS, as false positives may overwhelm analysts. XAI techniques (e.g., SHAP, LIME) make ML-driven IDS more transparent, increasing trust and usability [10].

Challenges in ML-Driven IDS

1. Data Quality and Imbalance – Malicious samples are rare relative to benign traffic, leading to skewed datasets [11].
2. Scalability – Real-time IDS must process gigabits of traffic per second; computational costs of deep learning can be prohibitive [12].
3. Adversarial Evasion – Attackers can craft traffic to mislead ML models, raising the need for adversarially robust training [10].
4. Deployment Complexity – Integrating ML into legacy infrastructures requires overcoming interoperability and cost barriers [9].

Future Directions

6.1 Federated Learning

Federated IDS models enable collaborative training across organizations without sharing raw data, enhancing privacy while improving detection [11].

6.2 Hybrid Approaches

Combining signature-based and ML-based detection improves robustness, capturing both known and novel threats [8].

6.3 Quantum-Resilient IDS

Future IDS must anticipate quantum-enabled cyberattacks, requiring post-quantum cryptography and quantum-enhanced detection algorithms [10].

6.4 Integration with Zero-Trust Architectures

Embedding IDS within Zero-Trust security frameworks enhances adaptive verification, ensuring that threats are detected even within trusted environments [11].

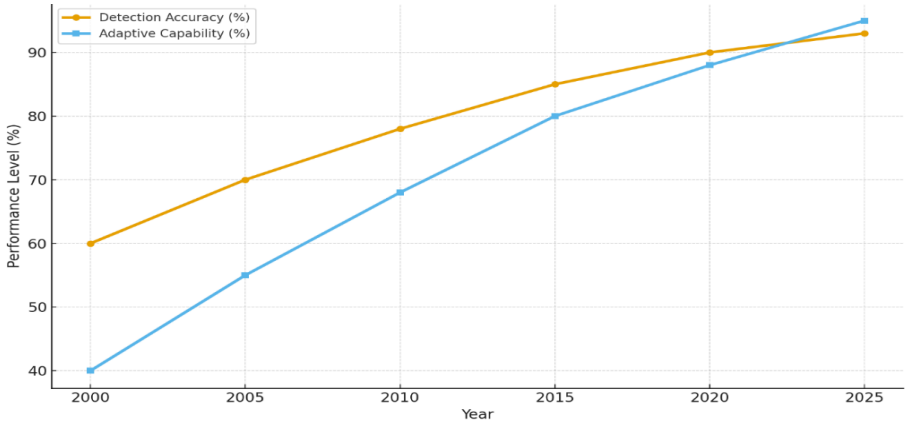

Figure 1. Evolution of Detection Accuracy and Adaptability Across ML-IDS Paradigms

Conclusion

ML-driven IDS offer adaptive, anomaly-based, and real-time protection in dynamic networks. While challenges remain in scalability, interpretability, and robustness, advances such as federated learning, XAI, and hybrid models enhance resilience. ML-based intrusion detection is expected to remain essential for adaptive network defense against evolving cyber threats.

References

[1] Denning, D. (1987). "An Intrusion-Detection Model." IEEE Transactions on Software Engineering, SE-13(2), 222–232.

[2] Axelsson, S. (2000). "Intrusion Detection Systems: A Survey and Taxonomy." ACM Computing Surveys, 31(3), 265–318.

[3] Sommer, R., & Paxson, V. (2010). "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection." IEEE S&P Symposium.

[4] Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. (2009). "A Detailed Analysis of the KDD CUP 99 Data Set." IEEE Symposium on Computational Intelligence for Security and Defense Applications.

ENSURING TRUST IN DECENTRELIZED BLOCKCHAIN-BASED INFRASRTUCTURES FOR THE INTERNET OF THINGS

Diana Qasim Sabih[1], Areez Osama Fahad[2], Mykhailo Prygara[3]
[1,2]*AL-RAFIDAIN UNIVERSITY, Irag*
[3]*Uzhhorod National University, Narodna Square, Transcarpathian region, Uzhhorod, 88000, Ukraine*

Abstract

The Internet of Things (IoT) has transformed global connectivity, enabling billions of devices to interact across healthcare, manufacturing, and smart city infrastructures. However, IoT systems face significant security challenges due to their distributed and heterogeneous nature. Blockchain technology, with its decentralized consensus, immutable ledgers, and cryptographic guarantees, offers a promising paradigm for establishing trust in IoT ecosystems. This article explores blockchain-based security models for IoT, examining their role in enhancing authentication, data integrity, and resilience against cyberattacks. The article concludes that blockchain can significantly improve IoT security, but achieving large-scale deployment requires overcoming performance and interoperability barriers.

Introduction

The Internet of Things (IoT) is expected to exceed 25 billion connected devices by 2030, generating unprecedented volumes of data and supporting mission-critical applications [1]. However, IoT systems are inherently vulnerable to data breaches, botnet attacks and denial-of-service attacks due to their distributed architecture and limited device resources [2].

Blockchain technology offers a decentralized alternative. By leveraging distributed ledgers, consensus algorithms, and smart contracts, blockchain enables trust without central authorities and verifiable device interactions

Blockchain as a Trust Layer for IoT.

Blockchain eliminates single points of failure by distributing trust across a peer-to-peer network. Consensus protocols (e.g., Proof-of-Work, Proof-of-Stake, Byzantine Fault Tolerance) ensure integrity of IoT transactions [3]. Blockchain uses hashing, digital signatures, and Merkle trees to secure IoT data against tampering. Immutable ledgers record all device interactions, enabling traceability and accountability [4]. Smart contracts automate IoT operations such as device onboarding and data sharing, reducing reliance on centralized authorities [5].

Security Applications of Blockchain in IoT:

Blockchain provides decentralized identity (DID) frameworks that eliminate reliance on third-party authentication servers, mitigating credential theft and spoofing [6]. IoT data stored on or referenced by blockchain is immutable, ensuring integrity. Encrypted off-chain storage combined with on-chain hashes preserves confidentiality while guaranteeing tamper resistance [7]. Blockchain-enabled attribute-based access control models allow fine-grained permissions across IoT devices, enforced by smart contracts [8]. Blockchain ensures trustworthy device firmware distribution by maintaining verifiable update logs, preventing supply chain attack [9].

Challenges in Blockchain-Based IoT Security:

IoT generates massive transaction volumes. Public blockchains suffer from low throughput and high latency, making them unsuitable for real-time IoT applications [10]. Consensus mechanisms like Proof-of-Work are resource-intensive, conflicting with energy-constrained IoT devices. Blockchain growth increases storage overhead. Lightweight IoT nodes cannot store full ledgers, requiring scalable alternatives such as light clients or sharding. Diverse IoT ecosystems require interoperability across heterogeneous blockchains and legacy systems.

Emerging Opportunities:

Protocols like Proof-of-Authority, Delegated Proof-of-Stake, and Practical Byzantine Fault Tolerance (PBFT) are promising for IoT due to reduced computation and energy demands. Combining blockchain with edge computing reduces latency and enables localized trust management, vital for smart cities and autonomous systems.

Case Studies

Energy Sector: Blockchain-based IoT used for smart grid security enables secure peer-to-peer energy trading. Healthcare: IoT medical devices use blockchain for secure patient data exchange while ensuring

regulatory compliance (HIPAA/GDPR). Supply Chain: IoT sensors combined with blockchain ensure traceability and integrity of goods from origin to delivery.

Conclusions

Blockchain-based security models provide a transformative pathway for securing IoT infrastructures. By enabling decentralized trust and autonomous access control, blockchain addresses many of IoT's inherent vulnerabilities. However, widespread adoption requires solving challenges of scalability, energy efficiency, and interoperability. The integration of lightweight consensus protocols, edge computing, and AI-driven trust management points to a resilient future where blockchain secures the rapidly expanding IoT landscape.

References

Atzori, L., Iera, A., & Morabito, G. (2010). "The Internet of Things: A Survey." Computer Networks, 54(15), 2787–2805.

Antonakakis, M., et al. (2017). "Understanding the Mirai Botnet." USENIX Security Symposium.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

Crosby, M., et al. (2016). "Blockchain Technology: Beyond Bitcoin." Applied Innovation Review, 2, 6–10.

Christidis, K., & Devetsikiotis, M. (2016). "Blockchains and Smart Contracts for the Internet of Things." IEEE Access, 4, 2292–2303.

Dunphy, P., & Petitcolas, F. A. P. (2018). "Decentralized Identity." IEEE Security & Privacy, 16(4), 46–53.

Zhang, Y., & Wen, J. (2017). "An IoT Electric Business Model Based on the Blockchain Technology." ICCBDA.

Ouaddah, A., Abou Elkalam, A., & Ait Ouahman, A. (2017). "FairAccess: A Blockchain-Based Access Control Framework for IoT." IEEE Transactions on Internet of Things, 4(6), 2129–2141.

ZERO TRUST ARCHITECTURES: RESILIENT CYBERSECURITY FRAMEWORKS IN DISTRIBUTED SYSTEMS

Sinan Alaa Nadhim[1*], Sadeq Jaafar Jaber[2], Yurii Khlaponin[3]
[1,2] *AL-RAFIDAIN UNIVERSITY, Iraq*
[3] *STATE UNIVERSITY OF TRADE AND ECONOMICS, Ukraine*

Abstract

The rapid proliferation of distributed systems—ranging from cloud computing and Internet of Things (IoT) infrastructures to edge and multi-cloud environments—has challenged traditional perimeter-based security models. Zero-Trust Architecture (ZTA) has emerged as a paradigm shift, premised on the principle of "never trust, always verify." This article explores the theoretical foundations and practical implementations of Zero-Trust in distributed systems, highlighting its potential for building resilient cybersecurity frameworks. It examines the evolution from perimeter defense to zero-trust models, evaluates core components such as continuous authentication, micro-segmentation, and policy-based access control, and analyzes implementation challenges, including scalability, interoperability, and privacy concerns. By considering emerging applications in AI-driven security orchestration and quantum-resistant cryptography, the article argues that Zero-Trust Architectures represent a critical pathway towards securing distributed ecosystems in an era of escalating cyber threats.

Introduction

Distributed systems underpin modern computing, supporting critical infrastructures and global digital services. Their complexity and heterogeneity increase vulnerabilities, while traditional perimeter-based security assumes inherent trust within internal networks.

The Zero-Trust paradigm rejects this assumption, requiring continuous verification of users, devices, and processes based on contextual factors such as identity, device health, location, and behavior. This approach aligns security practices with dynamic, cloud-native, and hybrid environments.

Foundations of Zero-Trust Architecture

2.1 Principles of Zero-Trust

Zero-Trust is guided by three core principles:

1. Verify explicitly – Continuous authentication and authorization using multiple attributes.
2. Use least-privilege access – Granular access control via micro-segmentation and just-in-time access.
3. Assume breach – Design networks as though adversaries already have access, emphasizing detection, containment, and resilience [1].

2.2 Evolution from Perimeter Defense

Traditional perimeter security treated networks as trusted internal "castles" protected by firewalls. The rise of distributed and cloud systems revealed its limitations, while breaches at companies like Equifax and SolarWinds highlighted the risks of implicit trust and lateral movement, accelerating adoption of Zero-Trust strategies [2].

Zero-Trust in Distributed Systems

3.1 Principles of Zero-Trust

In Zero-Trust Architecture, identity serves as the "new perimeter." Strong authentication methods, including MFA, biometrics, and federated identity management, are central. Distributed systems require secure propagation of identity information across cloud and on-premises environments [3].

3.2 Micro-Segmentation and Policy Enforcement

Micro-segmentation divides networks into smaller trust zones, limiting the impact of breaches. Policy-based access control enforces least-privilege communication between nodes, services, or microservices [4].

3.3 Continuous Monitoring and Analytics

Machine learning strengthens Zero-Trust by analyzing user behavior anomalies, device integrity, and network traffic in real-time. This adaptive approach is essential in dynamic multi-cloud and IoT environments, where static policies are insufficient [5].

Implementation Challenges

4.1 Scalability

Implementing Zero-Trust in large-scale distributed systems requires managing billions of access requests daily, demanding high-performance authentication systems [6].

4.2 Interoperability

Distributed systems often span multiple cloud providers, legacy infrastructures, and IoT ecosystems. Standardization challenges hinder seamless Zero-Trust enforcement [7].

4.3 Privacy and Compliance

Continuous monitoring may conflict with data privacy regulations (e.g., GDPR, HIPAA). Balancing security with data minimization and transparency is an ongoing philosophical and legal challenge [8].

Emerging Trends and Future Directions

5.1 AI-Driven Security Orchestration

Artificial intelligence enables predictive risk assessment and automated response, making Zero-Trust adaptive and self-optimizing [9, 13].

5.2 Quantum-Resistant Cryptography

As quantum computing advances, Zero-Trust must integrate post-quantum cryptographic protocols to maintain secure authentication and data exchange [10].

5.3 Edge and IoT Security

Zero-Trust is increasingly applied at the edge, where IoT devices introduce vulnerabilities. Lightweight authentication and distributed ledger technologies (e.g., blockchain-based trust verification) offer promising directions [11].

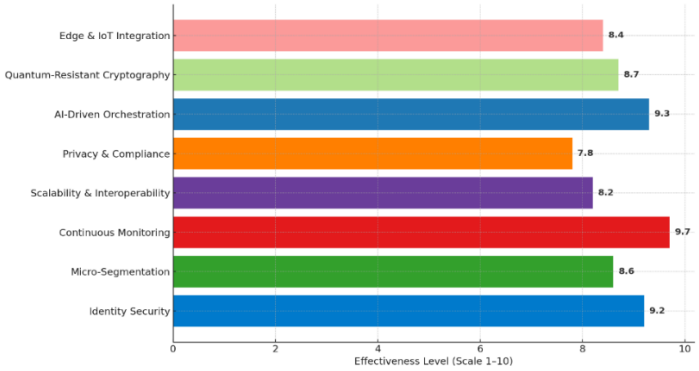

Figure 1. Comparative Effectiveness of Zero-Trust Components in Distributed Cybersecurity

Conclusion

Zero-Trust Architecture represents a paradigm shift in securing distributed systems. By rejecting implicit trust and enforcing continuous verification, ZTA provides resilience against insider threats, credential abuse, and advanced persistent threats. Despite challenges in scalability, interoperability, and privacy, Zero-Trust remains a robust framework for resilient cybersecurity in distributed environments. As AI, quantum computing, and edge systems evolve, integrating Zero-Trust principles will be essential for the security of global digital infrastructures.

References

[1] Kindervag, J. (2010). No More Chewy Centers: The Zero Trust Model of Information Security. Forrester Research.

[2] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture*. NIST SP 800-207.

[3] Alshammari, S., & Simpson, A. (2022). "Identity-Centric Security in Distributed Systems." *IEEE Access*, 10, 12631–12644.

[4] Scott-Hayward, S., O'Callaghan, G., & Sezer, S. (2016). "SDN Security: A Survey." *IEEE Communications Surveys & Tutorials*, 18(1), 623–654.

[5] Mavroeidis, V., & Bromander, S. (2017). "Cybersecurity Threat Intelligence Sharing." *Computers & Security*, 67, 70–90.

[6] Kumar, P., et al. (2021). "Scalability of Zero-Trust Models in Cloud Environments." *Future Generation Computer Systems*, 115, 233–245.

[7] Zhao, Y., & Hardjono, T. (2020). "Interoperability in Zero-Trust Architectures." *ACM Computing Surveys*, 53(4), 1–33.

[8] Taddeo, M. (2019). "Data Ethics and Cybersecurity." *Philosophy & Technology*, 32(2), 213–225.

[9] Chen, T., & Bridges, R. (2017). "Automated Behavior-Based Detection." *Journal of Information Security and Applications*, 42, 53–64.

EMBEDDED BACKDOORS AND THE EROSION OF DIGITAL TRUST: A KLEPTOHYGIENE FRAMEWORK FOR STATE AND INTERNATIONAL SYSTEM

Mykhailo Shelest[1], Yuliia Tkach[2], Oleksandr Polevod[3] and Vladyslav Somov[4]
[1,2,3,4] *Chernihiv Polytechnic National University, Shevchenka 95, 14030 Chernihiv, Ukraine*

Abstract

Kleptography was historically framed as the covert insertion of trapdoors into cryptographic primitives or black-box devices. In contemporary socio-technical ecosystems, however, embedded backdoors increasingly manifest as a systemic trust failure that spans standards, supply chains, build pipelines, firmware, and organizational governance. This paper proposes a trust-oriented perspective that connects classical kleptographic mechanisms (SETUP) with modern supply-chain intrusions and standardization risks, and introduces a practical concept of kleptohygiene - a set of preventive controls and verification routines that reduce the probability of undetected deliberate weaknesses in state and international information systems. We summarize lessons from widely discussed incidents (Crypto AG, Dual_EC_DRBG-related controversies, Juniper ScreenOS, and the XZ Utils backdoor) and derive actionable recommendations for procurement, independent validation, software transparency (SBOM), and reproducible verification.

Keywords

kleptography, embedded backdoors, digital trust, supply-chain security, SBOM, reproducible builds, critical infrastructure

Introduction

The security of modern digital infrastructures - especially those used by public administrations, defense sectors, and international organizations - relies on a fragile assumption: that cryptographic implementations and security products behave as specified. Yet the last decade has demonstrated that deliberate weaknesses can be introduced not only into algorithms, but also into devices, firmware, update channels, open-source dependencies, and even governance processes that define what is considered 'trusted'. This work treats embedded backdoors as a threat to digital trust rather than a purely technical anomaly.

We use the term kleptography in an expanded sense: intentional embedding of covert access mechanisms or undetectable weaknesses into any component of a digital system (including, but not limited to, cryptography). From this viewpoint, a backdoor is not simply an exploit; it is a long-term instrument of asymmetric influence, enabling selective surveillance, covert disruption, or strategic dependence.

The paper makes three contributions:

(i) it bridges classical kleptographic theory (SETUP) with current supply-chain realities;

(ii) it proposes a structured trust-surface model for analyzing where backdoors can be inserted and how they evade detection; and

(iii) it introduces a kleptohygiene framework, emphasizing preventive verification and institutional controls for high-trust systems.

From SETUP to Supply-Chain Backdoors

Early kleptographic research formalized the idea of Secretly Embedded Trapdoors with Universal Protection (SETUP): a mechanism hidden inside a cryptographic black box that leaks secret information to an attacker while remaining indistinguishable to the user. The classical focus was on algorithmic or protocol-level modifications that preserve outward correctness yet enable stealth exfiltration.

In present-day ecosystems, the same stealth principle appears at larger scales. Attackers increasingly target upstream dependencies, build scripts, signing keys, continuous integration systems, and distribution channels. The core shift is that 'the backdoor' may be a sequence of small, individually plausible changes that together create covert control. Consequently, purely algorithmic review is insufficient; trust must be assessed across the full lifecycle of software and hardware.

Trust Surfaces and Kleptographic Attack Paths

We define a trust surface as the set of components whose compromise yields a persistent, hard-to-detect advantage. For state and international systems, trust surfaces include:

(a) standards and reference implementations;

(b) cryptographic libraries and key management stacks;

(c) firmware, hardware security modules, and secure elements;
(d) update infrastructure and code-signing;
(e) supply-chain dependencies and build pipelines; and
(f) institutional processes (procurement, audits, compliance).

Kleptographic attack paths typically combine
(1) insertion (where the weakness is introduced),
(2) camouflage (how the insertion is made to look legitimate),
(3) activation (conditions under which the backdoor becomes exploitable), and
(4) persistence (how access survives updates and operational changes).

A key risk factor is asymmetric verifiability: the attacker may hold secret parameters or knowledge (e.g., manipulated constants, hidden keys, or off-path triggers) that are practically impossible for defenders to infer from black-box testing.

Kleptohygiene as Preventive Control

Kleptohygiene is proposed as a preventive discipline: a set of technical and organizational practices aimed at reducing the probability that deliberate weaknesses remain undetected in high-trust systems. Unlike incident response (reactive) or vulnerability management (often oriented to accidental flaws), kleptohygiene explicitly assumes intentional adversarial design.

At the technical layer, kleptohygiene includes: reproducible builds and independent rebuild verification; strict dependency policies; continuous integrity checks of build toolchains; signature verification with transparent key governance; diversified implementations (N-version programming) for critical primitives; and structured telemetry for anomaly detection. At the organizational layer, it includes: separation of duties in procurement and validation; mandatory third-party audits for critical components; and traceable attestation of secure development practices.

A pragmatic enabler is the Software Bill of Materials (SBOM), which provides a formal record of software components and relationships, allowing faster identification of inherited risks and unexpected dependencies. SBOMs are not sufficient by themselves, but they make verification programs measurable and enforceable.

Illustrative Cases and Lessons Learned

Crypto AG illustrates a long-term hardware and governance-level trust compromise: cryptographic equipment sold to many countries was reportedly influenced and used for intelligence advantages over decades. The case highlights how trust can be undermined through supply-chain control and institutional secrecy, even when devices appear operationally sound.

Dual_EC_DRBG controversies demonstrate how subtle parameter choices in standards can create an asymmetric advantage. The subsequent removal of Dual_EC_DRBG from recommendations shows that institutional trust can be damaged for years after a suspected weakness is introduced, even if the mechanism is technically complex and hard to prove in operational settings.

Juniper ScreenOS reveals a combined scenario: unauthorized code enabling administrative access and VPN decryption was found in firewall firmware, and the use of a controversial random number generator amplified the impact. This case underlines that backdoors may coexist with (or exploit) standardization weaknesses, and can remain undetected across multiple software revisions.

The XZ Utils incident demonstrates a modern supply-chain pattern: malicious code embedded upstream and activated during build processes, enabling potential compromise in widely deployed environments. It emphasizes the importance of independent builds, monitoring for anomalous changes in build artifacts, and focused review of maintainer transitions and contribution anomalies.

Recommendations for High-Trust Systems

For state and international systems, we recommend a layered program that combines:

(iv) transparent procurement requirements (including SBOM and secure development attestations);
(v) independent verification of critical software and firmware, with reproducible builds where feasible;
(vi) cryptographic agility and diversified implementations to avoid single points of trust;

(vii) governance controls on signing keys, update infrastructure, and privileged access; and

(viii) red-team exercises specifically focused on stealthy persistence and backdoor detection.

Finally, trust should be treated as a continuous process rather than a one-time certification. Kleptohygiene programs must be institutionalized: updated with new threat intelligence, audited regularly, and aligned with sectoral risk management for critical infrastructure.

Conclusion

Embedded backdoors represent a strategic threat because they target the very mechanisms by which systems establish security. By connecting classical kleptographic theory with modern supply-chain realities, and by proposing kleptohygiene as a preventive discipline, this paper aims to support more resilient trust policies for state and international digital infrastructures.

References

[1] A. Young and M. Yung, "Kleptography: Using Cryptography Against Cryptography," in Advances in Cryptology - CRYPTO '96, Lecture Notes in Computer Science, vol. 1109. Springer, 1997. doi:10.1007/3-540-69053-0_6.

[2] A. Young and M. Yung, "The Dark Side of 'Black-Box' Cryptography, or: Should We Trust Capstone?" in Advances in Cryptology - CRYPTO '96. Springer, 1996.

[3] National Institute of Standards and Technology (NIST), "NIST Removes Cryptography Algorithm from Random Number Generator Recommendations," Apr. 21, 2014.

[4] National Vulnerability Database (NVD), "CVE-2024-3094: XZ Utils / liblzma Backdoor," Mar. 29, 2024.

[5] Juniper Networks, "Multiple Security issues with ScreenOS (CVE-2015-7755, CVE-2015-7756)," Security Bulletin, Dec. 10, 2015.

[6] D. Scholl (Juniper Networks), "Important Announcement about ScreenOS," Dec. 17, 2015.

[7] T. Erb and D. Kobilke (Datadog Security Labs), "The XZ Utils Backdoor (CVE-2024-3094): what happened and what we know," Apr. 3, 2024.

[8] NIST, "Software Bill of Materials (SBOM) - Executive Order 14028: Improving the Nation's Cybersecurity," May 3, 2022.

[9] M. Ye. Shelest and Yu. M. Tkach, "Клептографія: від бекдору до політики довіри у цифрову епоху," Chernihiv, 2025, 312 p., ISBN 978-617-8539-04-7.

[10] Reuters, "Exclusive: Secret contract tied NSA and security industry pioneer," Dec. 20, 2013.

[11] The Washington Post, "How the CIA used Crypto AG encryption devices to spy on countries for decades," Feb. 11, 2020.

PHISHING WEBSITE DETECTION MECHANISMS

Olena Vysotska[1], Anatolii Davydenko[2] and Viacheslav Shmatukha[3]
[1] *State University "Kyiv Aviation Institute", ave. Liubomyra Huzara 1, 03058 Kyiv, Ukraine*
[2] *G.E. Pukhov Institute for Modelling in Energy Engineering NAS of Ukraine, str. General Naumov 15, 03164 Kyiv, Ukraine*
[3] *Kyiv School of Economaics, str. Mykoly Shpaka 3. 03113 Kyiv, Ukraine*

Abstract
This work is dedicated to the research and development of mechanisms for solving the task of phishing website detection, taking into account the current level of information technology development used in creating phishing attacks, and the necessary and relevant conditions for applying mechanisms to detect such websites. To this end, a neural network architecture was developed to solve the problem of phishing website detection, the proposed model was trained, and a series of experiments was conducted. A dataset was formed for training and testing this neural network, whose structure consists of two fields: the website URL and its type (legitimate site or phishing site), which allows the model to be trained for classifying sites into the corresponding two classes.

Keywords
Phishing sites, legitimate sites, neural network, classification, model training, characteristic features of phishing sites, dataset

Introduction

A well-known crime is organizing phishing attacks by creating or forging websites. Information about such attacks on well-known organizations appears in the media almost every day [1]. These facts are unacceptable for all enterprises, and even more so for critical infrastructure facilities. Therefore, the task of phishing website detection is undoubtedly relevant and requires research and development of mechanisms for its solution, taking into account the current level of development of information technologies used in creating phishing attacks, and the necessary and relevant conditions for applying phishing website detection mechanisms.

The task of phishing website detection.

The task of phishing website detection, like a significant number of other cybersecurity tasks [2], is a problem of pattern classification, meaning each website must be classified as either "phishing" or "legitimate". One of the most relevant and appropriate mathematical apparatuses for pattern classification is neural networks. Currently, there are a number of software solutions [3-4] for detecting phishing websites that use neural networks and machine learning to increase detection accuracy and reduce the number of false positives. However, each of these solutions has certain drawbacks and limitations. Therefore, the development of new software solutions for phishing website detection, based on neural networks that will be able to adapt to modern technologies for creating phishing sites and current conditions for detecting such sites, is relevant.

The goal of this work is the research and development of mechanisms for solving the problem of phishing website detection, taking into account the current level of information technology development used in creating phishing attacks, and the necessary and relevant conditions for applying mechanisms to detect such websites.

Develop a neural network architecture for solving the task

To achieve goal, the following tasks must be solved: Develop a neural network architecture for solving the problem of phishing website detection. Train the proposed model and, through experimentation. Draw conclusions based on the results of the experiments conducted.

Based on the analysis of the characteristics of the main types of neural networks, it was decided to use a Multilayer Perceptron (MLP) with the following architecture for the analysis of phishing websites in this study: Input Layer (number of neurons: 78, activation function: ReLU); Hidden Layer 1 (number of neurons: 10, activation function: ReLU); Hidden Layer 2 (number of neurons: 10, activation function: ReLU); Output Layer (number of neurons: 1, activation function: Sigmoid).

The proposed neural network model in this study, as mentioned earlier, used a vector of 78 features during training, but the most characteristic ones were identified in the course of the experiments. In these experiments, 100 legitimate and 100 phishing sites were analyzed, which resulted in the identification of the 19 critical features, the analysis of which is most appropriate for phishing website detection. Considering the level of technology development used to create phishing websites, analyzing the basic (fundamental) website characteristics, which is performed by most existing software for phishing website detection, is not always

sufficient for detecting such sites. To take into account the level of modern phishing website creation mechanisms, this study proposes carrying out a series of additional checks.

Based on the results of the conducted experiments, the following conclusions were drawn: the probability of correct classification of sites as phishing and legitimate, using this model, is 90%; a list of 19 website features that are most characteristic for classifying sites as legitimate and phishing was determined; it was determined that the proposed checks, which go beyond the analysis of basic (fundamental) website characteristics, due to the fact that they take into account characteristic factors relevant to modern phishing site creation technologies, allow for a more accurate determination of phishing sites and are therefore appropriate and effective; it was determined that when using an imbalanced dataset, the neural network begins to "favor" the class of which there were more samples in the training dataset, which is unacceptable when solving the problem of phishing website detection and proves the necessity of using a balanced dataset when training the neural network.

Conclusions

As a result of the conducted research, the following results were obtained:

A neural network architecture for solving the problem of phishing website detection was developed. The proposed model was trained and, through experimentation: the proposed model was evaluated; the most characteristic website features indicating its phishing nature were determined; the impact of performing the proposed checks, which go beyond the analysis of basic (fundamental) website characteristics performed by most existing software tools for phishing website detection, on the probability of correct site classification was determined; the impact of using imbalanced datasets on the quality of training the proposed neural network model was determined.

References

[1] Phishing Trends Report (Updated for 2025), 2025. URL: https://hoxhunt.com/guide/phishing-trends-report.

[2] O. Vysotska, A. Davydenko, O. Potenko, Modeling the mindfulness people's function based on the recognition of biometric parameters by artificial intelligence elements, Radioelectronic and computer systems 3 (2023), pp. 136-149. doi:10.32620/reks.2023.3.11.

[3] Hung Le, Quang Pham, Doyen Sahoo, Steven C.H. Hoi, URLNet: Learning a URL Representation with Deep Learning for Malicious URL Detection, 2018. URL: https://arxiv.org/pdf/1802.03162.

[4] Prevent. Detect. Respond. URL: https://deepphish.in/.

APPLICATIONS OF ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

Anton Herasymenko[1] and Oleksandr Korchenko[1]
[1] *State University of Information and Communication Technologies, Solomianska 7, 03110 Kyiv, Ukraine*

Abstract
This article presents an analysis of the evolving role and applications of Artificial Intelligence (AI) in cybersecurity, aiming to outline the possibilities of using machine learning algorithms, determine the dominant research focus, and identify the associated challenges. Bibliometric analysis of scientific publications reveals that the dominant research focus is dedicated to IDS (≈13% share) and Malware Classification (≈10% share), confirming the priority given to real-time anomaly detection and fighting common threats. However, the integration of AI introduces complex challenges, including the rise of Adversarial AI (AI used by attackers) and the vulnerability of AI models to manipulation (Adversarial Attacks). Consequently, fast-growing research trends are dedicated to developing resilient systems, such as Federated Learning for data privacy and Explainable AI (XAI) to address the "Black Box" problem and build trust in automated decision-making

Keywords
Artificial intelligence, cybersecurity of automating processes, dominant focus of using artificial intelligence in cybersecurity tasks, cybersecurity, adversarial attacks, explainable AI, federated learning

Introduction

The core role of AI, particularly Machine Learning (ML) and Deep Learning, is to enhance the speed and scalability of defensive mechanisms, which is critical for counteracting modern, highly automated cyber threats. The primary concern is the vulnerability of AI models themselves to Adversarial Attacks, where attackers manipulate data to bypass defenses. In response, there is a growing interest in developing robust systems and implementing Explainable AI (XAI), which allows humans to understand the system's decision-making logic. Additionally, Federated Learning is actively researched as a method for training AI models while preserving data privacy and confidentiality [1,2].

Therefore, the research tasks include: Outlining the possibilities of using machine learning algorithms in cybersecurity tasks by analysis publications; Determining challenges and threats of using artificial intelligence in cybersecurity tasks.

The main role of AI is to complement and enhance cybersecurity by automating processes and improving detection accuracy [3].

Analysis of publications

To obtain statistical data on publications, we will search for "bibliometric analysis of AI in cybersecurity" in scientific search engines (for example, Google Scholar or ResearchGate). Examples of the found studies [4,5] show general trends. Scientific research in the field of AI for cybersecurity has been undergoing a period of rapid acceleration since the mid-2015s. Therefore, we will formulate more appropriate criteria and conduct a new search limited to the last ten years. To conduct this study, we relied to search for articles about Cybersecurity and AI. The following search query was used to the literature search: "((cybersecurity OR cyber security OR cyber-security) AND Artificial intelligence)". To ensure a thorough picture of current research tendencies, a search was done to include publications from 2015 (the beginning of the past decade) up to the present year.

The vast majority of scientific articles (over 44,000 publications in the past ten years) focus on a few key applied areas, mainly related to the use of Machine Learning (ML) and Deep Learning (DL) for threat detection.

The United States, India, the United Kingdom, and China make significant contributions to research, highlighting the global nature of interest in this field.

Despite significant advantages, the integration of AI into security creates new challenges that are the focus of contemporary scientific research. The main problem is the vulnerability of AI models themselves to Adversarial Attacks, where attackers manipulate data to bypass protections. In response, there is growing interest in developing robust systems and implementing Explainable AI (XAI), which allows humans to understand the reasoning behind system decisions.

Bibliometric analysis of scientific publications reveals that the dominant research focus is dedicated to IDS (≈13% share) and Malware Classification (≈10% share), confirming the priority given to real-time anomaly detection and fighting common threats. However, the integration of AI introduces complex challenges, including the rise of Adversarial AI (AI used by attackers) and the vulnerability of AI models to manipulation (Adversarial Attacks). Consequently, fast-growing research trends are

dedicated to developing resilient systems, such as Federated Learning for data privacy and Explainable AI (XAI) to address the "Black Box" problem and build trust in automated decision-making.

Based on the bibliometric analysis, potential areas for future research are Explainable AI in Cybersecurity: Enhancing the interpretability and transparency of AI algorithms can be using in AI-based Cybersecurity.

Conclusions

This work proposes analysis of publications with main topics using AI in Cybersecurity. The main conclusion of analysis is: Dominant Focus: The largest share of research effort is dedicated to Intrusion Detection Systems (IDS) and Malware Classification. This highlights the scientific community's priority in using AI for real-time anomaly detection and fighting the most common and damaging threats. Emerging Trends: The topics of Adversarial Machine Learning (making AI models resilient to attack) and Federated Learning (AI training while preserving data privacy) show significant dedicated research, even if their percentages are currently smaller than the traditional detection topics. These areas are, however, among the fastest-growing trends. Broad Scope: The large "Other" category (≈47%) indicates the vast interdisciplinary nature of the field, encompassing niche yet critical areas like Explainable AI (XAI), advanced Authentication mechanisms, and specific Cloud Security applications.

References

[1] Yazici, I. Shayea, and J. Din, "A survey of applications of artificial intelligence and machine learning in future mobile networks-enabled systems," Engineering Science and Technology, an International Journal, vol. 44, pp. 0-0, 2023.

[2] Lande D., Novikov O., Alekseichuk L. Application of Large Language Models for Assessing Parameters and Possible Scenarios of Cyberattacks on Information and Communication Systems // Theoretical and Applied Cyber Security. Vol. 6 No. 1 (2024). DOI: 10.20535/tacs.2664-29132024.1.315242

[3] F. Hang, L. Xie, Z. Zhang, W. Guo, and H. Li, "Artificial intelligence enabled fuzzy multimode decision support system for cyber threat security defense automation," Journal of Computer Virology and Hacking Techniques, vol. 19, no. 2, pp. 0-0, 2023.

[4] O. S. Albahri and A. H. AlAmoodi, “Cybersecurity and Artificial Intelligence Applications: A Bibliometric Analysis Based on Scopus Database,” Mesopotamian Journal of CyberSecurity, vol. 2023, pp. 158–169, Sep. 2023, doi: 10.58496/MJCSC/2023/018.

[5] S. Saeed, S. A. Suayyid, M. S. Al-Ghamdi, H. Al Muhaisen, and A. M. Almuhaideb, “A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience,” Sensors, vol. 23, no. 16, p. 7273, Aug. 2023, doi: 10.3390/s23167273.

METHODS OF IMPROVE THE SECURITY OF INFORMATION PROCESSING IN USING TOOLS WITH OPEN VIDEO INFORMATION EXCHANGE CHANNELS

Yuliia Tkach[1] and Ihor Diuba[1]
[1] *Chernihiv Polytechnic National University, str. Shevchenko 95, 14030 Chernihiv, Ukraine*

Abstract

This study analyzes the limitations and proposes a multi-faceted approach to enhance data protection in the management of devices with open information channels. Furthermore, this work proposes the application of a multilevel access system model for planning UAV missions. This model leverages secret data from a state information system to construct flight paths that inherently mitigate the risk of tactical information disclosure, granting authorization based on the task's sensitivity level rather than solely the user's access rights.

Keywords
access protection, multi-level access model, confidentiality assurance

Introduction

The use of information technologies provides many advantages, but these advantages, in cases of conflict situations, can be used by the other side of the conflict. For example, intercepting a drone with a flight path recorded on a flash drive can lead to the disclosure of the launch point coordinates and potentially reveal the position of the drone operator. The purpose of this study is to analyze the limitations that arise when using tools with open video information exchange channels and to develop methods that can improve the security of information processing in these cases [1].

The task of improve the security of information processing in using tools with open video information exchange channels.

To solve the task, we will consider three main directions:

1)Lightweight Cryptography and Channel Authentication (Lightweight Security). This direction is key, as UAV onboard systems have limited resources (battery, computational power).

2)Secure Video Coding at the Compression Level. This area leverages video compression features (e.g., H.264/H.265) to integrate protection.

3)Channel Resilience and Protection against EW/Interception (Anti-Jamming & Anti-Eavesdropping). These studies concern the physical resilience of the transmission channel under conditions of active hostile interference.

The goal of this work is the research and development of mechanisms for solving the task of improve the security of information processing in using tools with open video information exchange channels.

Using a multilevel access model for data protection for solving the task

To achieve goal, the following tasks must be solved: The first problem can be solved organizationally by changing the deployment location after launching the drone. The third problem cannot be resolved within the initial conditions and requires switching to a secure communication channel, which is not always possible, or transferring surveillance to another reconnaissance means. The second problem could be solved through preliminary planning, but this requires additional information that may be unavailable due to the operator's insufficient access level. Therefore, the task of using a multilevel access model for data protection when planning UAV routes is relevant, and this is precisely what is proposed in this work. Multilevel access systems to information resources ensure the possibility of implementing optimal procedures for accessing data and other means of an information system [2].

A user presenting a task that requires data characterized by secrecy, for example, of the first level, is registered in the access system, and the task is registered in the authorization granting system. If the access system has authenticated the user, then, in the case where the task requires data with the first level of secrecy, it must provide the system with specific data about the task. The user who enters the task into the system may not know the level of secrecy of the data required for the task. Therefore, the task information can be entered in full. After the task is granted authorization, fragments of algorithms that define the permissible ways of using the first-level data perform the corresponding transformations, and only the result of these

transformations, which no longer has a secrecy level, is transmitted to the task, and the task is activated from the point for which the data from the system are inputs [3].

In our case, this can be interpreted as follows: mapping information about the route is available to the user, while operational information with restricted access must be processed taking into account the UAV's properties and a special subroutine belonging to the system. Based on this, a UAV movement route is built, the use of which reduces the probability of information disclosure [4,5].

The study included modeling the system's operation using hypothetical route and operational data, and demonstrated the feasibility of using this approach.

Conclusions

A model of a multilevel access system is proposed for defining the parameters of application tasks. This model, by using secret data from the state information system independently of the user who presented the corresponding task, allows the authorization granting system to make decisions while avoiding dangers that may arise under the influence of user actions.

References

[1] C. Chen, Z. Wang, Z. Gong, P. Cai, C. Zhang, Y. Li, Autonomous Navigation and Obstacle Avoidance for Small VTOL UAV in Unknown Environments, Symmetry 2022, 14, 2608. https:// doi.org/10.3390/sym14122608.

[2] Constantin-Adrian Ciolponea, The integration of unmanned aircraft system (uas) in current combat operations, Land Forces Academy Review, Vol. XXVII, No 4(108), 2022. URL: Available: [https://www.researchgate.net/publication/367055350_The_Integration_of _Unmanned_Aircraft_System_UAS_in_Current_Combat_Operations].

[3] O. Sulima, Model of multilevel access system, Ukrainian Scientific Journal of Information Security, 2017, vol. 23, issue 2, p. 122-129. doi: 10.18372/2225-5036.23.11817.

[4] Y. Zhou, L. Ma, M. Wen, Task-Constrained RBAC Model and Its Privilege Redundancy Analysis, 2nd International Conference on Information Science and Control Engineering, pp. 489–492, 2015.

[5] M. Ren, B. Wang, J. Liu, Conception of Foreign Heterogeneous Electronic Warfare UAV Cross Domain Cooperative Operations. In: Y. Qu, M. Gu, Y. Niu, W. Fu, eds, Proceedings of 3rd 2023 International Conference on Autonomous Unmanned Systems (3rd ICAUS 2023). ICAUS 2023. Lecture Notes in Electrical Engineering, vol 1171. Springer (2024), Singapore. doi:10.1007/978-981-97-1083-6_2.

HYBRID METHOD FOR MALICIOUS ACTIVITY DETECTION IN INFORMATION SYSTEMS

Halyna Haydur[1] , Dmytro Hamza[2]
[1,2] *State University of Information and Communication Technologies, Solomianska 7, 03110 Kyiv, Ukraine*

Abstract
In this paper, we propose a hybrid ensemble method (stacking) for cyberattack detection, consisting of classical algorithms and gradient descent. Special attention is paid to complex preprocessing: normalization, application of SMOTE for class balancing, and PCA for dimensionality reduction. The Pareto front method is used for model selection. Experiments on the CSE-CIC-IDS2018 database showed an accuracy of 98.07% and a prediction time of 7.16 ms. The hybrid approach has proven its effectiveness for real-time system protection.

Keywords
Threats, intrusion detection, hybrid classification, stacking, cybersecurity, cyber defense, machine learning, models, malicious activity

Introduction

The increasing complexity of digital infrastructure makes traditional signature-based intrusion detection (ID) systems ineffective against new and polymorphic attacks [1]. Although machine learning methods provide adaptability, individual classifiers (SVM, kNN, neural networks) have limitations in terms of scalability and sensitivity to noise. Ensemble methods, in particular stacking, can overcome these shortcomings, improving the generalization ability and efficiency of the system, but the issue of balancing accuracy and fast real-time stability remains relevant. To solve these problems, a hybrid stacking architecture is proposed, which integrates classical algorithms (SVM, Random Forest, kNN) and gradient boosting models (XGBoost, LightGBM, CatBoost) [3]. A feature of the approach is the use of multi-level metaclassifiers and modern preprocessing methods: the SMOTE algorithm for class balancing, PCA for dimensionality reduction, and a temporal engineering feature. This ensures efficient processing of multidimensional data and adaptation to changes in network traffic behavior.

The research method is the creation and verification of a highly accurate low-latency SVR for corporate environments. Experimental validation this year on the current CSE-CIC-IDS2018 dataset. The work is aimed at achieving accuracy rates of over 98% and time prediction within 5–10 ms, which meets the requirements for a modern cyber defense system capable of operating effectively under high load in real time.

Methodology

The proposed hybrid malicious activity detection system uses the following algorithms, selected based on their basic proven advantages in classification and anomaly tasks:

1. Support Vector Machine (SVM).
2. Random Forest.
3. k-Nearest Neighbors (kNN) is used in classification tasks.
4. XGBoost (Extreme Gradient Boosting) solves the speed and accuracy.
5. LightGBM scales well on large datasets
6. CatBoost: a boosting model with built-in support for categorical feature processing and less sensitive to the choice of hyperparameters.

The combination of different algorithms allows to compensate for the weaknesses of each individual method, minimizing the risk of overtraining and, as a result, providing a significant increase in the accuracy and stability of the system to new, previously unknown types of cyberattacks.

Experimental Results

Stacking Ensemble Performance

Comparison of different combinations of base classifiers within the stacking approach demonstrates significant improvement compared to individual models. Table 1 presents the performance of various stacking configurations with different base model combinations and meta-classifiers [2].

Two approaches were used to select the best combination of models: comparison with the average values of metrics and construction of the Pareto front.

The Pareto front method. The Pareto front method was used to analyze the effectiveness of model combinations, which allows you to determine a set of architectures that are not inferior to each other

simultaneously in accuracy, F1-score and prediction time, providing an optimal choice depending on system requirements.

Based on the data, two non-dominated combinations were identified:

1. Accuracy = 0.9807, F1-score = 0.9657, Time = 7.16 ms (XGBoost, CatBoost, LightGBM with XGBoost as metaclassifier)

2. Accuracy = 0.974, F1-score = 0.959, Time = 6.51 ms (CatBoost, LightGBM, Extra Trees with XGBoost as metaclassifier)

Table 1. Comparative table of user digital fingerprinting methods.

Base Models	**Meta-Classifier**	**Accuracy**	**F1-Score**	**Time (ms)**
XGBoost + CatBoost + LightGBM	XGBoost	0.9807	0.9657	7.16
XGBoost + CatBoost + Random Forest	XGBoost	0.9801	0.9654	7.57
XGBoost + CatBoost + Random Forest	Gradient Boosting	0.9797	0.9637	7.83
XGBoost + CatBoost + LightGBM	Gradient Boosting	0.9793	0.9633	7.4
XGBoost + CatBoost + LightGBM	Random Forest	0.9787	0.9647	7.48
XGBoost + CatBoost + Random Forest	Random Forest	0.9785	0.9632	7.91
XGBoost + CatBoost + LightGBM	Logistic Regression	0.9767	0.9617	6.91
XGBoost + CatBoost + Random Forest	Logistic Regression	0.9761	0.9603	7.31
CatBoost + LightGBM + Extra Trees	XGBoost	0.974	0.959	6.51
CatBoost + LightGBM + Extra Trees	Gradient Boosting	0.973	0.957	6.73

Among all combinations, only one met these conditions: Accuracy = 0.9807, F1 = 0.9657, Prediction Time = 7.16 ms. This combination is implemented based on the XGBoost, CatBoost, LightGBM models with XGBoost as a metaclassifier.

Conclusions

The obtained results demonstrate that the stacking model can surpass the efficiency of individual classifiers and can be practically implemented in high-load corporate information systems.

References

[1] G. I. Haydur, S. O. Gakhov, D. E. Hamza, Model for detecting malicious activity in the organization's information system based on hybrid classification, Modern Information Security, 4(60) (2024) 30–38. doi:10.31673/2409-7292.2024.040003.

[2] Canadian Institute for Cybersecurity, IDS 2018 Dataset, University of New Brunswick, 2018. URL: https://www.unb.ca/cic/datasets/ids-2018.html.

[3] G. Kaur, H. S. Saini, Stacking ensemble learning for network intrusion detection systems, International Journal of Computer Applications, 184(12) (2023) 15–23. doi:10.29130/dubited.737211.

EXPERIMENTAL STUDY OF A PROBABILISTIC CYBERATTACK DETECTION MODEL WITH MARKOV PROPERTY

Nataliia Vyshnevska[1], Valerii Kozlovskyi[2], Yurii Lystskyi[3], Stanislava Kudrenko[4] and Diana Kozlovska[5]
[1,2,3,4,5] State University "Kyiv Aviation Institute" Ukraine, Kyiv,Lubomyr Huzar Ave.,1

Abstract
This paper presents the results of an experimental evaluation of the effectiveness of a probabilistic cyberattack detection model with a Markov property. The model is based on multiscale network traffic analysis, computation of an integrated anomaly indicator, and estimation of the posterior probability of the system state while accounting for previous dynamics. The behavior of the model is analyzed under normal, anomalous, and noisy activity conditions.

Keywords
Probabilistic model, Bayesian approach, Markov property, anomaly detection, cyberattack, network traffic

1. Introduction

Ensuring timely and reliable detection of cyberattacks is one of the key challenges faced by modern information systems. The diversity of attack vectors, unpredictable dynamics of network traffic, and the presence of noise events significantly complicate the operation of traditional security systems based on static thresholds or signature-based approaches.

Detection of inertial and stealth attacks poses a particular challenge, as such attacks evolve gradually and may be masked by background fluctuations. This necessitates the development of adaptive models with probabilistic logic capable of incorporating integrated anomaly indicators and contextual information from previous system states for effective threat recognition.

Therefore, experimental validation of such approaches under mixed load scenarios—where normal operation, attack phases, and noise coexist—is of particular relevance.

2. Main Body.

The effectiveness of the proposed probabilistic cyberattack detection model was evaluated through a series of simulation experiments. For each scenario, a set of traffic parameters was generated, integrated anomaly indicators were computed, system states were determined, and the posterior probability of an attack at each time instant was estimated [1, 2].

The model performance was demonstrated over 100 network traffic time steps. The test dataset included periods of normal operation, three attack intervals occurring at time steps 20–25, 45–55 and 75-78 as well as two noise events, aimed at assessing the model's robustness to fluctuations and false alarms.

The values of the integrated anomaly indicator I_t varied within the range of [0,1; 0,9]. Deviations within the interval [0,1; 0,55] - were not classified as anomalies, even in the presence of short-term peaks or background noise. Values in the range of [0,6; 0,75] did not immediately trigger detection but could lead to attack identification when accumulated over time. Single or sustained values exceeding 0,75 often resulted in threat detection.

A decrease of indicator values below 0,6 corresponded to threat attenuation. However, if an attack had been observed previously, the system state could remain elevated due to the inertia inherent in the model.

The conditional likelihood of an anomaly was defined as the result of mapping the integrated anomaly indicator through a transformation function.

$$\tilde{y}_t = f(I_t) = \begin{cases} 0, & I_t < \theta_0 \\ \dfrac{I_t - \theta_0}{1-\theta_0}, & I_t \geq \theta_0 \end{cases},$$

To account for process inertia, the posterior probability of the system state was computed using a Markovian update mechanism.

$$Y_t = \alpha \cdot f(I_t) + (1-\alpha) \cdot Y_{t-1},$$

The model's response to different event types—attack phases, normal activity, and noise bursts—was analyzed.

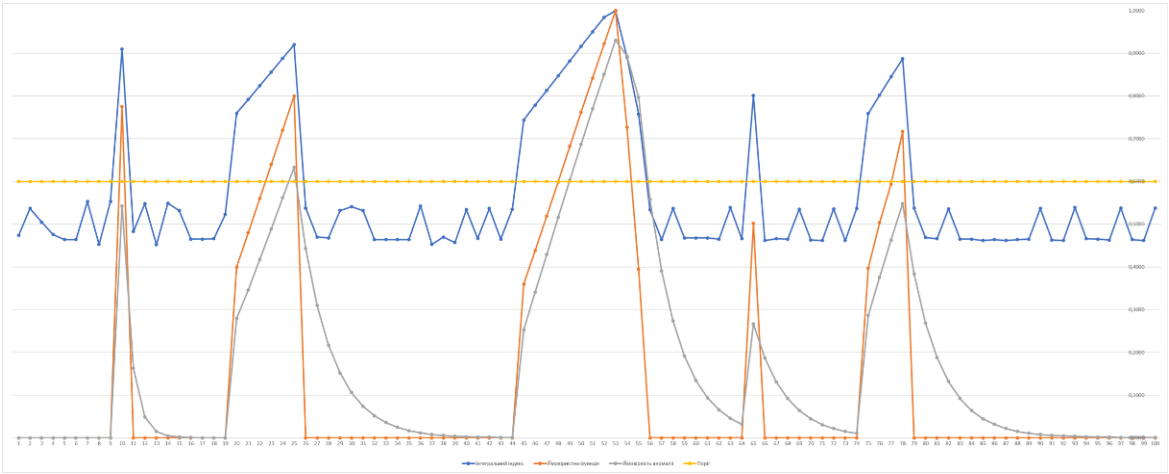

Figure 1 illustrates the dynamics of the integrated anomaly indicator, the conditional likelihood, and the posterior probability of an attack under simulated mixed network load conditions.

According to the simulation results, all three attacks were successfully detected, as the posterior probability exceeded the threshold during the intervals 20–25, 45–55, 75–78. Short-term noise peaks did not cause false alarms, as inertia-based smoothing kept the posterior probability below the detection threshold. One false-positive event was recorded at time step 65 due to the combined influence of short-term noise and weak inertia.

The developed probabilistic model can be integrated into network traffic monitoring systems. Its implementation does not require storing the complete observation history, which simplifies real-time application. To enhance flexibility, dynamic updating of model parameters based on accumulated statistical data reflecting network behavior is recommended [1, 3, 4].

3. Conclusions.

The probabilistic model demonstrates high threat detection accuracy, adaptability to changing network conditions, and robustness against false-positive detections. The results of the demonstration simulation confirm its capability to identify both pronounced attacks and gradual or masked attack phases. A promising direction for further improvement involves incorporating mechanisms for real-time dynamic parameter updating, including adaptive adjustment of thresholds, inertia coefficients, and transition probabilities based on evolving traffic statistics. In future research, the model may be adapted for online response systems, integrated into cybersecurity architectures for critical infrastructure, and extended toward multiclass classification of attack types.

References:

[1] Liang Liu, Huaiyuan Wang, Zhijun Wu, Meng Yue, The detection method of low-rate DoS attack based on multi-feature fusion, Digital Communications and Networks, Volume 6, Issue 4, 2020, Pages 504-513, ISSN 2352-8648, https://doi.org/10.1016/j.dcan.2020.04.002.

[2] Anukool Lakhina, Mark Crovella, and Christophe Diot. 2004. Diagnosing network-wide traffic anomalies. SIGCOMM Comput. Commun. Rev. 34, 4 (October 2004), 219–230. https://doi.org/10.1145/1030194.1015492

[3] Mulualem Bitew Anley, Angelo Genovese, Davide Agostinello, Vincenzo Piuri, Robust DDoS attack detection with adaptive transfer learning, Computers & Security, Volume 144, 2024, 103962, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2024.103962.

[4] Xiong A. Theory of Markov Chain Monte Carlo and its several applications//Science & Technology of Engineering, Chemistry and Environmental Protection. 2024. Vol. 1.

ANALYZING SECURITY OF DSTU 9041:2020 AND ITS MODIFICATIONS AGAINST DISTINGUISHING ATTACKS

Oleksii Bespalov [1], Anatolii Davydenko[1], and Lyudmila Kovalchuk[1]
[1] *G.E. Pukhov Institute for Modelling in Energy Engineering NAS of Ukraine*

Abstract
The National Standard of Ukraine "Information Technologies. Cryptographic Protection of Information. Algorithm for Encryption of Short Messages Based on Twisted Edwards Curves" (DSTU 9041:2020, [1]) was adopted 5 years ago. This is a so-called hybrid encryption algorithm based on the KEM/DEM (Key Encapsulation Mechanism/Key Decapsulation Mechanism) paradigm. The algorithm uses both symmetric and asymmetric encryption methods. It is primarily focused on the transmission of encrypted keys for symmetric algorithms, but can also be used to transmit encrypted messages together with the encryption key.The most important distinguishing attacks are Chosen Ciphertext Attack and Chosen Plaintext Attack. Security of DSTU 9041 against these two attacks is the subject of investigation in this work. We proved its security against CPA, under hardness of DDHP, and showed why we cannot prove the same statement for CCA. Next, we proposed some approaches, which may cause CCA security.

Keywords
Aasymmetric cryptology, hybrid encryption, distinguishing attacks, CPA, CCA, DDHP

The National Standard of Ukraine "Information Technologies. Cryptographic Protection of Information. Algorithm for Encryption of Short Messages Based on Twisted Edwards Curves" (DSTU 9041:2020, [1]) was adopted 4 years ago. This is a so-called hybrid encryption algorithm based on the KEM/DEM (Key Encapsulation Mechanism/Key Decapsulation Mechanism) paradigm. The algorithm uses both symmetric and asymmetric encryption methods. It is primarily focused on the transmission of encrypted keys for symmetric algorithms, but can also be used to transmit encrypted messages together with the encryption key.

Its secure against basic cryptoattacks has been analyzed in several publications, in particular, it was proven that it is impossible to recover the plaintext or key, provided that the discrete logarithm problem is hard to solve [2]. However, the question of security of this algorithm against so-called distinguishing attacks still remains open.

The most important distinguishing attacks are CCA (Chosen Ciphertext Attack) and Chosen Plaintext Attack (CPA) [3]. Security of DSTU 9041 against these two attacks is the subject of investigation in this work. Security DSTU 9041 against CPA and CCA.

In the current conditions of the continuous evolution of cyberattack techniques, the use of traditional static methods of user identification is insufficient. The formation of a digital fingerprint is based on the principle of variable combinations of unique browser attributes, operating system (OS) settings, and user device characteristics [1].

A comprehensive analysis of modern user identification techniques allows for their detailed examination, determination of advantages and disadvantages, and drawing certain conclusions regarding their application for identifying anonymous users in countering cyber threats to critical infrastructures.

According to the theorems 11.12 and 11.14 [3], hybrid encryption:

- is CPA-secure, if KEM is CPA-secure and has indistinguishable encryption in the presence of an eavesdropper;

- is CCA-secure, if KEM and $E_t(\cdot)$ are CCA-secure.

Then to prove its security, we need to split it into parts, KEM and symmetric encrypting algorithm, and analyze their security separately.

Algorithm 1. KEM-mechanism in DSTU-9041

Input: elliptic curve parameters (corresponding prime field, coefficients a and d, base point P, subgroup order q);

Alice`s public key H;
message m.

1. Choose randomly ε, $2 \le \varepsilon \le q-2$, and calculate curve point $R = \varepsilon P = (x_R, y_R)$.

2. Set $r = x_R$.

3. Calculate point $T = \varepsilon H = (x_T, y_T)$.

4. Set $t = x_T$.

Output: key t; ciphertext r.

Algorithm 2. Symmetric encryption $E_t(\cdot)$ in DSTU 9041.

Input: key t

elliptic curve parameters (corresponding prime field, coefficients a and d, base point P, subgroup order q);

Alice`s secret key h;

symmetric encryption algorithm E;

key t for symmetric encryption.

1. Calculate $u = E_t(m)$, using t (or some part of its bit representation, according to key format) as key for symmetric decryption algorithm.

Output: ciphertext u.

Theorem (CPA-security of DSTU 9041).

Under the DDH-assumption and assumption that algorithm Kalyna has indistinguishable encryption in the presence of an eavesdropper, hybrid encryption algorithm from DSTU 9041 is CPA-secure.

Proof (scratch). According to the theorem 11.12 [3], it's enough to prove that KEM, described in Algorithm 3, is CPA-secure. Prove from contradiction: let the adversary can distinguish between the triplet (H, r, t), obtained according to Algorithm 3, and the triplet (H, r, u), where u is x-coordinate of random point of corresponding elliptic curve group (in this case, key space coincides with this group). It means, that, according to the Note 1, he can distinguish between the triplet (H, R, T), obtained according to Algorithm 3, and the triplet (H, R, U), where U is random point of elliptic curve group (or of its subgroup). Then they can solve DDH problem, and we get contradiction with our assumption about CPA-security of DDHP.

The theorem is proved. In this work we proved that, under Distinguishing Diffie-Hellman assumption, and the corresponding assumption about algorithm Kaluna (in Key Wrapped Mode), the hybrid encryption algorithm, proposed in DSTU 9041:2020, is secure against Chosen Plaintext Attack. But the question about its security against Chosen Ciphertext Attack is still opened. As we cannot apply theorem which formulates sufficient conditions for its security, we can neither confirm nor deny the statement about its security.

But it may be possible to modify this algorithm in a such way that allows to achieve desired security. For example, one of the possible ways may be adding some transformation with specific properties in this algorithm, like hashing. But in this case the corresponding definitions should be formulated, concerning properties of cryptographic hash-function and its security against distinguishing attacks.

References

[1] DSTU 9041:2020 Information technology. Cryptographic information protection. Short message encryption algorithm, based on twisted Edwards curves. https://ukrmts.com/docsdb/28885.html

[2] A. Bessalov, L. Kovalchuk, N. Kuchynska, O. Telizhenko, *Algorithm for short messages encryption on twisted Edward curves*, *20th Central European Conference on Cryptology,* CECC 2020, Zagreb, p. 16-17. https://web.math.pmf.unizg.hr/~duje/cecc2020/

MULTIAGENTIC PRODUCT LIFECYCLE SUPPORT PLATFORM - THE BASIS OF UKRAINE'S CYBERSECURITY

Andrii Sobchak[1], Volodymyr Kvasnikov[2], Nikita Sobchak[3], Denis Sobchak[4] and Nataliia Kovshar[5]
[134]National Aerospace University«Kharkiv Aviation Institute», Vadim Manka 17, 61070 Kharkiv, Ukraine
[2]State University «Kyiv Aviation Institute», Liubomyra Huzara Avenue 1, 03058 Kyiv, Ukraine
[5]SPE KIATON GRUP, Astronomichna 17, 61085 Kharkiv, Ukraine

Abstract:

The article presents an original development — the KIATON MAS 2025 multi-agent platform designed to support the full product life cycle at virtual instrument manufacturing enterprises.

Unlike existing analogues, the platform integrates self-learning mechanisms for agents, blockchain-based transaction authentication, and intelligent cyberthreat prediction.

The development was first implemented in the industrial environment of KIATON GRUP LTD and demonstrates a significant increase in efficiency and data security.The methodological contribution of this research lies in the conceptualization of a hyper-resilient cyber-physical enterprise, where informational, production, and managerial processes are integrated into a unified semantic and trust-based digital environment. The KIATON MAS 2025 platform illustrates the transition from traditional management systems to self-organizing adaptive ecosystems capable of autonomous evolution under conditions of high uncertainty.

Keywords: multi-agent system, cybersecurity, instrument engineering, product life cycle, blockchain, machinery, KIATON MAS 2025

Introduction

Current trends in the digitalization of Ukraine's industry require the integration of intelligent systems and cybersecurity tools.

The digitalization of production processes in Ukraine, particularly in the field of instrument engineering, is a strategically important direction for the modernization of the national economy. In the context of Russian aggression, global competition, and integration into global production chains, Ukrainian enterprises are faced with the need to introduce advanced technologies that ensure increased efficiency and competitiveness.

Traditional PLM systems are not flexible enough to adapt to dynamic cyber threats. At the same time, multi-agent systems (MAS) provide decentralized decision-making and self-organization, making them the basis for building cyber-resilient digital enterprises.

The relevance of this topic stems from the need for a comprehensive approach to cybersecurity based on modern technologies, including machine learning, blockchain, and multi-agent methods. Research in these areas contributes to the creation of intelligent security systems capable of adapting to the dynamic conditions of the digital environment and ensuring the stable operation of industrial and information systems.

The goal of this study is to develop a multi-agent platform to support product lifecycle elements at virtual instrument manufacturing enterprises in Ukraine, with an emphasis on ensuring cybersecurity. To achieve this goal, the following tasks were set:

1. Develop the architecture of a multi-agent platform with the integration of machine learning and blockchain technologies.
2. Find methods for analyzing and managing risks in production activities.
3. Propose algorithms for detecting anomalies and predicting threats in real time.
4. Conduct practical testing of the platform using Ukrainian enterprises as examples.

The proposed approach not only increases the level of cybersecurity, but also optimizes the product life cycle, creating conditions for the effective digital transformation of Ukrainian industry.

Multi-agent systems in industry

Multi-agent systems (MAS) are a collection of intelligent software agents that interact with each other and the external environment to achieve common goals. Agents minimize inter-node information interactions by eliminating the human factor while maintaining performance quality and reducing information processing time.

Multi-agent systems demonstrate high potential for managing complex production processes and ensuring the safety of smart factories. The use of adaptive learning models increases the flexibility and resilience of virtual manufacturing plants [1].

General concept of the KIATON MAS 2025 platform

The platform consists of three hierarchical levels:

1. Analytical agents (AI-Core): self-learning, anomaly detection, forecasting, risk assessment.

2. Functional agents (ProdAgent): resource management, production control, data aggregation, data collection.

3. Security agents (SecAgent): blockchain verification, cryptography, authentication, encryption, threat mitigation.

The system uses a distributed blockchain registry (Trust-Ledger) to ensure data integrity.

Each agent interacts with others via the secure MAS-Link protocol, forming a trusted information exchange environment.

All communication events are recorded in the Trust-Ledger blockchain registry, ensuring data immutability and traceability.

Analytical model of interaction

4.1. Model of data exchange between agents

$$I_{ij}(t) = \alpha_{ij} \times \ln(1 + \beta D_i R_j), \quad (1)$$

where

$I_{ij}(t)$ — is the intensity of information interaction,

α_{ij} — is the confidence coefficient of communication,

D_i — is the volume of data,

R_j — is the level of receiver resources.

3.2. Model of dynamic stability of the system

$$S(t) = \frac{\sum_{i=1}^{n} (Di \pm Qi)}{\sqrt{\sigma^2 + \mu^2}}, \quad (2)$$

where

Q_i — agent performance quality,

σ^2— incident variance,

μ — average threat intensity.

3.3. Adaptive agent learning function

where

L — agent error level,

E — system error,

W — machine learning model weights,

η — learning rate.

Cybersecurity methods

The SecAgent module operates on the principle of three-level protection:

Level 1: Cryptographic protection (RSA/AES-256) for inter-agent communications.

Level 2: Blockchain authentication (Trus-Ledger) protection against event forgery.

Level 3: Machine learning for anomaly detection (Isolation Forest, Autoencoder).

The reactive threat response protocol provides predictive protection.

The system's response to threats is described by the function:

$$R(t) = k \times e^{-\lambda t}, \quad (3)$$

where

R(t) — is the probability of successful defense,

λ — is the rate of threat propagation,

k — is the adaptive response coefficient.

Results of implementation at KIATON

In 2025, the KIATON MAS 2025 multi-agent platform was implemented in the enterprise production management system.

Simulations were performed in MATLAB and Python. The following results were obtained:

Table 1

Indicator	Before implementation	After implementation
Average response time to threats, from	14	5
Number of cyber incidents/month	23	13
Data analysis performance	100%	135%
Data protection level (ENISA assessment)	0.72	0.93

Conclusions

Modern instrument-making enterprises in Ukraine are facing increasing demands for digital transformation in line with Industry 4.0–5.0 standards. Therefore, in the context of the rapid development of digital technologies, cybersecurity issues are becoming paramount. The growth of data volumes, the introduction of the Internet of Things, distributed computing, and artificial intelligence are creating new opportunities for industrial development, but simultaneously increasing the vulnerability of digital systems to cyberattacks and unauthorized access [3].

The practical implementation of security systems requires a comprehensive approach, incorporating hardware and software. Research on digital integrated circuits and virtual manufacturing systems shows that combining theoretical models and experimental data improves enterprise performance [4].

One of the key areas of modern development is the use of machine learning and artificial intelligence to enhance the resilience of cybersecurity systems [2]. These technologies automate the threat detection process, adapt defense mechanisms to changing conditions, and improve the effectiveness of network activity monitoring.

Effective product lifecycle management (PLM) requires the integration of distributed intelligent systems capable of autonomous decision-making, threat detection, and adaptive control [5].

Multi-agent systems (MAS) offer a promising approach, allowing autonomous agents to interact dynamically to optimize production, predict cyber threats, and maintain system stability.

However, existing MAS platforms often lack mechanisms for the secure integration of lifecycle elements in highly sensitive industrial environments.

To address this challenge, the KIATON MAS 2025 platform has been proposed, providing a secure, adaptive, and analytically transparent environment for virtual instrument manufacturing enterprises in Ukraine.

The system was implemented and industrially validated at the research and production enterprise KIATON, where it was tested under real production conditions for managing the life cycle of instrument-engineering products.

In conclusion, KIATON MAS 2025 can be regarded as a reference architecture for cyber-resilient intelligent manufacturing systems, achieving a balance between autonomy, security, and cognitive adaptability. The obtained results establish a foundation for further research in multi-agent technologies, industrial artificial intelligence, and next-generation cybersecurity frameworks.

References

[1] Kopei V. Designing a Multi-Agent PLM System for Threaded Products / V. Kopei // Machines. – 2023. – Vol. 11, No. 2. – P. 263–275. – DOI: https://doi.org/10.3390/machines11020263/.

[2] Li X., Zhang P. Blockchain-Driven Security in Industrial Systems / X. Li, P. Zhang // IEEE Transactions on Industrial Informatics. – 2023. – Vol. 19, No. 4. – P. 512–524. – DOI: https://doi.org/10.1109/TII.2023.3234567/.

[3] Pavlenko A., Kozlov V. Adaptive Multi-Agent Learning for Smart Factories / A. Pavlenko, V. Kozlov. – Warsaw : Elsevier, 2024. – 238 p. – URL: https://www.elsevier.com/books/adaptive-multi-agent-learning/.

[4] Sobchak A., Shcherbak Y. Elektronni prystroi na tsyfrovykh intehral′nykh mikroskhemakh : metod. vkazivky do lab. robit z dysts. Mikroskhemotekhnika* / A. Sobchak, Y. Shcherbak. – Kharkiv: KhDAZT, 2000. – 36 s. – URL: https://www.khdazt.edu.ua/elektronni-prystroi/.

[5] Sobchak A. P., Shostak I. V. Otsinka efektyvnosti funktsionuvannia virtual′noho vyrobnychoho pidpryiemstva z vykorystanniam poniattia hiperustiikosti / A. P. Sobchak, I. V. Shostak // Traektoriia Nauky : elektron. nauk. zhurn. – 2016. – №2(7). – S. 4.2–4.10. – URL: https://traektoria.com.ua/article/virtual-production-efficiency/.

DIAGONAL AND SEQUENTIAL CIPHERS AND THEIR COMPOSITIONS

Dmytro Dyiak[1], Oleg Gutik[2], Yaryna Kokovska[3], and Petro Venherskyi[4]
[1]Ivan Franko National University of Lviv, Universytetska 1, 79000 Lviv, Ukraine
[2]Ivan Franko National University of Lviv, Universytetska 1, 79000 Lviv, Ukraine
[3]Ivan Franko National University of Lviv, Universytetska 1, 79000 Lviv, Ukraine
[4]Ivan Franko National University of Lviv, Universytetska 1, 79000 Lviv, Ukraine

Abstract
We present the sequential cipher S, which generated main principles of the Vigenère cipher, has high resistance to breaking, and is conceptually closer to the Gilbert-Vernam cipher. The sequential cipher has a linear complexity and hence its encryption and decryption are very quick. Also, we consider the diagonal cipher D which is presented in [2] and its encryption and decryption have the linear complexity, as well. We study the composition $\mathcal{DS}$ and $\mathcal{SD}$ of the diagonal and the sequential ciphers.

Keywords
diagonal cipher, sequential cipher, permutation, complexity of encryption, complexity of decryption.

Introduction

One of the first attempts to generalize the shift cipher (Caesar's cipher) was the Vigenère cipher. Although the Vigenère cipher was first proposed by the Italian Giovanni Battista Bellaso in 1553 in the monograph "La cifra del Sig." [1], it is named after the French diplomat Blaise de Vigenère and was described in his monograph "Traicté des Chiffres ou Secrètes Manières d'Escrire" in 1586 [4]. This cipher was used by many countries for a long time (until the 1940s) [3].

In this paper, we propose the sequential cipher that is a generalization of the principles of the Vigenère cipher, has high resistance to breaking, and is conceptually closer to the Gilbert-Vernam cipher. The composition of the sequential cipher and the diagonal cipher proposed in [2] is sufficiently resistant to classical cryptanalysis methods.

Diagonalization algorithm

One of the encryption and description methods using the diagonalization algorithm is described in [2]. This cipher consists of independently encrypting the odd characters C^1=$\mathrm{c}_1\mathrm{c}_2 \ldots \mathrm{c}_k$, of the word C and the even characters C^2=$d_1 d_2 \ldots d_k$ of the word C by distinct permutations σ_1 and σ_2 which are defined on the symbols of the words C^1 i C^2, respectively. The key to such a cipher is an ordered pair of permutations (σ_1, σ_2). In [2] a more robust encryption method is also described. It consists of the following.

Remark 1. We observe that the procedure in [2] the random choice of the number c_i has a linear complexity. Also, the choice of the number d_i , calculating the double text C, the permutations σ_1 and σ_2, the transformation $\iota_{n_{2k}}$ of the word C have a linear complexity, as well. This implies that the complexity of the encryption of the diagonal cipher is linear. Similarly, the dual arguments to above imply that the complexity of the decryption of the diagonal cipher is linear, too.

Sequential cipher

We present the algorithm which generates a cipher, and it is like the Vernam cipher. This cipher is called a sequential cipher.

Remark 2. The complexity of encryption and decryption of the sequential cipher is linear.

Diagonal sequential cipher

The diagonal sequential cipher algorithm has two variants:

1. The plaintext M at first encrypted by the diagonal cipher with the key $(\sigma_1, \sigma_2, i_{n_{2n}})$ and then the resulting ciphertext is encrypted by the sequential public-key cipher X and by the secret key $Ss_1, s_2, \ldots, s_p$.

2. The plaintext M at first encrypted by the sequential public-key cipher X and by the secret key $Ss_1, s_2, \dots, s_p$ and then the resulting ciphertext is encrypted by the diagonal cipher.

Later, diagonal and sequential ciphers will be denoted by $\mathcal{D}$ і $\mathcal{S}$, respectively, and their compositions (sequential encryptions) by $\mathcal{DS}$ and $\mathcal{SD}$. Obviously that $\mathcal{DS}$ and $\mathcal{SD}$ also have linear encryption complexity. Similarly to the encryption, the complexity of decryption of compositions $\mathcal{DS}$ and $\mathcal{SD}$ is linear.

Since the diagonal cipher $\mathcal{D}$ has a probabilistic choice of the number c_i for the symbol m_i of the plaintext, then the methods of linear and differential cryptanalysis do not work in the case of the cipher $\mathcal{D}$, as well as the ciphers $\mathcal{DS}$ and $\mathcal{SD}$. Similarly, crypto attacks of the "known plaintext/chosen plaintext/chosen ciphertext" type do not provide an opportunity to break the encrypted text.

References

[1] Giovan Battista Bellaso, *La cifra del Sig. Giovan Battista Bel[l]aso, gentil'huomo bresciano, nuovamente da lui medesimo ridotta à grandissima brevità et perfettione*, Venetia, 1553.

[2] O.V. Gutik, O.B. Popadiuk, V.A. Vlasov. Symmetric algebraic cipher. Theoretical and Applied Cybersecurity. Proceedings of the Third All-Ukrainian Scientific and Practical Conference (TACS-2025). Kyiv, Politekhnika, 2025, P. 139-141.

[3] D. Kahn, The codebreakers: the story of secret communication from ancient times to the Internet, Scribner, New York, NY, 1996.
Blaise de Vigenère, *Traicté des Chiffres ou Secrètes Manières d'Escrire*, Paris, 1586.

SYMMETRIC CRYPTOGRAPHIC ALGORITHM IN A POLYNOMIAL HIERARCHICAL RESIDUE NUMBER SYSTEM

Ihor Yakymenko
West Ukrainian National University, 11 Lvivska Str. , 46009 Ternopil, Ukraine

Abstract
This research is dedicated to the development and analysis of a symmetric cryptographic algorithm based on the use of a polynomial hierarchical residue number system (HPRNS). The paper considers the theoretical foundations of constructing hierarchical systems of moduli that allow for a gradual reduction in the order of polynomials at each level of the hierarchy. The advantages of using this approach are analyzed, including the possibility of optimizing arithmetic operations, reducing computational costs, and increasing processing speed through parallel data processing. The processes of representing plaintext in polynomial form, the encryption procedure by obtaining residues at various levels, and the algorithm for recovering the original message in reverse order are described.

Keywords
Hierarchical residue number system, symmetric encryption algorithms, cryptographic data protection

Introduction

Solving modern information security problems is closely associated with improving the performance and cryptographic strength of symmetric encryption algorithms under conditions of increasing computational capabilities. Traditional information security systems based on integer arithmetic require increasing key lengths and operand sizes, which leads to reduced performance. Therefore, a promising direction is the use of polynomial arithmetic in combination with a hierarchical residue number system (HRNS). This approach makes it possible to optimize arithmetic operations and reduce the amount of required computations while maintaining a high level of data security.

Theoretical Foundations of the Hierarchical Polynomial Residue Number System

The hierarchical polynomial residue number system (HPRNS) is based on the mathematical principles of polynomials over finite fields [1, 2]. With the increasing volumes of information processing, transmission, and storage, it becomes necessary to increase both the number of polynomials and their orders. This leads to greater complexity of hardware and longer operation times. Therefore, optimization is required, and one of the approaches is HPRNS, which allows reducing the order of polynomials. For simplicity, we assume that the number of polynomials in each system at any level is the same and equals *l*.

Let the main system $p_1(\mathrm{x}), p_2(\mathrm{x}), \ldots, p_l(\mathrm{x})$ provide the ability to perform operations in the range $[0, P_1(\mathrm{x}))$, where $P_1(\mathrm{x}) = p_1(\mathrm{x})p_2(\mathrm{x})\ldots p_l(\mathrm{x}) = \prod_{i=1}^{l} p_i\,(\mathrm{x})$. The maximum computation range achievable in this system during multiplication is $(p_l(x)\text{-}1)^2$**.** Then, all residues of the main system can be represented in a new system with bases $q_{11}(x)$, $q_{12}(x)$, ..., $q_{1l}(x)$, $q_{21}(x)$, $q_{22}(x)$, ..., $q_{2l}(x)$, ..., $q_{l1}(x)$, $q_{l2}(x)$, ..., $q_{ll}(x)$with the corresponding ranges. Subsequently, the residues of the second level are represented, according to the respective requirements, in the system of moduli of the third level. This procedure continues up to the last (*k*-th) level. The number of levels is usually determined based on the required level of security for a specific task. This process of transitioning to polynomials of lower order significantly simplifies implementation. Moreover, HPRNS can have a large key space, which makes them resistant to brute-force attacks and allows parallel processing on multi-core or distributed systems, thereby increasing operational speed.

Theoretical Foundations of Symmetric Encryption in a Hierarchical Residue Number System

In symmetric encryption using a hierarchical residue number system (HRNS), at each of the k levels ($k \geq 1$ the number of which is agreed upon by both communicating parties, residues are computed with respect to the corresponding system of moduli and then passed to the next level. Each residue of the *r*-th level corresponds to l systems with l^{r-1} residues. Thus, l^r residues are transmitted to the r+1 level ($l > 1$, $r = 1, 2, \ldots, k-1$). Consequently, the ciphertext consists of l^k polynomials, which are the residues of the final level of the HRNS. The sets of moduli are known to both the sender and the receiver.

For encryption, alphabetic information is first represented in numerical form using ASCII codes. After that, it is expressed as a polynomial with coefficients corresponding to the alphabetic information, i.e., the plaintext $N(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 x^o$, where a_i is the sequence of numerical representations of characters,

$i = \overline{0 \dots n}$, n+1 is the message length. Then, the plaintext block $N(x)$ is represented in the polynomial residue number system according to expression:

$$N(x) = \left(\sum_{i=1}^{l} b_i(x)\, M_i(x) m_i(x)\right) mod\ P\ (x) \quad (1)$$

where $M_i(x) = \frac{P(x)}{p_i(x)}$, and $m_i(x)$ is determined according to the expression $m_i(x) = M_i(x)^{-1}\, mod\ p_i\ (x)$.

Thus, in the proposed polynomial hierarchical method, the ciphertext is a set of residues obtained by formula $b_i(x) = N(x) \bmod p_i(x)$. at the final level of each block. The recovery of the original message (polynomial) is performed in reverse order, starting from the k -th level down to the first level, based on the use of expressions:

$$N_1(x) = b_1(x);$$

$$N_2(x) = N_1(x) + \gamma_1(x) p_1(x) = b_1(x) + \gamma_1(x) p_1(x); N_2(x)\, mod\ p_2\ (x) \equiv b_2(x);$$

$$\dots\dots\dots\dots\dots\dots\dots\dots \quad (2)$$

$$N_i(x) = N_{i-1}(x) + \gamma_{i-1}(x) p_1(x) p_2(x) \dots p_{i-1}(x); N_i(x)\, mod\ p_i\ (x) \equiv b_i(x);$$

$$N_k(x) = N(x) = N_{k-1}(x) + \gamma_{k-1}(x) p_1(x) p_2(x) \dots p_{k-1}(x); N_k(x)\, mod\ p_k\ (x) \equiv r_k(x).$$

As a result of the computations at the k-th level, values are obtained that represent residues (polynomials) of the $k-1$-th level. At each level during the decryption process, the number of polynomial residues is reduced by a factor of l.

Conclusions

The developed cryptographic algorithm in the HPRNS features a hierarchical structure that provides a gradual reduction in the order of polynomial moduli at each level. This, in turn, reduces computational costs, enhances the efficiency of cryptographic operations, and allows adaptive tuning of the algorithm's parameters to ensure the required level of security.

References

[1] Tadeusz Tomczak. Hierarchical residue number systems with small moduli and simple converters. International Journal of Applied Mathematics and Computer Science. Vol. 21 (2011), ISSUE 1, March 2011, pp.173-192.

[2] Bajard J.-C., Marrez J., Plantard T., Véron P. On Polynomial Modular Number Systems over Z/pZ. Advances in Mathematics of Communications (in Press). 2022. DOI: 10.3934/amc.2022018

METHOD FOR PREDICTING FAILURES AND CYBER THREATS IN ON-BOARD EQUIPMENT IN THE CONTEXT OF DIGITAL TRANSFORMATION

Yuliia Kovalenko
State University of Information and Communication Technologies, Solomianska 7, 03110 Kyiv, Ukraine

Abstract

This paper presents an advanced artificial intelligence–based method for the predictive analysis of failures and cyber threats in the onboard equipment complex of Integrated Modular Avionics (IMA). The proposed approach addresses the growing challenges associated with the increasing complexity, interconnectivity, and digitalization of modern avionics systems. By integrating probabilistic reliability modeling, diagnostic data analytics, and intelligent cyber threat detection, the method enables the identification of latent interdependencies between hardware degradation, software malfunctions, and cyber-induced anomalies.

Keywords

artificial intelligence, predictive modeling, integrated modular avionics, cybersecurity, reliability, onboard systems.

The continuous evolution of aircraft systems toward highly integrated, software-intensive, and networked architectures necessitates a unified approach to reliability, fault tolerance, and cybersecurity. Integrated Modular Avionics (IMA) architectures have become the dominant paradigm in modern aircraft design due to their flexibility, scalability, and efficient utilization of computational resources. However, the high degree of interconnection and shared resources inherent in IMA systems introduces new classes of risks that cannot be adequately addressed by traditional diagnostic and reliability assessment methods.

Conventional approaches are predominantly focused on isolated hardware failures and deterministic fault scenarios, while contemporary avionics systems increasingly face hybrid failure modes arising from the interaction of technical malfunctions and cyber threats. These challenges are further amplified by the ongoing digital transformation of aviation, which expands the attack surface and increases system complexity [1-3].

Artificial intelligence (AI), particularly machine learning and expert-based reasoning, provides powerful tools for predictive maintenance, anomaly detection, and proactive risk mitigation. This research builds upon the author's doctoral work on information support for the design and operation of IMA onboard equipment and proposes an intelligent predictive method capable of detecting potential failures and cyber threats at early stages, before they lead to critical system degradation

The proposed method was validated using a comprehensive simulation environment developed in MATLAB/Simulink. Integrated AI modules were implemented with automatic code generation via the Embedded Coder framework and deployed under the XtratuM real-time operating system, compliant with ARINC 653 requirements. The experimental dataset included both nominal operation scenarios and a wide range of fault and cyberattack conditions affecting avionics network behavior.

Method	Fault Prediction Accuracy (%)	Cyber Threat Detection Accuracy (%)	Average Recovery Time (s)
Traditional reliability model	78,4	52,3	12,4
Neural anomaly detection only	88,6	83,1	9,2
Proposed AI-based method	95,2	91,8	6,7

Future research will focus on embedding the developed algorithms into real-time digital twins of avionics platforms, enabling continuous monitoring, adaptive certification support, and enhanced compliance with evolving aviation software standards.

References:

[1] Stanton I**.** 2023. Predictive maintenance analytics and implementation for aerospace systems: A systematic literature review. *Systems Engineering*, INCOSE Online Library. https://incose.onlinelibrary.wiley.com/doi/full/10.1002/sys.21651

[2] RTCA. 2011. *DO-178C: Software Considerations in Airborne Systems and Equipment Certification*. RTCA Inc., Washington, DC, USA.

[3] ARINC. 2015. *ARINC Specification 653-1: Avionics Application Software Standard Interface*. Aeronautical Radio, Inc., USA.

OPTIMIZATION OF SDN TOPOLOGY BASED ON COMBINED NETWORK PARAMETERS

Maksym Kuklinskyi[1], Viacheslav Treitiak[2], Tetiana Holyavkina[3], Mykyta Zhyzhkin[4] and Andrii Bondarenko[5]
[1,2,5] *State University of Information and Communication Technologies, Solomianska 7, 03110 Kyiv, Ukraine*
[3,4] *State University «Kyiv Aviation Institute», Liubomyra Huzara Avenue 1, 03058 Kyiv, Ukraine*

Abstract

Software-defined networks (SDNs) represent complex systems composed of a central controller, switching nodes, and communication channels that ensure interaction between all elements. The network's topological structure plays a decisive role in determining efficiency, reliability, and the effectiveness of traffic management. Optimizing this topology is therefore critical for the overall performance of SDNs. This study proposes two complementary methods for topology optimization: the random search approach and the structure tree method. The random search generates multiple candidate network structures and selects the most promising ones, while the structure tree method systematically improves these structures by iteratively removing or adjusting connections based on efficiency criteria. Key performance metrics, such as redundancy, structural unevenness, diameter, compactness, and centralization degree, are used to assess network efficiency. The comparison of results demonstrates that the structure tree method provides superior performance metrics but requires significant computational resources. Combining both methods using the random search to generate initial networks and the structure tree to refine them – offers a practical and effective approach to SDN design. This two-stage optimization can enhance network reliability, reduce operational costs, and improve overall traffic management, thereby contributing to more efficient and resilient software-defined networks.

Keywords

Software-defined network, topology optimization, network performance, traffic management, SDN design

Like most modern technologies, software-defined networks are subject to continuous enhancement and periodic updates. Due to the inherent complexity of these systems, the process of their improvement tends to be relatively lengthy. The primary objectives of such upgrades include enabling diverse types of information exchange, enhancing reliability, increasing data transmission speed, and ensuring stable operation of network components. At the same time, the topological structure remains a fundamental element across all types of networks.

Consequently, the task of optimally designing the architecture of a software-defined network remains highly relevant and attracts considerable research interest. Effective synthesis of network topology must account not only for the connectivity between nodes but also for factors such as network reliability, response times, and operational efficiency. Achieving an optimal structure allows the network to perform efficiently while maintaining resilience and cost-effectiveness.

The services offered by software-defined networks (SDNs) categorize them as part of data transmission systems [1]. Current research indicates that significant attention is being directed toward studying these systems, which is reflected in the abundance of publications on the topic.

This interest is largely due to the extensive range of challenges and applications that data transmission systems encompass across various industries. Numerous studies provide classifications and describe diverse methods and approaches to data transfer [2–3]. However, in most cases, these works either assume standard topologies without detailed explanation or omit topology descriptions altogether.

Additionally, some publications focus on the design of data transmission systems, yet they are often limited to specific industrial contexts, narrowing the scope of their findings because the analysis is tied to the characteristics of a single industry. Articles that specifically explore the optimization of data transmission systems are relatively rare [4], and this scarcity is even more pronounced in the context of software-defined networks [5].

Given this situation, the present article aims to introduce a method for optimizing the structure of SDNs and to evaluate its effectiveness in improving system performance. The goal is to provide a framework that not only supports the efficient formation of network topology but also enhances the reliability and operational efficiency of software-defined networks in diverse applications.

When synthesizing the structure of a software-defined network (SDN), efficiency is evaluated using indicators such as cost, reliability, response time, transmission delay, and network congestion. The SDN topology can be represented as a symmetric graph, where nodes correspond to network elements and edges represent communication links. Key topological indicators include structure redundancy (Rs), unevenness

(Ns), diameter (Ds), compactness (Bs), and degree of centralization (Cs), which collectively describe the reliability, performance, and economic feasibility of the network.

Redundancy and unevenness primarily affect fault tolerance and reliability: low redundancy leads to network fragmentation upon failures, while excessive redundancy increases cost and implementation complexity. Diameter and compactness characterize the average residence time of information in the network, with lower values indicating shorter transmission paths and higher performance. These indicators also reflect the survivability and stability of the SDN, as efficient topologies minimize delays and reduce the risk of network disintegration due to link failures.

The degree of centralization determines the network control model and significantly influences reliability, load distribution, and management complexity. Highly centralized structures depend critically on the central controller and are vulnerable to its failure, whereas decentralized structures require greater coordination overhead and behave similarly to peer-to-peer networks. Since the indicators have different dimensions and optimization goals, they are normalized into dimensionless, minimizable criteria and combined into an aggregated efficiency metric, which serves as the objective function in a nonlinear optimization framework.

Two algorithms are proposed to solve the optimization problem: random search optimization and the structure tree method [6–7]. In the random search approach, multiple connected network topologies are generated by randomly removing edges from a fully connected graph, and the best solution is selected based on a generalized optimization criterion. The process is controlled by parameters such as the minimum and maximum number of removable edges and the maximum number of iterations, which influence network connectivity and solution reliability.

Each iteration begins with the random selection of a number of edges to remove, while ensuring that the resulting network remains connected. For every generated topology, partial efficiency criteria are computed and combined using a nonlinear compromise scheme to form a generalized criterion. The obtained result is compared with the current best solution, which is updated if an improvement is found. Increasing the number of iterations enhances the accuracy and robustness of the optimization by expanding the set of evaluated network configurations.

The structure tree method performs optimization by iteratively selecting the best edge to remove based on the generalized criterion. Starting from a fully connected network, an optimization tree is constructed in which nodes represent network variants and edges correspond to edge removals. At each step, the most promising leaf node is expanded by evaluating all possible single-edge removals, and the process continues until stopping conditions are met. This method enables systematic exploration of the solution space and allows interruption at any stage while retaining the best result obtained so far.

The analysis of the considered optimization methods shows that the structure tree method provides the highest solution quality; however, it is characterized by significant computational complexity. At the same time, the use of a fully connected network as an initial solution is inefficient, since such a topology has an unfavorable value of the generalized optimality criterion and is far from the optimal configuration. In this context, the random search method is more suitable for generating initial network topologies that are closer to the optimal region of the solution space.

Based on this observation, a combined optimization approach is proposed, which integrates the advantages of both methods. At the first stage, an initial connected network is generated using the random search algorithm. At the second stage, this network is treated as the root of the optimization process and is further refined using the structure tree method, which iteratively improves the network characteristics by selective edge removal.

The application of the proposed two-stage optimization approach to software-defined networks enables a significant reduction in computational load on the central controller. This advantage is particularly important both at the network design stage and during subsequent optimization and adaptation processes, thereby increasing the overall efficiency and practicality of SDN topology synthesis.

References

[1] Kaljic E, Maric A, Njemcevic P, Hadzialic M. 2019. A survey on data plane flexibility and programmability in software-defined networking. IEEE Access 7:47804-47840

[2] Hamdan M, Hassan E, Abdelaziz A, Elhigazi A, Mohammed B, Khan S, Vasilakos AV, Marsono MN. 2021. A comprehensive survey of load balancing techniques in software-defined network. Journal of Network and Computer Applications 174(2019):102856

[3] Prabu, U., Geetha, V. (2023). Towards the Implementation of Traffic Engineering in SDN: A Practical Approach. In: Suma, V., Lorenz, P., Baig, Z. (eds) Inventive Systems and Control. Lecture Notes in Networks and Systems, vol 672. Springer, Singapore.

[4] U Tupakula, KK Karmakar, V Varadharajan, B Collins 2022 13th International Conference on Network of the Future (NoF), 2022

[5] Ayodele, B., Buttigieg, V. SDN as a defence mechanism: a comprehensive survey. Int. J. Inf. Secur. 23, 141–185 (2024).

[6] Voronin A.N. Multicriteria solutions: models and methods: monograph / A.N. Voronin, Y.K. Ziatdinov, M.V. Kuklinsky. - K.: NAU, 2011 .- 348 page.

[7] A. Voronin, M. Kuklinskyi, T. Holyavkina, I. Gyza, L. Kharlai (2019) Multi-Criteria Synthesis of the Software-Defined Network Structure: International Workshop on Conflict Management in Global Information Networks (CMiGIN 2019), Lviv, Ukraine, 29 November, 2019, 594-603.

HYBRID CLASSIFICATION-DRIVEN ARCHITECTURE FOR ROBUST CLEANSING OF HETEROGENEOUS IOT DATA

Dmytro Nishchemenko[1], Kateryna Nesterenko[1] and Viktoriia Zhebka[1]
[1] *State University of Information and Communication Technologies, Solomianska 7, 03110 Kyiv, Ukraine*

Abstract
This research addresses the challenge of reliability in Internet of Things (IoT) sensor data within smart home environments, where heterogeneous noise such as drift, outliers, and constant values often degrades data quality. Standard cleaning methods, being non-adaptive, create cybersecurity vulnerabilities, allowing false data injection attacks to go undetected. This paper proposes H-AD-CLEAN, a novel hybrid classification-gated architecture that utilizes parallel 1D-CNN streams for waveform analysis and discrete wavelet transform (DWT) for texture analysis. The system intelligently protects clean data while applying the Kalman Filter only to noisy segments. Experimental results demonstrate a 34.66% improvement in RMSE and a 21.1% improvement in MAE compared to the standard Kalman Filter, proving that a "classify-first" approach is significantly more efficient than blind filtering.

Keywords
Data cleaning, internet of things, noise classification, machine learning.

Introduction

Modern smart homes are complex IoT ecosystems generating continuous streams of sensor data essential for automated control and predictive analytics. The accuracy of this data is a critical requirement for infrastructure stability [2]. Data errors lead to automation failures and create vulnerabilities where distorted data can mask real cyber incidents or provoke false alarms [3, 4]. Traditional approaches like the Rolling Median or the standard Kalman Filter (KF) are non-adaptive, applying filtering to the entire stream without distinguishing between noise and valid data. This leads to "oversmoothing," which essentially adds error to high-quality data and makes the system vulnerable to False Data Injection Attacks. Therefore, the objective is to develop an adaptive framework that dynamically selects a cleaning strategy based on multi-class identification of noise types to ensure data integrity.

Theoretical foundations of adaptive IoT data cleaning

In the conditions of evolving cyber threats, traditional static filtering methods are insufficient. Existing research shows that while deep learning models offer high accuracy, they are often computationally intensive and act as "black boxes" [1]. The H-AD-CLEAN methodology departs from traditional "blind" filtering in favor of an adaptive, classification-gated approach. The main idea is to create a "smart dispatcher" that diagnoses the signal state before applying any cleaning operators.

H-AD-CLEAN: Hybrid Classification-Gated Architecture

The H-AD-CLEAN architecture is based on the concept of an intelligent adaptive gateway that dynamically manages data streams depending on their actual state and noise level. The system is based on a hybrid classifier that combines two parallel analysis methods to achieve maximum accuracy in anomaly recognition. The first stream uses one-dimensional convolutional neural networks (1D-CNN) for deep waveform analysis and detection of complex time dependencies in the signal, while the second stream uses the discrete wavelet transform (DWT) to decompose the signal and extract statistical features from the frequency coefficients, which allows identifying textural features of different types of noise.

The logic module, which acts as a cleaning manager, uses the labels received from the classifier to select the optimal processing strategy for each specific data segment. If a segment is classified as “clean,” the system applies a pass-through operator, which preserves the original integrity of the data and completely avoids the unwanted over-smoothing effect that typically occurs with traditional filters. In cases where drift, outliers, or constant values are detected, the system automatically routes the data to a Kalman filter for selective reconstruction. This approach not only provides higher accuracy compared to “blind” filtering, but also creates an additional layer of cybersecurity by preventing False Data Injection attacks from masquerading as natural signal distortions.

Experimental evaluation and comparative analysis were performed on the synthetic dataset "Contrast", which simulates temperature fluctuations with superimposed anomalies. The performance of the H-AD-CLEAN system was compared with standard baseline methods. The final comparison of cleaning efficiency is presented in Table 1.

Table 1. Final comparison of overall cleaning efficiency.

Method name	RMSE	MAE	RMSE Improv. (%)	MAE Improv. (%)
Noisy Signal	1.0758	0.4824	—	—
Moving Median	0.9679	0.6811	10.03%	−41.19%
Kalman Filter	0.7175	0.4126	33.31%	14.47%
H-AD-CLEAN	0.7029	0.3253	34.66%	32.57%

The results confirm that the hybrid approach outperformed the standard Kalman Filter by achieving lower typical error (MAE) through the protection of valid data segments.

Conclusions

The research demonstrates that while the Kalman Filter is effective for noise smoothing, its non-adaptive nature results in significant corruption of valid data. The proposed H-AD-CLEAN system, using a "classify-and-act" approach, provides a robust solution for maintaining data integrity in heterogeneous IoT systems. By preventing unnecessary processing of clean data, the system achieves higher accuracy and resistance to data manipulation, although future work is required to test its effectiveness on real-world, chaotic IoT data.

References

[1] An, N., Ding, Y., & Zhao, H. (2024). Statistical feature analysis and preprocessing assisted artificial neural network for cleaning multi-type concurrent anomalies in time series data. 2024 7th International Symposium on Autonomous Systems (ISAS), 1–5.

[2] Ding, X., Wang, H., Li, G., Li, H., Li, Y., & Liu, Y. (2022). IoT data cleaning techniques: A survey. Intelligent and Converged Networks, 3(4), 325–339.

[3] Kasaraneni, P. P., Kumar, Y. V. P., Moganti, G. L. K., & Kannan, R. (2022). Machine learning-based ensemble classifiers for anomaly handling in smart home energy consumption data. Sensors, 22(23), 9323.

[4] Liu, Y., Dillon, T. S., Yu, W., Rahayu, W., & Mostafa, F. (2020). Missing value imputation for industrial IoT sensor data with large gaps. IEEE Internet of Things Journal, 7(8), 6855–6867.

CYBERSECURITY AS A FUNDAMENTAL CONDITION FOR SMART GOVERNANCE: REGULATORY AND ORGANIZATIONAL DIMENSION

Alina Liubyma, Andrii Panibratov
Kyiv Applied College of Tourism and Hospitality, *Romana Mstyslavycha Kniazia*, *26*, *02192 Kyiv*, *Ukraine*

Abstract

The development of smart governance is inseparably linked to the digital transformation of public administration and the widespread use of information and communication technologies. However, it must be noted that increasing reliance of government services on digital platforms has a hidden issue – significant growth of cybersecurity risks. Considering that cybersecurity works as a strategic factor that enhances government efficiency, resilience, and public trust, these themes were given prime attention. The study emphasizes the necessity of a holistic cybersecurity framework as the foundation for effective smart governance in the context of digital transformation.

Keywords

Smart governance, e-government, public administration, cyber risk management.

Introduction

In the recent year rapid implementation and introduction of digital government services, smart governance models have greatly increased the reliance of public authorities on digital infrastructure, network services, and interconnected information systems. This increasing dependence creates exposure of the state institutions to a wide range of cyber threats, making cybersecurity a strategic concern rather than just a technical one. Presence of such issue leads to a simple conclusion: strong cybersecurity measures are essential to ensure the continuity and efficiency of e-government services, as well as to protect sensitive citizen data and safeguard national digital assets.

Theoretical foundations for cybersecurity in smart governance.

In the context of digital transformation of all spheres, traditional approaches to protecting smart governance services are insufficient. Cyber threats are not only becoming more frequent and diverse, they are changing the object of influence and are increasingly directed not only at technical infrastructure, but also at organizational processes and regulatory mechanisms. Effective cybersecurity requires a comprehensive approach that combines technical, organizational and managerial mechanisms.

A comprehensive analysis of these approaches allows us to assess their effectiveness, identify best practices and ensure the sustainability of digital public services [1].

Regulatory and organizational measures in smart cybersecurity management

The implementation of smart governance requires a clearly defined regulatory and organizational framework. There are several steps to this.

1) The regulatory framework includes national cybersecurity laws, industry regulations, international standards (ISO/IEC 27001, NIST) and widely recognized cybersecurity frameworks such as COBIT, CIS Controls and ITIL Security Management.

2) Organizational governance is split into several clearly defined division of functional responsibilities, defining roles for cybersecurity teams, establishing incident response procedures and regular monitoring of digital platforms [2].

3) Regular security audits, vulnerability assessments, penetration testing and prioritizing protective measures based on risks insure on all levels of responsibility.

4) Awareness raising is imperative for upgrading employee skills, promoting an overall security culture, ensuring better training practices.

Together, these measures will enable government agencies to proactively manage cyber risks, maintain business continuity and ensure the resilience of e-government platforms [3].

Practical significance for Ukraine

For Ukraine, the implementation of smart governance requires the adaptation of international approaches and cybersecurity standards to the national context. Such steps include:

- harmonization of national legislation with international cybersecurity standards;
- development of coordination mechanisms between state bodies;
- creation of conditions for intersectoral cooperation between state institutions, business and the public;
- increasing cyber literacy and qualifications of specialists in the field of cybersecurity.

These measures aim to ensure the resilience of digital public services, as well as to achieve other essential goals (protect citizens' data, and align Ukraine's smart governance initiatives with international best practices).

Conclusions

Smart government cannot function without solid cybersecurity. This analysis shows that e-government services depend on three pillars: reliable digital infrastructure, coherent legal frameworks, and clear organizational responsibilities. When any of these elements is weak, service delivery suffers and public confidence erodes. What works in practice is a layered approach, that, in its implementation, includes combining technical safeguards with sound policy and well-defined governance structures. This allows agencies to anticipate threats rather than simply react to them, and helps rebuild trust when incidents do occur. There is still much to explore. Future studies should examine how specific national contexts shape cybersecurity implementation, and whether emerging tools (particularly AI-driven threat detection and automated response systems) deliver on their promise in real government settings.

References

[1] Kumar, S., Garg, A., & Niranjan, M. (2025). Enhancing Government Efficiency Through Cybersecurity Hardening. Proceedings of the 26th Annual International Conference on Digital Government Research (DGO 2025). https://doi.org/10.59490/dgo.2025.1047

[2] Magnusson, L., Iqbal, S., Elm, P., et al. (2025). Information security governance in the public sector: investigations, approaches, measures, and trends. International Journal of Information Security. https://link.springer.com/article/10.1007/s10207-025-01097-x

[3] Viale Pereira, G., Temple, L., Wild, M., Janowski, T., Musiatowicz-Podbial, G., Estevez, E., Mezzomo Luciano, E., & Rodríguez Bolivar, M. P. (2025). Building Capacity for Smart Cities and Urban Resilience through Digital Transformation. Conference on Digital Government Research, 26. https://doi.org/10.59490/dgo.2025.1012

AN ANALYSIS OF ORGANIZATIONAL DETERMINANTS OF CORPORATE VULNERABILITY TO SOCIAL ENGINEERING ATTACKS

Svitlana Lehominova[1], Mykhailo Zaporozhchenko[2]
[1,2] *State University of Information and Communication Technologies, Solomianska 7, 03110 Kyiv, Ukraine*

Abstract

The paper presents a generalized analysis of organizational factors influencing the vulnerability of corporate environments to social engineering attacks. It is shown that organizational characteristics play a systemic role in shaping susceptibility to manipulation, even in technologically protected systems. Structural, procedural, and cultural-communicative factors are identified as key determinants of organizational resilience. The results substantiate the need for an integrated organizational approach to counteracting social engineering threats within ISMS.

Keywords

Cybersecurity, social engineering attacks, information security, risk management, corporate culture

Introduction

Social engineering attacks represent a persistent and highly effective class of threats to corporate information systems, primarily due to their reliance on organizational conditions and patterns of human interaction rather than on the exploitation of technical vulnerabilities. Empirical analyses of security incidents indicate that organizational structures, procedural maturity, internal communication mechanisms, and security culture significantly affect the level of susceptibility to such attacks. However, despite the increasing maturity of technical protection measures, the organizational dimension of information security remains insufficiently formalized and systematically addressed in both research and practical risk management approaches.

Therefore, the **objective** is to conduct an analytical assessment of the impact of organizational factors on the vulnerability of corporate environments to social engineering attacks and to determine their role in enhancing organizational resilience to such threats.

Theoretical foundations of research

The study is based on the analysis of recent scientific publications, international information security standards, and documented security incident reports. Existing research predominantly focuses on technical, cognitive, or behavioral aspects of social engineering, while organizational factors are rarely treated as independent variables. This gap necessitates a systematic examination of organizational determinants within a risk-oriented security framework.

Results

The analysis reveals that organizational factors exert a systemic influence throughout all stages of social engineering attacks, including initiation, detection, response, and recovery. Three interrelated groups of factors are identified: 1) Structural factors determine responsibility distribution, decision-making mechanisms, and coordination efficiency. Vulnerabilities arise when roles are unclear or coordination mechanisms are absent. 2) Procedural factors reflect the maturity and operational integration of security policies and training practices. Declarative or outdated procedures significantly reduce organizational resilience. 3) Cultural and communicative factors shape behavioral norms, trust levels, and readiness to report suspicious activities. An institutionalized security culture enhances collective threat identification [1].

The study demonstrates that isolated improvements within individual factor groups do not significantly reduce vulnerability. Effective protection is achieved only through the integrated reinforcement of all organizational components.

Conclusions

Organizational resilience depends on the coherence of management structures, the operational effectiveness of procedures, and the maturity of security culture. The integration of structural, procedural, and cultural-communicative elements into a unified organizational security system enables early threat detection, effective response, and adaptive recovery. The results provide a conceptual basis for improving organizational information security management practices aimed at mitigating social engineering risks.

References

[1] Albladi S., Weir G.R.S. Predicting individuals' vulnerability to social engineering in social networks. Cybersecurity. 2020. Vol. 3. 7. URL: https://doi.org/10.1186/s42400-020-00047-5

A HYBRID MACHINE LEARNING AND EXPLAINABLE AI FRAMEWORK FOR FALSE POSITIVE REDUCTION AND CONTEXTUAL INSIGHTS IN NETWORK INTRUSION DETECTION SYSTEMS

Sergii Gakhov[1], Yurii Korovaichenko[2]
[1,2] *State University of Information and Communication Technologies*

Abstract

Modern network infrastructures face evolving cyber threats such as unauthorized access, DoS/DDoS attacks and zero-day exploits, leading to 71% of organizations reporting an increase in cyberattack frequency over the past year, according to VikingCloud's 2025 cybersecurity statistics. Traditional signature-based Intrusion Detection Systems are ineffective against unknown threats, while machine learning models suffer from high false positive rates, overwhelming cybersecurity teams. This paper proposes a hybrid framework that combines the Random Forest algorithm for network traffic classification with SHAP-based Explainable Artificial Intelligence to provide contextual explanations and reduce false positives without losing accuracy. Comparison with literature models confirms the advantages of the hybrid in interpretability and organizational efficiency, contributing to faster verification of alerts.

Keywords

intrusion detection systems, random forest, explainable AI, CIC-IDS2017, machine learning

Introduction

Modern network infrastructures, from corporate networks to critical sectors, are vulnerable to complex cyber threats: unauthorized access, malware distribution, DoS/DDoS attacks, APT and zero-day exploits. According to VikingCloud's 2025 cybersecurity statistics, 71% of organizations reported an increase in cyberattack frequency over the past year. Traditional signature-based Intrusion Detection Systems are ineffective against unknown threats, while machine learning models suffer from high false positive rates, overwhelming cybersecurity teams.

A hybrid approach of machine learning and artificial intelligence is necessary because classic machine learning models do not provide transparency: without context (for example, why the model marks traffic as malicious), analysts waste time on manual verification, while integration with artificial intelligence allows generating comments and explanations, turning alerts into actionable insights.

Background and Evolution of Intrusion Detection Systems

The Random Forest algorithm is an ensemble machine learning method that consists of a set of decision trees. It aggregates the predictions of individual trees to improve the accuracy and robustness of the model. For regression problems, aggregation is performed by averaging the predictions of all trees, while for classification problems, majority voting is used.

The hybrid approach's benefits include reducing security team workload through interpretable insights. Traditional Random Forest models, resilient to noise, often produce excessive false positives in imbalanced datasets, where benign traffic dominates. XAI integration, particularly SHAP, dynamically assesses feature importance and discards erroneous alerts via thresholds, lowering false positive rate to 0.07% without affecting overall accuracy.

Proposed Hybrid Framework

The model is based on the RandomForestClassifier classifier from the scikit-learn library. The explanatory AI module is implemented to increase transparency and reduce false positives by contextually analyzing predictions. Figure 1 shows a comparison of the ML and ML+AI models. All bars are almost identical. This illustrates the lack of difference in metrics, but highlights the potential to reduce false positives in real noisy environments while adding context to events.

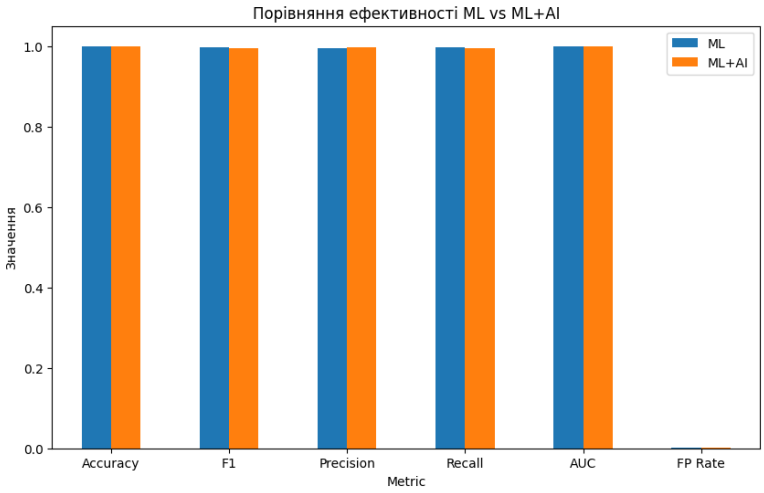

Fig. 1. Comparison of key performance metrics between pure ML and hybrid ML+AI models

A key element of this study is the context-rich nature of the triggers. During the simulation, XAI provided contextual explanations, such as:

- "Malicious prob 0.79: High SHAP from Destination Port - check Destination Port for anomaly (no IP/ timestamp available)";
- "Malicious prob 0.86: High SHAP from Packet Length Variance - check Packet Length Variance for anomaly (no IP/ timestamp available)";
- "Malicious prob 0.87: High SHAP from Fwd IAT Min - check Fwd IAT Min for anomaly (no IP/ timestamp available)".

Conclusions

A hybrid framework is proposed that combines the Random Forest algorithm with SHAP-based Explainable Artificial Intelligence demonstrates significant potential in improving the efficiency of Intrusion Detection Systems in modern network environments. The integration of XAI not only provides transparency of decisions through contextual explanations, but also helps reduce the burden on security teams by turning alerts into actionable insights and reducing the time to verify incidents. This makes the framework not just a technical solution, but a tool for stable human-AI interaction.

References

[1] Alabdulatif A. A. A Novel Ensemble of Deep Learning Approach for Cybersecurity Intrusion Detection with Explainable Artificial Intelligence. Applied Sciences, 2025. URL: https://www.researchgate.net/publication/394009970_A_Novel_Ensemble_of_Deep_Learning_Approach_for_Cybersecurity_Intrusion_Detection_with_Explainable_Artificial_Intelligence DOI: https://doi.org/10.3390/app15147984

[2] Xu Z., Liu Y. Robust Anomaly Detection in Network Traffic: Evaluating Machine Learning Models on CICIDS2017. arXiv preprint arXiv:2506.19877, 2025. URL: https://arxiv.org/abs/2506.19877.

[3] Ferrão T., Manene F., Ajibesin A. A. Multi-Attack Intrusion Detection System for Software-Defined Internet of Things Network. Computers, Materials & Continua, 2023. URL: https://www.researchgate.net/publication/370462346_Multi-Attack_Intrusion_Detection_System_for_Software-Defined_Internet_of_Things_Network

[4] Alyahya M., Lahza H., Mosli R. Toward Reducing IDS Misclassification Using Hybrid DL and ML Approach. Advances in Artificial Intelligence and Machine Learning, 2024. URL: https://www.oajaiml.com/uploads/archivepdf/811443161.pdf

ZERO-TRUST FOR SMBs IN CLOUD

Yuriy Pepa, Tetiana Nimchenko, Viktoria Korsunenko
State University of Information and Communication Technologies, Solomianska 7, Kyiv, Ukraine

Abstract
The paper presents a telecom-aligned Zero-Trust concept for small and medium-sized businesses (SMBs) operating in multi-cloud and 5G/FWA environments. The approach shifts focus from perimeter security to identity and access context, applies policies as code (policy-as-code), and employs ZTNA together with SASE/SD-WAN as enforcement points. The architectural foundations cover service microsegmentation, end-to-end mTLS with short-lived certificates, and telemetry from IdP/EDR/MDM, SD-WAN, and 5G to form a dynamic risk profile. It is explained how a single policy language ensures consistency across cloud, offices, and remote sites, reducing attack surface, accelerating incident containment, and simplifying access audits. Practical value for SMBs is outlined: gradual migration from VPN, alignment with telecom operators, and predictable costs through managed SASE bundles. Key challenges—asset and role inventory, legacy compatibility, and operational habit change—are highlighted along with mitigation approaches.

Keywords
Zero-Trust, policy-as-code, ZTNA, SASE, SD-WAN, 5G slicing, IAM/IdP, mTLS, microsegmentation, SIEM/SOAR, SMB.

Digitalization of small and medium-sized businesses (SMBs) is accompanied by growth in cloud services, distributed teams, and hybrid connectivity (public Internet, 5G/FWA, private links). Perimeter models increasingly mismatch this reality: staff work from diverse devices and locations, data reside across multiple clouds, and partner integrations open additional risk vectors. Against this backdrop, Zero-Trust is seen as a baseline paradigm: access is not granted "by default"; decisions are made based on identity, context, and current risk; and control targets specific services and data flows rather than the "network as a whole." Telecom infrastructure—primarily SASE/SD-WAN and 5G—creates natural touchpoints for implementing this approach. SASE unifies networking functions with security services in a single managed platform, while SD-WAN ensures consistent policy application across branch networks and remote sites. 5G adds traffic segmentation (slicing) and stable quality of service for mission-critical flows, including IoT/OT. The approach is identity-oriented: decisions are taken not by network addresses, but by who (person, application, microservice) is requesting access and under what context. Access is granted to a specific service rather than to the entire network—this is the essence of ZTNA. All traffic is encrypted using mTLS, short-lived certificates are employed, and session windows are constrained. Workloads are divided into isolated domains with least-privilege rules, reducing attack surface. Policies are expressed as human-readable code and pass linting, testing, signing, and controlled rollout with change audit. The decision process is supported by telemetry: signals from IdP, EDR/MDM, SD-WAN, and 5G, together with access logs and UEBA, form a current risk profile and influence permissions in real time.

A unified source of rights and attributes is provided by the IdP/IAM stack with multi-factor authentication. A policy controller reads declarative rules, evaluates context, and returns a verdict—permit, deny, or limited. At the network edge, the ZTNA/SASE layer with proxy and security gateways performs filtering, DLP, CASB, FWaaS, and device-posture checks. SD-WAN and 5G add transport reliability and quality of service for branches, mobile users, and IoT, while also supplying valuable telemetry for policies. Endpoint state is enforced via EDR/MDM (disk encryption, patching, antivirus, configurations), and PKI/CA handles issuance and rotation of short-lived certificates. Events are collected in SIEM/UEBA, while SOAR enables fast responses—session isolation, privilege reduction, or token revocation. A user authenticates through the IdP with MFA; the system then checks device posture and other contextual attributes. If policies are satisfied, a short-lived authorization is issued for the precise service required, and an encrypted connection is established via ZTNA/SASE. Continuous monitoring follows; upon suspicious signals—e.g., a sudden geolocation shift or posture change—rights are automatically narrowed to read-only, or the session is isolated without manual administrator intervention.

The model provides a single way to manage access across hybrid environments: regardless of whether a service resides in the cloud or on-premises, the same rules apply, easing the burden on small support teams. Access is tied to specific applications, reducing excessive privileges and complicating lateral movement for an attacker. Policies are stored as code with versioning and audit, making it easy to justify why a particular user has certain access and to quickly revert to a previous state when needed. Automated anomaly responses

shorten the time from event detection to containment, and integration with SASE/SD-WAN and 5G ensures policies are enforced consistently at network boundaries. Migration can be gradual: start with critical services and gently replace broad VPN tunnels with granular connections. As a result, the number of disparate products decreases, administration is simplified, and costs stabilize thanks to managed operator bundles. The approach requires a mindset shift: teams accustomed to "network rights" move to a "service rights" model, which demands training and time. A high-quality inventory of services, data, and roles is a prerequisite; otherwise, least-privilege remains aspirational. Some legacy systems may interact poorly with proxies or mTLS, necessitating workarounds and staged activation. Decision accuracy depends on posture and UEBA signal quality; "grace" modes, time-bound exceptions, and progressive tightening help mitigate false positives. It is also important to control "shadow" services via CASB and DLP and to coordinate security, networking, development, and operations, since policies affect code, infrastructure, and user experience alike.

Market conditions favor adoption: cloud is now standard, remote work is commonplace, and 5G provides mass reliable data transport. The industry offers mature services around ZTNA, CASB, and FWaaS, lowering the barrier to entry for SMBs. Policies as code naturally fit DevOps/DevSecOps processes, enabling swift, controlled changes without manual configuration errors. Most importantly, the model manages risk rather than perimeter: decisions account for access context, better matching today's threat dynamics and distributed teams. In finance units, for example, an analyst works with ERP only via ZTNA, and data export is blocked if the device fails encryption policies. In engineering teams, a developer sees only required repositories; when logging in from an unverified device, rights are automatically reduced to read-only. For warehouse and IoT systems, telemetry can flow through a dedicated 5G slice with its own access rules, and control panels open only from attested gateways within short sessions. Partners and contractors receive narrow, time-bound access to specific SaaS resources with geofencing, and rights are revoked automatically after work completion.

3. Conclusion

The method demonstrates that combining Zero-Trust with policy-as-code and the telecom pillars of SASE/SD-WAN and 5G yields a coherent, manageable, and scalable access model for SMBs in hybrid environments. Shifting emphasis from network perimeters to identity and context—reinforced by service microsegmentation, end-to-end encryption, and automated policy enforcement—reduces attack surface, accelerates incident containment, and enables transparent access auditing. Consistency of rules at network edges and in the cloud simplifies operations, while operator SASE bundles make expenditures more predictable for resource-constrained organizations. At the same time, sustainable results depend on disciplined asset and role inventory, signal quality for risk assessment, and gradual user adoption of the new model. Diligent work on legacy compatibility, control of "shadow" services, and coordination across security, networking, and development are required. With these prerequisites, the concept offers a timely response to the challenges of digitalization: it gives SMBs a practical path to improved cyber-resilience and aligns security policy with real telecom processes and cloud practice.

References:

[1] Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. Gaithersburg, MD: NIST, 2020. 59 p. DOI: 10.6028/NIST.SP.800-207.
[2] 3GPP TS 23.501. System Architecture for the 5G System (5GS). Valbonne: 3GPP, 2018–2025.
[3] 3GPP TS 23.502. Procedures for the 5G System (5GS). Valbonne: 3GPP, 2018–2025.
[4] 3GPP TS 33.501. Security Architecture and Procedures for 5G System. Valbonne: 3GPP, 2018–2025.
[5] ETSI GR NFV-EVE. Network Functions Virtualisation (NFV): Evolution and Ecosystem. Sophia Antipolis: ETSI, 2019–2024.

AUTOMATED ASSESSMENT OF PERSONAL DATA LOSS CONSEQUENCES IN COMPLIANCE WITH GDPR

Iryna Lozova[1], Mykhailo Rizak[2] and Oleksandr Kotyk[3]
[1,2] *State University of Information and Communication Technologies, Solomianska 7, 03110 Kyiv, Ukraine*
[3] *State University "Kyiv Aviation Institute", Liubomyra Huzara Avenue 1, 03058 Kyiv, Ukraine*

Abstract

This paper presents a software system designed to assess the negative consequences of personal data loss in compliance with the General Data Protection Regulation (GDPR). The proposed solution integrates legal, algorithmic, and analytical components to enable automated evaluation of data breach incidents, calculation of potential financial penalties, and generation of mitigation recommendations.

The system is based on a formalized structural and algorithmic model that supports risk assessment under varying incident conditions. Implementation using C# and the .NET Framework ensures scalability, efficient data processing, and automated report generation. The system can be applied as a decision-support tool for data protection officers and cybersecurity professionals to improve compliance and risk management.

Keywords

GDPR; personal data protection; data breach; risk assessment; decision support system; algorithmic modeling; C#.

The rapid digitalization of society has led to a significant increase in the volume of personal data processed by organizations, accompanied by growing risks of unauthorized access, data loss, and breaches. Ensuring compliance with the General Data Protection Regulation (GDPR) has therefore become a critical challenge, requiring not only formal privacy policies but also effective risk assessment mechanisms. Traditional qualitative approaches are often insufficient for accurately evaluating the consequences of data breaches under complex legal, technical, and organizational conditions [1]. Consequently, there is a need for an automated and GDPR-compliant system capable of assessing incident severity, estimating potential financial losses, and supporting informed decision-making in the field of personal data protection.

The proposed system is based on a previously developed formal GDPR model of personal data parameters [2] and a method for assessing the consequences of confidentiality breaches [3]. A structural model of the system was created, consisting of the following main modules [4]: data formation and storage; violation identification and classification; expert data input; expert data processing and evaluation.

The system allows experts to enter information related to incident characteristics, risk levels, data sensitivity, and organizational response measures. These inputs are processed using weighted coefficients that reflect the relative importance of each parameter. This approach enables the formalized calculation of the most probable financial loss resulting from a data breach.

Algorithmic support plays a key role in transforming the structural model into an operational solution. The developed algorithms implement the logical sequence of actions required for processing data breach incidents in compliance with GDPR requirements. The main stages of system operation include: incident identification (entering information about the organization, incident type, and scope of impact); violation severity determination (automatic classification of the breach based on violated GDPR articles); financial impact assessment (calculation of potential fines and losses through a set of evaluation subprocesses); report generation (creation of a final assessment with recommendations for risk mitigation and compliance improvement).

An integrated database of incident parameters and evaluation indicators supports data collection, processing, storage, and reuse. The database structure follows a hierarchical GDPR-oriented model, enabling efficient expert analysis.

The software system was implemented using the C# programming language within the .NET Framework environment. This platform provides stable operation with large datasets, supports automated generation of reports in DOCX and PDF formats, and enables the development of an intuitive user interface. The modular design ensures scalability and ease of integration into existing information security infrastructures [5].

The system includes modules for enterprise identification, selection of violated GDPR articles, multi-stage fine assessment, and automated report generation with analytical results and recommendations.

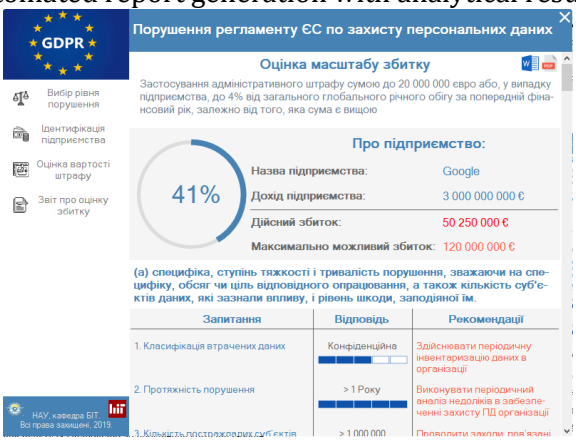

Fig. 1. Generated Report with the Predicted Impact on the Company

System verification was conducted using five case studies with varying initial parameters. The results demonstrated high sensitivity to changes in data confidentiality levels, retention periods, and organizational response measures. Incidents involving sensitive personal data and extended retention periods resulted in significantly higher estimated financial penalties.

The analysis showed that final loss values depend not only on quantitative factors, such as incident duration and data volume, but also on qualitative factors, including the presence of an incident response plan, notification of supervisory authorities, and the organization's reaction to the breach. The system also accounts for internal threats, which increase the overall risk coefficient.

These results confirm the system's ability to integrate legal, technical, and organizational factors in accordance with GDPR provisions.

This study presents a software system for assessing the negative consequences of personal data loss in compliance with GDPR. The proposed solution integrates algorithmic, legal, and analytical components into a unified framework for automated incident evaluation.

The system formalizes the assessment process, supports quantitative financial estimation, and generates practical recommendations for risk mitigation. Implementation in C# / .NET Framework ensures reliability, scalability, and usability. The system can be effectively used as a decision-support tool for information security and data protection professionals.

Future work will focus on integrating machine learning techniques for predictive analysis and developing a cloud-based version of the system to expand its applicability.

References

[1] Лозова І.Л., Різак М.В., Хохлачова Ю.Є., Котик О.В. Аналіз моделей, методів та систем оцінювання втрат від витоку персональних даних. Сучасний захист інформації. 2025. № 3 (63). С. 99-107. DOI: 10.31673/2409-7292.2025.031228

[2] Корченко О., Дрейс Ю., Лозова І., Педченко Є. Теоретико-множинна GDPR-модель параметрів персональних даних. Захист інформації. 2020. Т. 22, № 2. С. 120-141. URL: https://doi.org/10.18372/2410-7840.22.14871

[3] Шульга В.П., Корченко О.Г., Заріцький О.В., Лозова І.Л., Педченко Є.М. Метод оцінювання негативних наслідків від порушення конфіденційності персональних даних. Захист інформації. 2023. Т. 25, № 4. С. 254-268. URL: https://doi.org/10.18372/2410-7840.25.18232.

[4] Корченко О.Г., Лозова І.Л. Структурна модель системи оцінки негативних наслідків втрати персональних даних. Наукові записки ДУІКТ. 2024. №2 (6). С.165-170. URL: https://doi.org/10.31673/2786-8362.2024.028264

[5] Комп'ютерна програма «Програмний модуль оцінки негативних наслідків від витоку персональних даних»: а. с. 96927 Україна/ Ю. Дрейс., І. Лозова, Є. Педченко. Заявл. 27.03.2020; опубл. 29.05.2020, Бюл. № 58. URL: https://sis.nipo.gov.ua/uk/search/detail/1625864/.

THE CONCEPT OF THE PRINCIPLES OF INFORMATION WARFARE IN THE CONTEXT OF HYBRID AGGRESSION AGAINST UKRAINE

Svitlana Lehominova [1], Tetiana Kapeliushna [2], Tetiana Muzhanova [3]
[1,2,3] *State University of Information and Communication Technologies, Solomianska 7, 03110 Kyiv, Ukraine*

Abstract

The development of a digitalized and information society significantly reformats the nature of conflicts on a global scale, leading to the emergence of new forms of confrontation, in particular hybrid wars and latent information warfare. The large-scale implementation of digital technologies, global communication networks and data exchange platforms promotes the active use of information as a strategic resource, a tool of influence and management, which are used to adjust political, economic and social processes. The latent nature of information warfare in the digital environment complicates its timely detection and counteraction, which requires a scientific understanding of the role of information and cybersecurity as domains of hybrid confrontation, as well as the formation of the concept of the principles of information warfare in the context of hybrid aggression against Ukraine.

Keywords

hybrid warfare, information warfare, information theories, concept of information security

Introduction

Cyberspace has become one of the domains of confrontation, where cyberattacks are carried out against critical information infrastructure, state registers, financial systems, and energy facilities in order to destabilize governance processes and create an effect of uncertainty. At the same time, instruments of latent information warfare are actively employed, including disinformation campaigns, information and psychological operations, fake accounts, bot farms, and targeted influence technologies that enable covert pressure without direct military intervention.

The informatization of society and rapid digitalization have caused hybrid warfare and latent information warfare to acquire a systemic character, combining military, political, economic, informational, and cyber instruments of influence. A revision of approaches to information counteraction under conditions of hybrid warfare is inevitable, as traditional warfare is aimed primarily at the physical destruction of the adversary, whereas hybrid warfare (including the information domain) is focused on achieving cognitive capitulation. The primary objective of such warfare is the manipulation of the logosphere – the totality of social meanings through which individuals interpret reality – as a lever of influence on human consciousness.

The development of a new approach to information counteraction in hybrid warfare should be grounded in a semantic approach that considers information through the prism of quality, significance, and its ability to reduce entropy (uncertainty) in public discourse, as well as in information security theory, where information is classified as a weapon capable of ideological diversion and semantic manipulation [1; 2].

In this context, the study of the Ukrainian experience becomes particularly relevant, as information attacks are superimposed on prolonged psycho-emotional stress within society. A decade-long period of continuous traumatization – from territorial occupation to full-scale aggression and the challenges of the COVID-19 pandemic – has created conditions for reduced cognitive resilience. This makes the population more vulnerable to technologically sophisticated manipulations amplified by artificial intelligence algorithms .

At present, information warfare operates at the intersection of mathematical modeling, psychological destabilization, and technological expansion, generating new challenges not only for Ukraine but also for the global security order. The effectiveness of the aggressor's information attacks is largely обусловлена the specific condition of Ukrainian society, which has been living under prolonged and continuous stress for more than ten years. Assessing societal sensitivity to influence is based on an analysis of the causes of cognitive distortions resulting from long-term, multi-level neurotization. The chronology of stress factors includes the occupation of part of the territory in 2014, the COVID-19 pandemic, and the full-scale invasion in 2022. The combination of these events has produced a cumulative effect of psycho-emotional exhaustion. Persistent traumatization associated with wartime losses, destruction, and uncertainty about the future has led to increased emotional non-resilience and a decline in critical thinking abilities. As a result, society becomes more vulnerable to disinformation attacks, prone to wishful thinking or total pessimism, which increases overall informational vulnerability and amplifies negative content.

The use of artificial intelligence further destabilizes information security by combining three types of models: mathematical models that allow precise identification of the informational value of messages for specific audiences; logical models used to construct formally correct but substantively false conclusions; and

cognitive models aimed at directly distorting human perception of reality. Such technological convergence enables the creation of realistic deepfakes and automated bot networks that scale disinformation exponentially [3; 4].

At the same time, information warfare is not confined to Ukraine's borders; at the global level, its strategic objective is to erode international support through:

– economic blackmail, implemented via narratives about "Ukraine's responsibility for global increases in energy and grain prices," which stimulate protest sentiments in EU countries and exert pressure on governments to reduce assistance;

– discrediting aid by spreading fakes about the "resale of Western weapons on the black market," often using AI-generated videos, deliberately causing delays in arms supplies due to verification requirements and provoking political debates in partner countries. Humanitarian inversion is also employed (for example, accusing the Armed Forces of Ukraine of "killing civilians in Bucha" and labeling the tragedy as a "staged event"), aimed at creating "gray zones" in the perception of truth, undermining trust in facts, and eroding the ability to distinguish truth from fabrication.

Based on the research conducted, a scheme was formed that reflects the concept of the principles of information warfare, taking into account the cognitive impact and technological challenges of hybrid aggression.

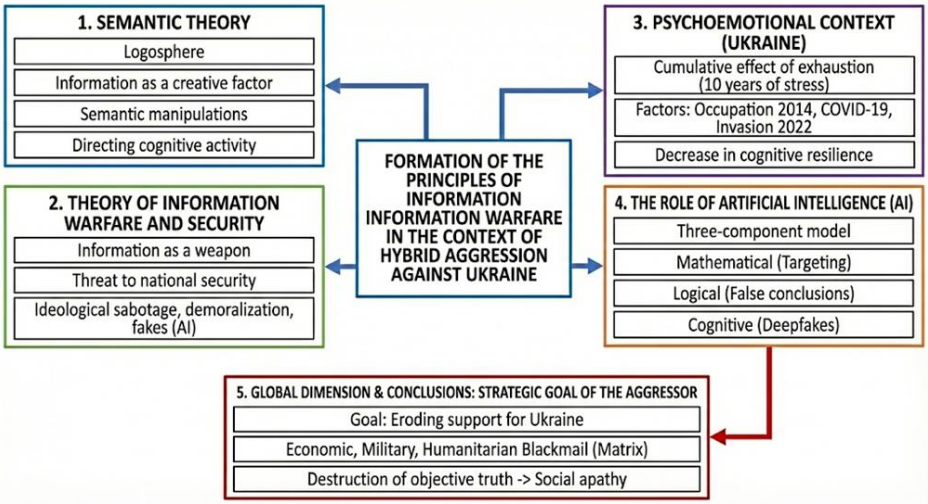

Figure 1: The concept of the principles of information warfare: cognitive impact and technological challenges of hybrid aggression

The proposed conceptual framework of information warfare principles will serve as a tool for the theoretical understanding and practical overcoming of mass social apathy and war fatigue, which pose a threat of declining support for Ukraine. Adherence to the principles formulated above makes it possible to transform society from a passive object of influence into an active subject of resistance, capable of effectively and sustainably countering cognitive distortions under conditions of hybrid warfare and disinformation.

References

[1] Etymological-semantic dictionary of the Ukrainian language. (1988) Volyn Research Institute, part 39. bihhiner Canada. URL: https://diasporiana.org.ua/wp-content/uploads/books/1095/file.pdfKurban O.

[2] Theory of information warfare: basic framework, methodology and conceptual apparatus. ScienceRise, (2015). URL: https://11. 95. 10.15587/2313-8416.2015.53940

[3] Długosz, Piotr. (2025). The Impact of the Russo-Ukrainian War on Mental Health and Stress-Coping Strategies in Central and Eastern Europe. 10.13140/RG.2.2.13830.84801.

[4] Yasenok, Viktoriia and Baumer, Andreas and Petrashenko, Viktoriia and Kaufmann, Marco and Frei, Anja and Rüegger, Seraina and Ballouz, Tala and Loboda, Andrii and Smiianov, Vladyslav and Seifritz, Erich and Bachmaha, Mariya and Suvalo, Orest and Kriemler, Susi and von Wyl, Viktor and Kostenko,

MODEL FOR ASSESSING THE SECURITY FOR PERSONAL DATA IN EVENT REGISTRATION DATABASES

Anna Vaskovska[1], Maksym Marchenko[1], Yevheniia Ivanchenko[1] and Ihor Ivanchenko[1]
[1] *State University of Information and Communication Technologies, Solomianska 7, 03110 Kyiv, Ukraine*

Abstract

The article considers the issue of personal data protection in event registration databases. The main cyber threats inherent in such systems are analyzed, as well as key methods and technologies for their neutralization in accordance with the international standards NIST, GDPR and ISO/IEC 27001. Examples of practical application of modern approaches to ensuring security in registration systems used during mass sports events are given. A model for assessing the level of personal data security in event registration databases is proposed, which includes five key components: authentication, availability, content, protection and deletion of data. A five-point scale is used for each component, which allows calculating the integral system security indicator. This approach provides an objective measurement of the level of security, identification of weaknesses and prioritization of measures to eliminate them.

Keywords

information protection, cyber protection, critical information resources, cybersecurity, GDPR, NIST, ISO/IEC 27001, registration base, database, information security

In the modern digital environment, personal data has become a highly valuable asset, making its protection a key priority for both public and private sectors. Mass sporting events, which gather tens of thousands of participants each year, require the processing of large volumes of sensitive information, including identification details, medical data, and payment information. As a result, registration databases (RDs) for sports events have become attractive targets for cybercriminals.

Effective protection of RDs requires a comprehensive approach that combines technical and organizational measures, security policies, and continuous monitoring. International standards such as OWASP Top 10, NIST SP 800-53, and GDPR emphasize the need for multi-layered security, including TLS encryption, multi-factor authentication, role-based access control, web application firewalls, intrusion detection and prevention systems, and centralized incident monitoring.

This issue is especially critical in countries facing heightened cyber threats or wartime conditions, such as Ukraine, where large sporting events are held amid ongoing information warfare. Despite this, many registration systems still rely on basic security measures, which are insufficient against modern threats. The lack of regular security assessments allows vulnerabilities to persist and weakens incident response. Therefore, developing a model to assess the security level of personal data in sports event registration databases is essential to identify weaknesses, provide mitigation recommendations, and enhance cyber protection in line with international best practices.

Modern sports event registration systems handle large volumes of sensitive data and therefore require strong security measures. A fundamental requirement is protecting data during transmission using HTTPS with modern versions of TLS, which ensures confidentiality and integrity and prevents interception of personal, medical, and payment information. Another key element is multi-factor authentication (MFA), which greatly reduces the risk of account compromise. While simplified authentication may be acceptable for regular participants, MFA is essential for administrative and other high-privilege accounts. Effective access control, particularly through role-based access control (RBAC), further limits unauthorized actions by granting users only the permissions necessary for their roles.

Equally important is continuous monitoring and detection of security threats. Tools such as SIEM, IDS/IPS, and detailed audit logs enable real-time detection of attacks and rapid incident response. However, as digital infrastructures expand, attack surfaces grow, and common threats—identified in OWASP Top 10—include injection attacks, weak authentication, data leaks, and insufficient monitoring. Many event organizers struggle with limited resources, lack of unified security policies, and human factors, making ad hoc protection insufficient. These challenges highlight the need for a structured security assessment model that objectively evaluates protection levels, identifies vulnerabilities, and supports effective security improvements without excessive costs.

The developed model for assessing the security of the sports event registration database is based on five key components: authentication (A), availability (B), content (C), protection (K), data deletion (M). Each of these elements covers critically important aspects of cybersecurity that determine the level of protection of

personal data throughout the entire information life cycle. A five-point scale is used for assessment, where 5 is a high level of protection, 0 is no measures. The integrated security level indicator (RDSL) is calculated as the arithmetic average of the scores of the five components:

$$RDSL = \frac{A + B + C + K + M}{5}$$

The model involves the following stages: system identification, information collection, criteria verification, scoring, and report generation. The advantages of the model are objectivity, versatility, ease of implementation, compliance with international security standards, and practical benefits for organizations working with large amounts of personal data. First, to assess the security of the RD, it is necessary to enter the parameters, where: parameter A is authentication in the RD; parameter B is accessibility in the RD; parameter C is content in the RD; parameter K is ensuring RD protection; parameter M is deleting data from the RD. It is also necessary to introduce a rating system for each of the points of each parameter. In this case, I will use a five-point rating system, where: 5 - yes, the system is protected; 0 - no, there is no protection. Each parameter will be the arithmetic average of the ratings of all its sub-points, that is, the overall security rating will be equal to the arithmetic average of all parameters and is also derived using a 5-point system. Each parameter includes an analysis of the following elements:

Table 1. Detailed value of each parameter

Parameter	Item	Question
A	A_1	Is there a login and password?
	A_2	Is there multi-factor authentication for all users?
	A_3	Is there two-factor authentication for RD administrators?
	A_4	Does the user have the ability to change their password at any time?
	A_5	Do users have the ability to change their data in their personal account?
	A_6	Do users have the ability to delete all their data from the RD?
B	B_1	Are administrators required to update their passwords at a certain frequency, or is such functionality not provided?
	B_2	Who has access to the administrative part of the RD?
	B_3	Is there access for a regular user in the RD admin?
	B_4	Who provides administrative access to the RD?
	B_5	Are there different levels of access to the RD?
C	C_1	Is access granted for permanent use or for a certain period?
	C_2	Who enters the personal data of participants?
	C_3	Who sets the data parameters from users?
	C_4	Does the administrator have access to edit the data entered by the user?
	C_5	How is the RD tested?
K	K_1	Are the users asked for consent to the processing of the personal data they entered?
	K_2	Is open-source testing performed for vulnerabilities?
	K3	Does the registry have its own interface?
	K_4	Is the website protected?
	K_5	Does the website have a built-in access control system?
M	M_1	Is it possible to access the administrative part of the RD from the public Internet?
	M_2	Is it possible to restore deleted data?
	M_3	Can all RD administrators delete data?
	M_4	Is the history of changes to information in the RD visible?
	M_5	Who provides access to delete data?

The article considered the problem of cyber protection of personal data in sports event registration databases. The main threat vectors and modern technical and organizational solutions for their minimization were analyzed. The proposed security level assessment model allows for a systematic and objective assessment of the state of cyber protection, identification of weaknesses and formation of

priorities for improvement. The practical value of the model lies in its versatility, ease of application and compliance with international standards GDPR, NIST, ISO/IEC 27001. It can be adapted for different types of registration systems or mass ticket sales services for concerts, festivals or other events. Prospects for further research include audit automation, integration with SIEM and IDS/IPS systems, comparative analysis of different platforms and development of tools for monitoring the dynamics of the security level. Thus, the proposed approach can become a practical tool for sports event organizers, IT teams and cybersecurity specialists.

References

[1] Guide to Protecting Personally Identifiable Information (PII) // NIST. - URL: https://csrc.nist.gov/pubs/itlb/2010/04/guide-to-protecting-personally-identifiable-inform/final
[2] Security and Privacy Controls for Information Systems and Organizations // NIST SP 800-53 Revision 5 Update 1. - URL: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
[3] ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи забезпечення безпеки. Системи управління інформаційною безпекою. Вимоги. — Київ: Держстандарт України, 2015.
[4] Council of Europe Convention on Access to Official Documents, Tromso, 2009 / / CETS № 205.
[5] VeriSign, Inc. Vulnerability Management: Best Practices for Secure IT Systems / VeriSign. — Mountain View: VeriSign, 2019.

OPTIMIZING IDS FUNCTION PLACEMENT IN MULTI-LAYER EDGE–FOG–CLOUD IOT ARCHITECTURE: A MILP-BASED APPROACH

Daniel Pastushchak[1], Andrii Mishchenko[1]

[1] *State University "Kyiv Aviation Institute", Liubomyra Huzara Avenue 1, 03058 Kyiv, Ukraine*

Abstract

This paper presents a mixed-integer linear programming (MILP) model for optimizing intrusion detection system (IDS) function placement across Edge–Fog–Cloud layers in IoT networks. The model minimizes processing latency while respecting computational capacity, memory, bandwidth, and privacy constraints (ε). Hypothetical evaluation shows 20–40% latency reduction with $\varepsilon \leq 0.1$ and less than 2% accuracy degradation compared to traditional deployments.

Keywords

IoT security, intrusion detection, Edge–Fog–Cloud architecture, MILP optimization, differential privacy1

Traditional cloud-centric IDS architectures introduce significant latency, bandwidth consumption, and privacy risks for IoT networks. Multi-layer Edge–Fog–Cloud architectures enable distributed processing, but optimal function placement remains an open challenge. This work formulates IDS placement as a MILP optimization problem, balancing latency minimization with resource and privacy constraints.

The objective function minimizes total latency:

$\min \Sigma(k,\ell)\, a_{k,\ell}\, \lambda_k\, p_{k,\ell} + \Sigma(k,\ell\neq\ell')\, y_{k,\ell,\ell'}\, \lambda_{k+1}\, d_{\ell,\ell'}$

where $a_{k,\ell} \in \{0,1\}$ indicates whether function k executes at layer ℓ, $y_{k,\ell,\ell'}$ tracks data transfers, λ_k represents traffic intensity, $p_{k,\ell}$ is processing time, and $d_{\ell,\ell'}$ denotes network delay.

Key constraints include: CPU capacity ($\Sigma CPU_{k,\ell} \leq C_\ell$), memory limits ($\Sigma Mem_{k,\ell} \leq M_\ell$), privacy budget ($\Sigma\varepsilon_{k,\ell} \leq \varepsilon_{max}$), detection accuracy ($\Sigma err_{k,\ell} \leq Err_{max}$), and bandwidth ($\Sigma\lambda_{k+1} \leq BW_{\ell,\ell'}$).

The privacy parameter ε (differential privacy) quantifies information leakage: $\varepsilon \approx 0$ at Edge (local processing), $\varepsilon \approx 0.1$ at Fog (partial aggregation), $\varepsilon \approx 0.3$ at Cloud (centralized analysis).

Typical parameter values based on recent literature: Edge (5 ms delay, ε=0.0, CPU=100), Fog (20 ms, ε=0.1, CPU=300), Cloud (80 ms, ε=0.3, CPU=1000). The model was implemented using PuLP/Gurobi with hypothetical data.

Four deployment scenarios were compared:

Table 1. Comparison of IDS deployment scenarios.

Scenario	Avg. Latency (ms)	ε	Latency Reduction
Cloud-only	110	0.30	---
Edge-only	45	0.00	-59%
Fog-centric	38	0.12	-65%
MILP-optimized	32	≤ 0.10	-70%

The MILP-optimized configuration achieves 70% latency reduction while maintaining privacy budget $\varepsilon \leq 0.1$ and accuracy loss below 2%.

This MILP formulation enables quantitative optimization of IDS placement in Edge–Fog–Cloud architectures. Hypothetical evaluation indicates substantial latency improvements (20–40%) while satisfying privacy and resource constraints. Future work includes integration with streaming frameworks (Flink/Spark), scalability assessment, and experimental validation using Edge-IIoTset 2023, CICIoT 2023, and Bot-IoT 2020 datasets.

References

[1] Z. Hong et al., "Privacy-Preserving Task Offloading for Satellite–Terrestrial Edge Networks via Differentially Private Federated Learning," Computer Networks, 2025.

[2] A. Alwakeel, "Enhancing IoT Performance through NDN and Edge Computing Integration," Computer Networks, vol. 264, 2025.

[3] Z. Wang et al., "Joint Resource Allocation and Privacy Protection for MEC Task Offloading in Industrial Internet," Cluster Computing, 2025.

[4] Y. Chen et al., "Joint Task Caching and Privacy-Protecting Task Offloading for Edge Computing," Computing, vol. 107, no. 7, 2025.

[5] F. Palmese et al., "Resource Optimization for Evidence Collection in IoT Forensics-Ready Access Points," IEEE Trans. Network Service Mgmt., vol. 22, no. 5, 2025.

[6] M. A. Aleisa, "Blockchain-Enabled Zero Trust Architecture for Privacy-Preserving Cybersecurity in IoT," IEEE Access, 2025.

APPLYING STRUCTURAL-FUNCTIONAL ANALYSIS TO PROTECT CORPORATE DATABASES

Yurii Shchavinsky, Oleksandr Budzynskyi, Diana Prymachenko, Nadiia Sviatska
State University of Information and Communication Technologies, Solomianska 7, 03110 Kyiv, Ukraine

Abstract

The current state of infrastructure development due to the spread of cyber threats requires the development of new approaches to protecting corporate databases, taking into account the structural and functional relationships between the components of the protection system and the processes of data collection. One way to solve the problem is to develop formalized models that allow quantitatively assessing threat levels and determining response priorities. The mathematical model developed in the research process represents three levels (structural, functional, threat level) and allows you to visualize critical points and the most important components of the system and quickly make decisions to apply countermeasures.

Keywords

Cyber threats, databases, structural-functional analysis, mathematical modeling

Introduction

The number of digital technologies grows daily, leading to the emergence of new cyber threats. There is a pressing need to improve techniques for detecting anonymous users, as malicious actors frequently exploit anonymity to carry out cyberattacks. Identifying anonymous users allows for the prevention and minimization of cyber incidents, thereby safeguarding critical state infrastructure through the monitoring and restriction of actions by unauthorized persons.

The aim of this study is to develop a mathematical model for structural-functional threat analysis, which formalizes the relationships between corporate database components, data processing functions, and potential security threats.

A considerable number of researchers have focused on the development and application of structural and functional analysis in various scientific domains, given its growing relevance in modern conditions. Most publications address its application in the social sciences [1– 2].

Basit et al. [3], when studying cybersecurity challenges, employed the Interpretive Structural Modeling (ISM) method combined with the Cross-Impact Matrix Multiplication Applied to Classification (MICMAC) approach developed by the United Nations. Their goal was to analyze barriers to solving cybersecurity problems. This constitutes a qualitative method for structuring poorly defined relationships among elements of complex systems. However, the study does not address the functional component of the system.

Zhylin et al. [4] focused mainly on the operation of a Security Operations Center (SOC), whose primary function is the monitoring and analysis of cybersecurity issues and incident response on the Internet. Such an approach pays insufficient attention to the stages of intrusion prevention and post-attack recovery, indicating a need to expand SOC functionality. At the same time, the authors note that these functions are not formalized or described in terms of their operational roles within the cybersecurity center.

The standards ISO/IEC 27005:2022 and NIST SP 800-150, although not explicitly using the term “structural and functional threat analysis,” contain several provisions and approaches that can be interpreted in this way. They provide guidance on information security risk management, including the process: establishing context - risk identification - risk analysis - risk evaluation - risk treatment. Two risk identification approaches are introduced:

- Event-based approach – considers risk scenarios at the level of risk sources, consequences, and context;

- Asset-based approach – begins with assets (system components), their vulnerabilities, threats, and related scenarios.

The standards do not prescribe specific evaluation methods (quantitative or qualitative) but allow organizations to select an approach adapted to their context.

Thus, the analysis of scientific literature and regulatory documents confirms the necessity of developing a structural and functional analysis model aimed at protecting corporate databases.Theoretical foundations of developing a method for structural and functional analysis of corporate database protection systems

The structural-functional analysis of threats to corporate databases formalized as a mathematical model that reflects the relationships between the structure of the information system, data processing functions, the nature of threats, and the resulting level of risk or security. The model combines a structural representation of the system (what exists) with a functional representation (what it does) in a single analytical scheme, where threats are described as impacts on these elements. The main idea of the model is that a threat is considered as a functional influence on a structural component of the system, leading to a change in the security state (e.g., loss of data integrity or availability). The model can be represented as a graph or a multi-level block diagram, including three main levels (Figure 1):

- Structural level, which describes the system elements – database servers; client applications; users (administrators, analysts, clients); network nodes (gateways, routers, VPNs, firewalls); authentication, logging, and backup subsystems;
- Functional level, which describes processes and interactions – executing database queries; access management (authorization, authentication); transaction processing; data transfer between client and server; security monitoring;
- Threat and impact level, which describes the "threat-component-function" relationships – types of threats (external/internal); implementation mechanisms (technical, organizational, social engineering); affected function (e.g., authentication or data transfer).

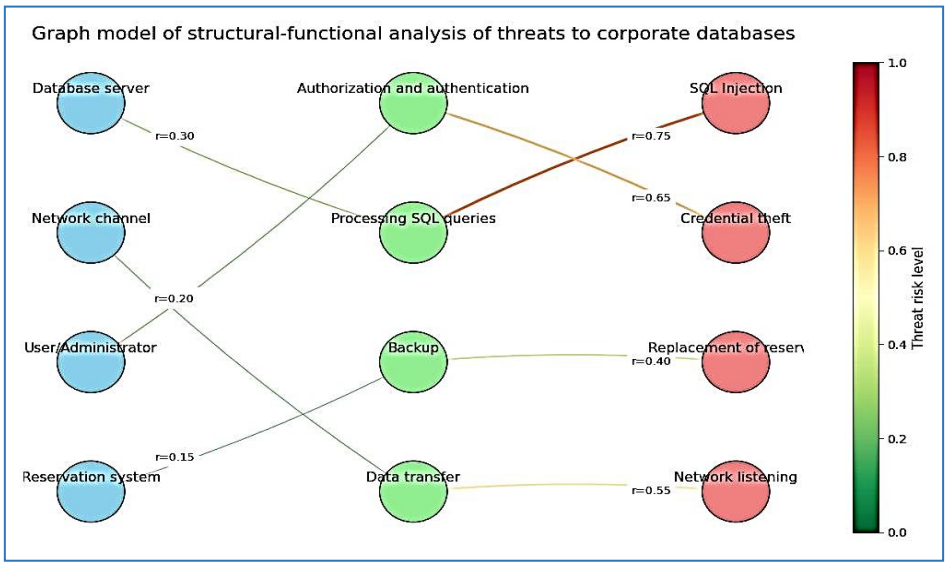

Figure 1: The result of the graph model of structural-functional analysis of threats to corporate databases.

The network infrastructure is represented as a weighted graph:

$$G=(C,T,E),$$

where C={ci} is the set of system components, T={tj} is the set of threats, and E⊆C×T denotes the relationships between them with weights wij indicating the impact level.

Functional dependencies among components are defined by the matrix:

$$F=[f_{ik}],\ f_{ik}\in[0,1],$$

where fik reflects the functional significance of component ci in performing function k.

The integrated system risk is calculated as:

$$R=\sum_{i=1}^{|C|}\sum_{j=1}^{|T|} w_{ij} f_{ik} p_j,$$

where pj is the probability of threat tj occurrence.

This model enables quantitative risk assessment considering both the structural topology and functional interdependencies of the corporate information system.

Conclusions

The method of structural-functional analysis of the corporate database protection system allows us to consider security not only as a set of technical measures, but as a holistic system that takes into account the structure of relationships, the functions of elements, the dynamics of risks and the effectiveness of countermeasures. It serves as a universal tool for studying corporate database security risks, optimizing protective measures and increasing the cyber resilience of enterprise information systems.

References

[1] Wearne, B. C. (2013). Exegetical Explorations: Parsons' Theoretical Faith and Hope in Structural Functional Analysis. The American Sociologist, 44(3), 245–258. https://doi.org/10.1007/s12108-013-9179-4.

[2] Potts, R., Vella, K., Dale, A., & Sipe, N. (2014). Exploring the usefulness of structural–functional approaches to analyse governance of planning systems. Planning Theory, 15(2), 162-189. https://doi.org/10.1177/1473095214553519 (Original work published 2016)

[3] Basit, Abdul & Qazi, Tehmina & Aziz, Abdul & Khan Niazi, Abdul Aziz & Aziz, Ifra. (2023). Structural Analysis of the Barriers to Address Cyber Security Challenges. 221-236. https://doi.org/10.5281/zenodo.7908753.

[4] Zhylin, A., Khudyncev, M., & Litvinov, M. (2018). Functional model of cybersecurity situation center.Collection "Information Technology and Security", 6(2), 51–67. https://doi.org/10.20535/2411-1031.2018.6.2.153490.

ABSTRACTS OF REPORTS OF THE INTERNATIONAL SCIENTIFIC AND PRA CTICAL CONFERENCE DIGITAL TRANSFORMATION: STRENGTHENING THE CYBERSECURITY CAPACITIES IN THE MODERN WORLD

4-5 November, Krakow
Published in the author's edition

Publisher: Tropea Publishing House
Signed for printing: 28 August 2024
Format: 75 × 100 1/32
Order No.: 712/24
Layout, design, and prepress preparation:
LLC "Pro Format"
Printed in accordance with the provided original layout by:
LLC "Pro Format"
Address:
73 Kostiantynivska Street, Kyiv, Ukraine
Certificate of registration of the publishing entity in the State Register:
DK No. 5942 dated 11 January 2018
Print run: 100 copies