DOI: https://doi.org/10.34069/AI/2023.65.05.15

How to Cite:

Bekmagambetova, G., Polukhin, A., Volodymyr, E., Denys, K., & Oksana, D. (2023). Algorithmic means of ensuring network security and websites: trends, models, future cases. *Amazonia Investiga*, *12*(65), 149-163. https://doi.org/10.34069/AI/2023.65.05.15

Algorithmic means of ensuring network security and websites: trends, models, future cases

Алгоритмічні засоби забезпечення мережевої безпеки та веб-сайтів: тренди, моделі, кейси майбутнього

Received: April 23, 2023 Accepted: June 1, 2023

Written by:
Gulmira Bekmagambetova[1]
https://orcid.org/0000-0002-8999-793X
Anton Polukhin[2]
https://orcid.org/0000-0002-3248-210X
Volodymyr Evdokimov[3]
https://orcid.org/0000-0001-9497-4030
Denys Kasmin[4]
https://orcid.org/0000-0002-3687-4688
Oksana Dmytriienko[5]
https://orcid.org/0000-0002-8414-1964

Abstract

The purpose of the study is to establish probable trends in the development of algorithmic means of network security and the protection of web resources in the future. The research methods used in this publication are a bibliometric analysis of 500 relevant publications, which allowed us to establish probable trends in the future development of the subject field. The study found that currently the most likely algorithmic means of network security and website protection that will be intensively developed in the future are blockchain technologies (to protect inter-resource contact), deep and machine learning (to analyze and detect attacks and digital anomalies), artificial intelligence and neural networks (to develop complex security algorithms), and predictive analysis (to prevent possible attacks and malicious data injections). At the same time, technological development makes it possible to identify alternative security tools, including quantum and post-quantum cryptography (which is possible due to the development of quantum

Анотація

Мета дослідження – встановлення ймовірних трендів розвитку алгоритмічних засобів мережної безпеки та захисту веб-ресурсів у майбутньому. У якості методів дослідження в даній публікації використаний бібліометричний аналіз 500 релевантних публікацій, що дозволив встановити ймовірні тренди майбутнього розвитку предметного поля. За результатами дослідження встановлено, що наразі найбільш ймовірними алгоритмічними засобами мережної безпеки та захисту веб-сайтів, що отримають інтенсивний розвиток у майбутньому є технології блокчейну (для захисту міжресурсного контакту), глибинного та машинного навчання (для аналізу та виявлення атак та цифрових аномалій), штучного інтелекту та нейромереж (для розробки складних безпекових алгоритмів), а також предиктивного аналізу (для попередження ймовірних атак та ін'єкцій шкідливих даних). Разом з тим, технологічний розвиток дозволяє визначити альтернативні безпекові засоби, серед яких квантова та пост-

[1] PhD, Associate Professor of Department of Information Technology, Kazakh University of Technology and Business, Republic of Kazakhstan.
[2] Postgraduate Student, Laboratory of Energy Markets Mathematical Modelling, G.E. Pukhov Institute for Modelling in Energy Engineering National Academy of Sciences of Ukraine, Ukraine.
[3] Candidate of Sciences in State Administration, Leading Researcher, G.E. Pukhov Institute for Modelling in Energy Engineering National Academy of Sciences of Ukraine, Ukraine.
[4] PhD in Economics, Associate Professor of Department of Social Economics, Faculty of Economy and Law, Simon Kuznets Kharkiv National University of Economics, Ukraine.
[5] PhD in Pedagogy, Associate Professor, Docent of the Department of Mathematical Analysis and Informatics, The Faculty of Computer Science, Mathematics, Physics and Economics, Poltava V.G. Korolenko National Pedagogical University, Ukraine.

computing), augmented reality (which is the next iteration of the development of the interface between machine-human interaction), biometric identification (which is the next iteration of authentication and recognition systems) and DevSecOps (which is a promising technology for the production of digital tools and systems that have a relatively lower level of vulnerability to known digital threats). The correlative impact of Industry 4.0 technologies and solutions on the studied aspects of the security sector of the World Wide Web has been established. The growth of the network of devices requires the improvement of security algorithms in the paradigm of Industry 4.0 technologies, which will allow more effective detection and prevention of cyberattacks and protection of user data.

Keywords: artificial intelligence, neural networks, machine learning, quantum cryptography, Industry 4.0.

квантова криптографія (що є можливою внаслідок розвитку квантового обчислення), розширена реальність (що є наступною ітерацією розвитку інтерфейсу машино-людської взаємодії), біометрична ідентифікація (що є наступною ітерацією систем автентифікації та розпізнання) та DevSecOps (що є перспективною технологією виробництва цифрових засобів і систем, що мають відносно нижчий рівень вразливостей до відомих цифрових загроз). Встановлений корелятивний вплив технологій та рішень Industry 4.0 на досліджувані аспекти безпекового сектору Всемережжя. Зростання мережі пристроїв вимагає вдосконалення безпекових алгоритмів в парадигмі технологій Industry 4.0, що дозволять ефективніше виявляти та запобігати кібератакам та захищати дані користувачів.

Ключові слова: штучний інтелект, нейромережі, машинне навчання, квантова криптографія, Industry 4.0.

Introduction

The information component is becoming increasingly important in civilizational development, forming a virtually digital twin of the real world, and the direct consequences of the financial and material ties between digital and physical reality are increasingly blurring the line between them. Given the progressive intensification of digitalization in virtually all areas of human activity, the issue of ensuring digital, network, and cyber-physical security is a constantly relevant and urgent task, the solution of which is largely in the realm of scientific research (Sharma et al., 2023; Hasan et al., 2023; Yang et al., 2023).

Statistical studies of specialized organizations prove the importance of researching and developing protective algorithms, tools, and systems, as cyber-digital threats are intensifying with the development of the digital sphere: in particular, in 2022, more than 25 thousand digital threats and vulnerabilities were detected, and identified, which is 20% more than in the previous year; in 2022, the average cost of data loss in the world was $ 4.35 million. The largest losses among digitalized industries in 2022 were in the healthcare sector, with the average cost of data loss in the world amounting to USD 10.1 million. Among the vulnerabilities that caused the largest financial losses in 2022 are phishing ($4.91 million with a 16% increase in data compared to 2021), losses in business correspondence ($4.89 million with a 6% increase in data compared to 2021), third-party software vulnerabilities ($4.55 million with a 16% increase in data compared to 2021), and a range of other vulnerabilities, with technical problems and system errors being the last. The latter fact proves that the architecture of global cyber-digital security requires systemic, cross-platform, and unitary solutions when organizing the interaction of technical means that form the Internet (Statista, 2023; National Institute of Standards and Technology, 2023; Vulnera, 2023; IBM, 2023).

Analytical studies on the vulnerabilities of digital systems and facilities point to interesting statistics: it has been found that systems that do not have a network connection (locally isolated systems) are more vulnerable to digital attacks, as their local digital security perimeter has a limited resource and information base, which contributes to the success of cyber threats and cyber-attacks. According to the study, the average time to fix critical vulnerabilities is 65 days; 33% of the vulnerabilities identified on the full stack in 2022 were found to have serious or critical vulnerability levels; the most common vulnerabilities at the application and API (Application Programming Interface) level are still related to malicious content injection (Injection); 13.5% of enterprise vulnerabilities are classified as high or critical vulnerability levels; 12% of all risks accepted by isolated systems in 2022 were critical. These analytical

conclusions prove the failure of the evolution of locally isolated digital and cyber-physical systems and focus on the development of global network security tools and systems as the only correct strategy for sustainable civilization development (Edgescan, 2023; Comparitech Limited, 2023; WPScan, 2023).

Thus, we note that the technical means of protection and damage to digital and cyber-physical systems are currently in relative parity (because technical vulnerabilities are not the root cause of significant financial losses), while global structures of the Internet require systemic solutions to ensure the effective functioning of the global digital security architecture (as evidenced by the increase in financial losses from systemic information and digital attacks), which, given the identified trend towards deeper integration of digital systems and means into physical reality (according to current scientific observations), requires an increase in the presence of scientific research in this security sector of sustainable civilizational development.

The purpose of the article is to study the issues of algorithmic means of ensuring network security and websites and to assess the prospects for their future development.

Theoretical Framework

According to the conclusions of Alemami, Al-Ghonmein, Al-Moghrabi, and Mohamed (2023), the use of algorithmic network and website security tools is critical to protecting information and ensuring security in cloud services. Similar conclusions about the effectiveness of cryptographic security algorithms (in particular in cloud services) were reached in the publications of Chauhan, Patel, Parikh, and Modi (2022), Lakshmi Narayanan, and Naresh (2023), Jabbar, and Bhaya (2023), Erondu, Asani, Arowolo, Tyagi, and Adebayo (2023), Bhagat, Kumar, Gupta, and Chaube (2023).

In their study, Sagu, Gill, Gulia, Singh, and Hong (2023) conclude that the use of algorithmic network security tools and websites is important for ensuring the security of the Internet of Things (hereinafter IoT). They describe the design of metaheuristic optimization algorithms for deep learning to secure IoT environments. The main conclusions of the study are that the use of metaheuristic optimization algorithms for deep learning can ensure the security of IoT network environments, allowing for improved efficiency and accuracy of security systems. Similar conclusions about the effectiveness of the technology of deep learning security algorithms are available in the publications of the following authors: Jose, and Jose (2023), Seh, Yirgaw, Ahmad, Faizan, Pathak, Zaman, and Agrawal (2023), Diaba, and Elmusrati (2023), Gheni, and Al-Yaseen (2023).

Chen, and Lee (2023) argues that the use of algorithmic means of ensuring network security and websites can be realized through the use of blockchain technology. In the article, the authors describe the use of blockchain-based algorithms for the development of IoT applications. The main conclusions are that the use of blockchain technology can ensure the security of IoT applications by allowing data to be stored and transmitted in a secure manner, without the risk of unauthorized access or modification. Khobragade, and Turuk (2023), Priyanka, Skandan, Shakthi Saravanan, Chandramohanan, Darshan, and Raswanth (2023), Zubaydi, Varga, and Molnár (2023) reached similar conclusions about the effectiveness of blockchain-based security algorithms.

Monika, Singh, and Wason (2023) explore the possibility of improving network security and website protection through the analysis and improvement of data protection algorithms. In particular, the article describes a study of the use of data protection algorithms in networks with multiprotocol label switching (GMPLS) technology. The conclusion of the paper is that improving data encryption and authentication algorithms can improve data security and privacy in GMPLS networks.

The article (Zoppi et al., 2023) discusses the possibility of improving network security and website protection through the use of intrusion detection algorithms. The article compares different types of intrusion detection algorithms, including supervised learning, unsupervised learning, and meta-learning. The general conclusion is that meta-learning intrusion detection algorithms are the most effective in detecting unknown attacks on networks and provide high accuracy and response speed. In addition, the article points out the importance of researching and developing new intrusion detection algorithms that will provide reliable and effective protection of networks and websites from various types of attacks. Similar conclusions about the effectiveness of machine learning security algorithms have been reached in some other publications (Upreti et al., 2023; Mughaid et al., 2023; Akhtar, & Feng, 2023; Al-Juboori et al., 2023).

Birrane, Heiner, and McKeever (2023) present the results of a study on improving network security and websites by using the security context of Delay-Tolerant Networks. The researchers conclude that the use of security context allows for a more accurate and efficient assessment of risks and threats to network security, which helps to increase security and privacy, as well as reduce the possibility of attacks and network security incidents. The use of security context is an important element in the development of new technologies and methods to ensure effective and reliable protection of web resources and networks, making it essential in improving network security.

Pradhan, Sahu, Rajeswari, Tun, and Wah (2023) highlight the opportunities for improving network security and websites by integrating artificial intelligence and machine learning into 5G technology. According to the study, the author notes that such integration can help increase data security and privacy, improve data transfer speeds, increase network reliability and efficiency, and allow solving complex network security and smart connectivity challenges. Pawełoszek, Kumar, and Solanki (2022), Bhuvaneshwari (2023), and Montasari (2023) reached similar conclusions about the effectiveness of AI-based security algorithm technology.

The transition of many markets to electronic trading platforms raises not only the issue of their security but also the violation of it can have severe consequences for the economy of a country or even a region. For example, in their work, Evdokimov and Polukhin (2022) considered optimizing trading on the wholesale electricity market, which can increase its efficiency. However, security breaches and illegal interference in the operations of such electronic trading platforms bring security concerns to the forefront, as trading failures can lead to real disruptions in the operation of the power system.

The use of algorithmic means of ensuring network security and websites is a hot topic in research and development in the modern world. Among the most used technologies are antivirus programs, intrusion detection and prevention systems, access control systems, blockchain, and others. It is also important to use artificial intelligence and machine learning to develop more complex and effective algorithms for network security and websites. Blockchain, artificial intelligence, deep learning, and machine learning are key technologies used to provide network and website security. Blockchain can ensure data security and privacy by storing information in distributed networks with blocks that cannot be altered or deleted without the prior consent of all network participants. Artificial intelligence and machine learning can help detect and prevent malicious attacks on networks and websites, as well as develop effective security algorithms and identify vulnerabilities. Deep learning is used to recognize and classify patterns, which helps to identify malicious objects and analyze the risks of using a malicious program. The use of these technologies can help ensure a high level of security for networks and websites, reduce the risks of their vulnerability to malicious attacks, and increase the efficiency of networks and websites. Research and development in this area is aimed at improving the security of networks and reducing the risks of their vulnerability to malicious attacks.

Methodology

In connection with the identified layers of non-systematic information in previous studies on the use of various algorithmic means of ensuring network security and websites in the context of generalizing and highlighting trends, models, and cases of future development of the global architecture of digital and cyber-physical security, it is advisable to apply the methods of bibliometric analysis of the focal area of the scientometric landscape in the current study.

Bibliometric analysis requires the use of specialized software that allows formulating an analytical information array in two iterations: (1) collection of relevant scientometric information in a selected current search horizon; (2) taxonomic analysis of the collected information with the subsequent formation of relevant analytical conclusions (Table 1).

Table 1.
Analysis of software and digital tools and resources for bibliometric analysis

Tool name	Analytical description
Tools for collecting scientometric information	
CRExplorer	Citation research is an important tool in analyzing scientific research, so Cited References Explorer uses data downloaded from Scopus and Web of Science databases to perform citation analysis over time. This tool is typically used to identify influential publications in a particular scientific field, which makes it indispensable in academic impact research (https://andreas-thor.github.io/CRExplorer).
Publish or Perish	Software that allows you to retrieve information from several databases, such as Web of Science, Scopus, Google Scholar, Microsoft Academic, and CrossRef. This tool is widely used to assess the academic impact of research and authors, which has made it indispensable for the scientific community. In particular, the program allows you to study the number of citations and the Hirsch index (h-index), which allows you to assess the scientific impact of individual researchers and their publications (https://harzing.com/resources/publish-or-perish).
ScientoPyUI	The open-source software that allows users to import data downloaded from Scopus and Web of Science databases to conduct scientific citation analysis. In particular, the program allows you to find the H-index and other important indicators that allow you to assess the scientific impact of individual researchers and their publications. This tool is open for use and can be useful for researchers who want to perform a detailed analysis of scientific data and find influential publications in their field (https://github.com/jpruiz84/ScientoPy/blob/master/README.md).
Tools for taxonomic analysis of scientometric data	
VOSviewer	A software tool designed to "build and visualize bibliometric networks". These networks can, for example, include journals, researchers, or individual publications and can be built on the basis of citation relationships, bibliographic relationships, co-citation, or co-authorship. This tool allows for detailed analysis of bibliometric data and visualization in a convenient and understandable format (https://www.vosviewer.com).
CiteSpace	A Java-based software tool used to analyze trends and patterns in the scientific literature. The tool uses data from the Web of Science as well as other sources such as arXiv, PubMed, and NSF Award Abstracts. CiteSpace allows users to perform various bibliometric analyses, including co-citation analysis, outlier detection, keyword analysis, and visualize the results using network and time zone maps (http://cluster.cis.drexel.edu/~cchen/citespace)
Bibliometrix	R is an open-source tool used for complex scientometric analyses. It uses data from Scopus, Web of Science, Dimensions, PubMed, and Cochrane. Requires deep knowledge of R, but has a new version (biblioshiny) that is designed for non-coders (https://www.bibliometrix.org)
Gephi	An open-source software for creating and visualizing network graphs that allows users to import data from almost any file format. To fully use the program, you need to know Java and/or OpenGL. Gephi allows you to perform a variety of analytical tasks on graphs, such as community analysis, identifying central nodes, and tracking changes in the network over time (https://gephi.org)
Sci2	An open-source visualization and analysis tool developed by scientists and librarians for scientists. Sci2 allows you to use data from various sources, including Scopus, Web of Science, MEDLINE, and others, to study scientific publications, including scientific relationships, references, citations, and author groupings (https://sci2.cns.iu.edu/user/index.php)

Source: created by the authors based on descriptions from software development sites

Taking into account the specifics of the study, we choose Publish or Perish as the software for collecting scientometric data, which has a comprehensive set of scientometric tools. As a digital software tool for taxonomic analysis of the selected information array of scientometric data, we will use the leading industry tool - VOSviewer, which has significant advantages over other software (Table 1): multi-format output data, intuitive interface, an informative graphical adaptation of taxonomic analysis, etc. With the help of VOSviewer, it is expected to determine the likely vectors of future development of algorithmic network security tools and websites.

Thus, the research scheme proposed for implementation in the current publication involves the following stages of bibliometric analysis:

1. Formation of an information array of scientometric data based on relevant scientific papers and publications in the

current search horizon using the digital software tool Publish or Perish. To ensure the indirectness and independence of the research results, a scientometric horizon of 500 specialized publications in a specific research vector on algorithmic means of ensuring network security and websites is taken into account for analysis.

2. Transfer of the generated information array of scientometric data to the VOSviewer software, which further generates taxonomic schemes that determine the likely vectors of development of algorithmic means of ensuring network security and websites.
3. Formation of analytical conclusions (based on the results of the previous stages of the study) on the future development of algorithmic network security technology and websites.

The implementation of the proposed research scheme will provide far-sighted analytical conclusions about the security sector and will allow potential researchers to focus on unresolved issues and specific problems.

Results and Discussion

Results of the formation of a separate section of the scientometric landscape on the technology of algorithmic means of ensuring network security and websites using Publish or Perish software - Table 2.

Table 2.
An information array of relevant publications and scientific papers created in the Publish or Perish software

Parameter	Meaning
Query	Algorithmic technology of network security from 2018 to 2023
Source	Web of Science, Scopus, Google Scholar, Microsoft Academic, CrossRef
Papers	500
Citations	114805
Years	5
Cites_Year	22961.00
Cites_Paper	229.61
Cites_Author	46760.30
Papers_Author	181.60
Authors_Paper	3.58
h_index	176
g_index	312
hc_index	197
hI_index	49.09
hI_norm	100
AWCR	38725.80
AW_index	196.79
AWCRpA	18984.41
e_index	217.47
hm_index	117.81
QueryDate	12.04.2023 23:52
Cites_Author_Year	9352.06
hI_annual	20.00
h_coverage	68.2
g_coverage	85.2
star_count	493
year_first	2018
year_last	2023
ECC	114805
acc1	500
acc2	500
acc5	496
acc20	461
hA	82

Source: created by the author at Publish or Perish

According to the formed information array (Table 2), made using data from Web of Science, Scopus, Google Scholar, Microsoft Academic, and CrossRef, 500 articles were collected for the period from 2018 to 2023 by the query "Algorithmic technology of network security". The total number of citations amounted to 114805 (which indicates a great interest of the scientific community in this topic), which gives a Cites_Year index of 22961.00 and a Cites_Paper index of 229.61. The Cites_Author and Papers_Author indicators are 46760.30 and 181.60, respectively. On average, there are almost 2 papers per author, which is reflected in the Authors_Paper index of 1.58. The Hirsch index (h_index) is 176, and its variants g_index and hc_index are 312 and 197, respectively. The value of the hI_index is 49.09, and hI_norm is 100. AWCR and AW_index are 38725.80 and 196.79, respectively, and AWCRpA is 18984.41. The efficiency index (e_index) is 217.47, and the hm_index is 117.81. The high AWCR, AW_index, and e_index scores demonstrate the high scientometric activity of researchers in this field. According to the report, the number of citations per year per author is 9352.06, and the hI_annual index is 20.00. The h_coverage and g_coverage coefficients are 68.2 and 85.2, respectively. The results of the analysis allowed us to mark 493 stars, with the first year of publication being 2018 and the last year being 2023 (which may be due to an increase in the number of citations of some outstanding works). The total number of articles that have received at least one citation is 500, which resulted in acc1, acc2, acc5, and acc20 scores of 500, 500, 496, and 461, respectively. It is noted that the average number of authors per article is 1.64, which is reflected in the hA index of 82.

In accordance with the proposed research scheme, the relevant information array of scientometric data generated in the Publish or Perish software is transferred to the digital software environment of the VOSviewer software.

Using the built-in tools of the VOSviewer software, we obtained a taxonomic scheme of the selected area of the scientometric landscape for the query "Algorithmic technology of network security" (Figure 1).

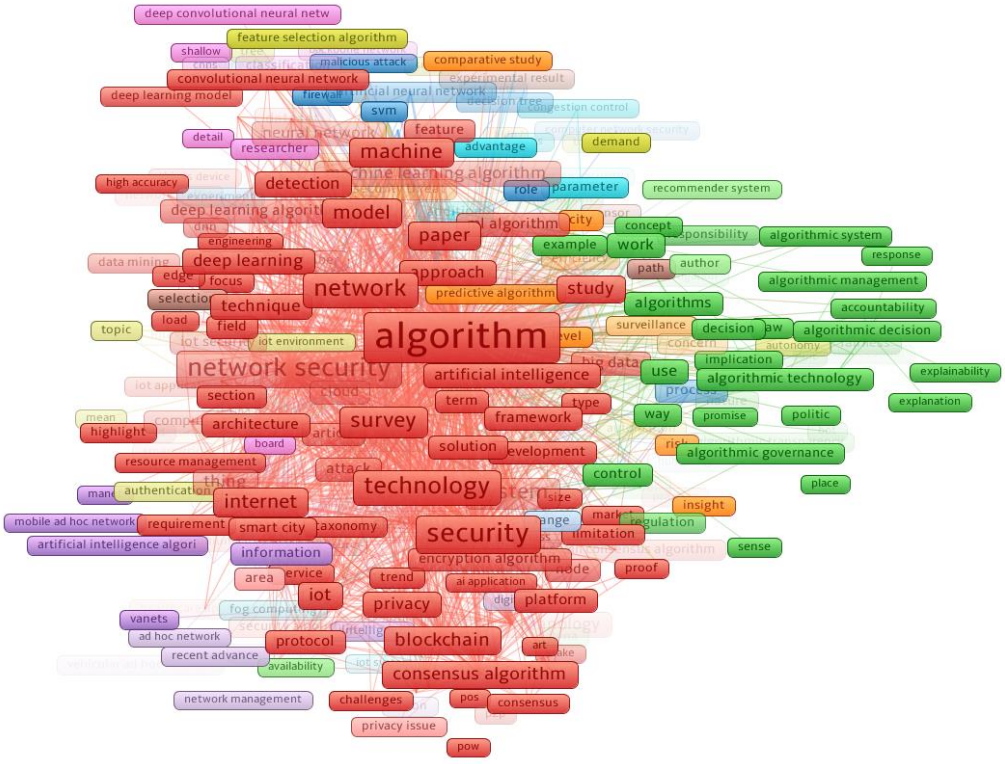

Figure 1. The taxonomic scheme formed on the results of 500 relevant scientific publications on the query "Algorithmic technology of network security" for the period 2018-2023.
Source: created by the author in VOSviewer software

The resulting taxonomic scheme (Figure 1) contains 482 taxonomic units (with binary simplification of calculations), which are combined into 19 clusters, interconnected by 9435 main links (with their full number - 15328 units). To perform analytical conclusions, the

modulation method of normalization of taxonomic units was used.

In order to determine the trends in the future development of algorithmic means of network security and protection of web resources, we perform a dynamic analysis of the obtained field of relevant taxonomy (Figure 2).

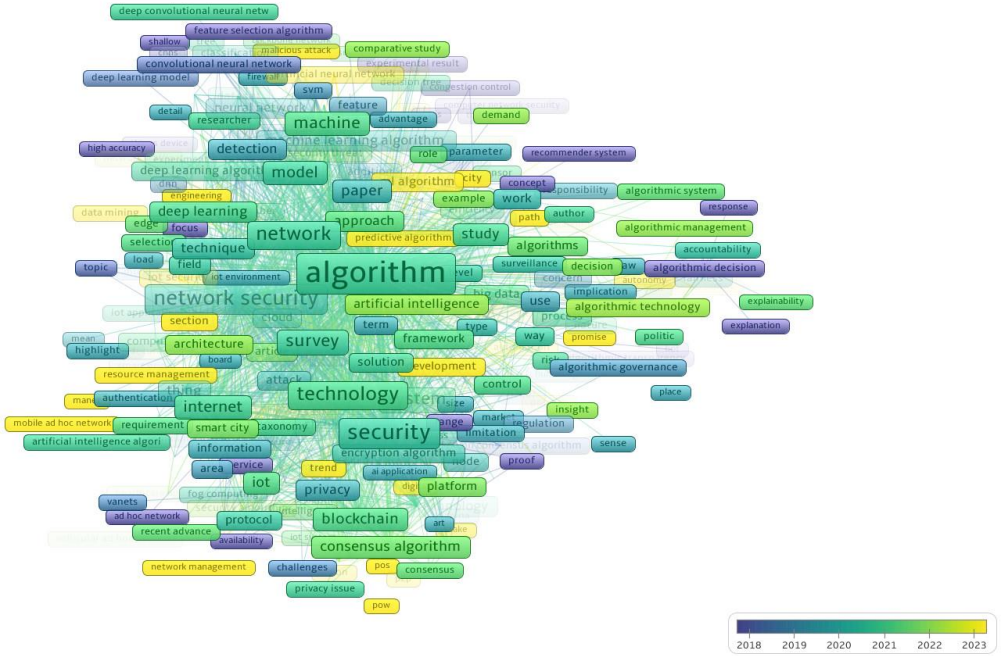

Figure 2. The taxonomic scheme formed based on 500 relevant scientific publications on the query "Algorithmic technology of network security" for the period 2018-2023 and adapted to the chronometric dynamics of the development of clustered research vectors (trends)
Source: created by the author in VOSviewer software

According to the timeline adapted to the dynamics of the clustered vectors that make up the selected relevant area of the scientometric landscape (Figure 2), we will identify the current research trends that are likely to have the greatest impact on the development of the subject area in the future (Figure 3):

1. *Development of blockchain technology*. In the future, blockchain technology will continue to evolve as an effective algorithmic means of ensuring network security and website protection. It is predicted that blockchain will be used to create secure decentralized networks where digital assets can be stored, exchanged, and transferred without intermediation. Also, blockchain can be used to develop secure systems for identifying and authenticating users on the Internet. Another area of development of blockchain technology may be its use to protect against cyberattacks and increase the reliability of network protocols. However, in order to achieve these goals, it is necessary to investigate and solve the problems of scalability and efficiency of blockchain technology (Figure 3 (*a*)).
2. *Development of deep learning technology*. The future development of deep learning technology opens up new opportunities to improve the security of networks and websites. The use of deep learning can help detect and prevent cyberattacks, as well as ensure the security of web applications and networks. Future developments in this technology may include expanding functions, such as improving risk analysis and identifying new threats, as well as improving the effectiveness of attack protection by training models on a variety of data and applying new deep learning techniques such as reinforcement learning and generative adversarial networks (Figure 3 (*b*)).
3. *Development of machine learning technology*. Machine learning is expected to continue to evolve in the context of the website and network security. With the help of learning algorithms, it will be possible to automatically detect vulnerabilities and potential threats to the network and website,

respond quickly to incidents, and prevent attacks. In particular, machine learning is expected to be used to develop more effective algorithms for monitoring, detecting, and predicting malicious actions, as well as to develop new systems for protecting against cyberattacks (Figure 3 (*c*)).

4. *Development of artificial intelligence technology*. Future developments in artificial intelligence technology may include increasing the efficiency and accuracy of detecting threats and attacks on networks and websites. Artificial intelligence may be used to prevent cyberattacks and predict future threats. New methods of interactive learning may also be developed to engage people in the process of identifying and combating cyber threats (Figure 3 (*d*)).
5. *Development of neural network technology*. The future development of neural network technology as one of the algorithmic means of network security and website protection involves their increasing use in cyberattack detection and prevention systems. To achieve this goal, neural networks will be developed taking into account the needs of security and attack resistance, in particular, risk management algorithms and methods of increasing attack resistance will be applied. Neural network technology is also expected to be used to develop intelligent systems for monitoring network activity and predicting the risks of website hacking. One of the most promising areas is the development of neural networks for detecting and analyzing abnormal activity in networks, which will allow for quick detection and response to cyberattacks (Figure 3 (*e*)).
6. *Development of predictive analysis technology*. Future developments in predictive analytics technology include the increased use of machine learning and artificial intelligence to predict future threats and identify critical risks in networks and websites. The development of Big Data and Cloud Computing technologies will allow the use of large amounts of data to build more accurate models that will increase the accuracy of predictive analysis. Such models can be used to identify threats that were not known before and predict the likelihood of their occurrence in the future (Figure 3 (*f*)).

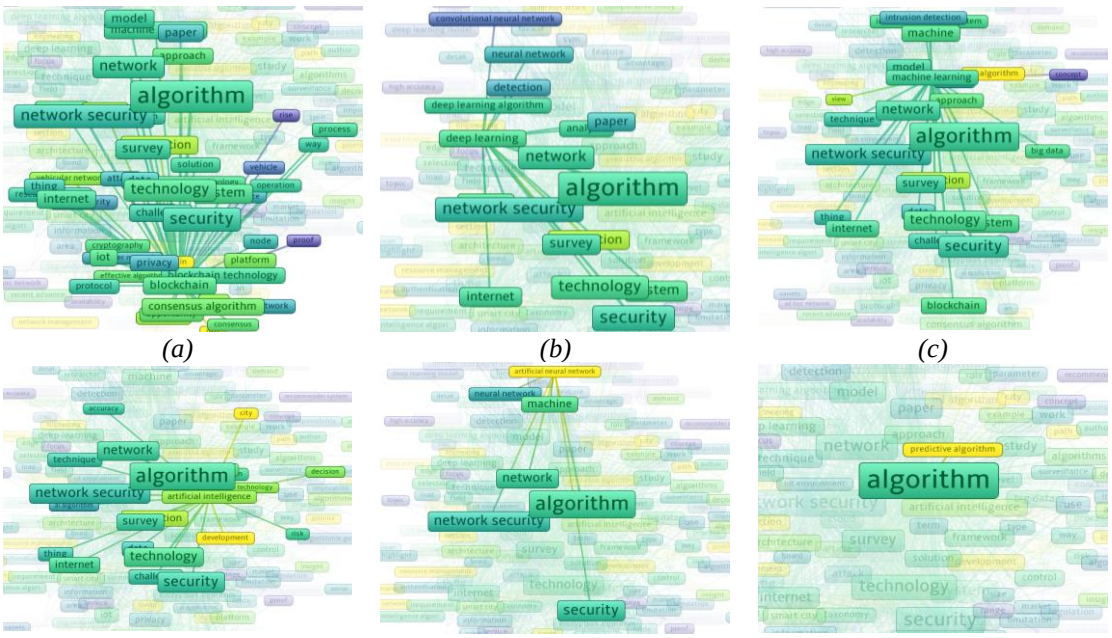

Figure 3. Identification of trends in the likely development of algorithmic means of network security and website protection in the future: (a) blockchain, (b) deep learning, (c) machine learning, (d) artificial intelligence, (e) neural networks, (f) predictive analysis.
Source: created by the author in VOSviewer software

The identified trends in the future development of algorithmic means of network security and website protection (Figure 3) correlate with the conclusions about the prospects for the specialized use of these tools in the security sector of the World Wide Web, which contain the relevant publications of the authors:

Hrynchyshyn (2021), Yarmoliuk (2022), Shiau, Wang, and Zheng (2023).

At the same time, in addition to the identified probable and promising vectors of development of algorithmic tools for the security sector of the Internet, there are the latest developments, among which the following cases should be highlighted:

1. *Quantum and post-quantum cryptography*. Quantum cryptography uses the principles of quantum mechanics to ensure the security of data transmission. With the future development of quantum computers that are capable of unraveling complex encryption algorithms, post-quantum cryptography is becoming increasingly important for securing networks and websites. This technology uses mathematical principles to create strong cryptographic systems that cannot be decrypted even by quantum computers. As interest in post-quantum cryptography grows, it could become an important algorithmic tool for network and website security in the future (Shalini et al.2023; Yi, 2023; Gazdag et al., 2023).
2. *Augmented reality*. In recent years, augmented reality (AR) technology has evolved significantly, especially in the field of network security and website security. AR can be used to create virtual training scenarios to help users recognize threats and learn how to respond to them. Also, AR can be used to visualize data from various sources, which will help identify possible security breaches and prevent them. The future development of AR technology envisages the growth of its use in such industries as medicine, military, and other areas where detailed and accurate data analysis is essential. The use of AR for website security involves the development of new technologies, such as virtual blockchains and smart contracts, which will ensure more efficient and secure data exchange on the network (Herbert et al., 2022; Alzahrani, & Alfouzan, 2022; Harris et al., 2023).
3. *Biometric identification*. Future developments in biometric identification technology include increasing the accuracy and speed of identification using biometric data such as fingerprints, facial recognition, and others. The use of biometric data for identification may become increasingly common in websites and network security, where it can be used to improve security and user experience. Progressive developments in artificial intelligence and machine learning technologies may lead to even more accurate and efficient biometric identification systems. However, there are potential privacy and personal data protection issues that should be considered and addressed in the future (Brogan et al., 2023; Shalini, 2023; Yadav et al., 2023).
4. Development of websites and applications with regard to possible DevSecOps vulnerabilities. DevSecOps is a combination of DevOps practices and security principles. This technology includes security testing tools, automated monitoring, and data analysis to identify vulnerabilities. It is expected that the future development of DevSecOps will be aimed at even greater integration of security into software development, as well as the use of other algorithmic network security tools, such as artificial intelligence, machine learning, blockchain, and others. An important part of DevSecOps development will be the integration of augmented reality to display security monitoring data and track critical vulnerabilities. Similar conclusions were reached in the publications (Li, & Zalialetdzinau, 2022; Martelleur, & Hamza, 2022; Dupont et al., 2023).

In general, in the context of the future development of algorithmic means of network security and protection of web resources, there is a correlative influence of the technologies of the fourth wave of industrial development (Industry 4. 0), which is agreed by researchers Ferencz, Domokos, and Kovacs (2021), Saura, Ribeiro-Soriano, and Palacios-Marqués (2022), Fernando, Tseng, Wahyuni-Td, de Sousa Jabbour, Chiappetta Jabbour, and Foropon, (2023). The fourth wave of the industrial revolution, associated with the growth in the number of devices connected to the network, has necessitated the improvement of algorithmic means of ensuring network security and protecting web resources. In particular, the introduction of smart devices and the expansion of the Internet of Things have led to an increase in the risk of cyberattacks. Therefore, modern algorithmic tools for network security and web resource protection should be improved by using the latest Industry 4.0 technologies, such as artificial intelligence, machine learning, data analytics, blockchain, Internet of Things, etc. Such tools allow for the development of more efficient algorithms, real-time security monitoring, detection and prevention of cyberattacks, and protection of users' personal data. It will also ensure the security of built

model support tools and various simulation models designed to perform analysis and calculations based on real input data that may be confidential. In the future, the development of Industry 4.0 technologies to the following variable iterations may lead to the emergence of new algorithmic means of network security and protection of web resources that will be more efficient and reliable.

Conclusions

This study aimed to establish the prospects for the development of algorithmic means of network security and website protection in the future. Based on the results of the bibliometric analysis of 500 relevant publications published in the period from 2018 to 2023, the probable directions of future development of the subject area were established, in which the following trends were identified:

1. *Blockchain*. Blockchain continues to evolve as an algorithmic tool for network security and website protection, used to create secure decentralized networks, user identification, and authentication systems, protect against cyberattacks, and increase the reliability of network protocols but requires research on scalability and efficiency.
2. *Deep learning*. The future development of deep learning technology may open up new opportunities to improve the security of networks and websites, including improved risk analysis and detection of new threats, as well as increased effectiveness of defense against attacks using new deep learning methods such as reinforcement learning and generative adversarial networks.
3. *Machine learning*. Machine learning will continue to evolve to automatically detect vulnerabilities and potential threats to the network and websites, as well as to develop more effective algorithms for monitoring, detecting, and predicting malicious actions, and new systems for protecting against cyberattacks.
4. *Artificial intelligence*. Future developments in artificial intelligence technology can increase the accuracy and effectiveness of detecting threats and attacks on networks and websites, including predicting future threats and new interactive learning methods that engage people in the process of combating cyber threats.
5. *Neural networks*. The future development of neural network technology involves their increasing use in cyberattack detection and prevention systems, taking into account the needs of security and attack resistance, as well as the development of intelligent systems for monitoring network activity and detecting and analyzing anomalous activity in networks.
6. *Predictive analysis*. The future development of predictive analytics technology involves the use of machine learning and artificial intelligence to predict future threats and identify critical risks in networks and websites using Big Data and Cloud Computing technologies.

The identified trends in the development of algorithmic means of network security and protection of web resources are most likely in the near future, but at the same time, technological development allows us to consider alternative technological capabilities of the security sector of the World Wide Web, which are determined by the following trends:

1. Quantum and post-quantum cryptography as a result of technological development and increase of computing power of quantum computers. The future development of quantum computers makes post-quantum cryptography important as a mathematical technology for creating reliable cryptographic systems that ensure the security of data transmission in networks and websites.
2. Augmented reality as the latest interface for machine-human interaction. With the help of augmented reality, you can create virtual training scenarios and visualize data to detect possible security breaches, making AR an important algorithmic tool for network security and website protection in the future.
3. Biometric identification as a secure authentication and recognition technology. The future development of biometric identification involves increasing the accuracy and speed of biometric identification, which can improve the security and convenience of websites and networks but also requires attention to privacy and personal data protection issues.
4. DevSecOps as a technology for developing invulnerable tools and systems. The future development of DevSecOps involves even greater integration of security into software development and the use of other algorithmic network security tools, including augmented reality to display security monitoring data and track critical vulnerabilities.

The study made it possible to establish the correlative impact of technological solutions of the fourth wave of industrial development on the implementation of security algorithms in network systems and web resources. The researchers agree that the growth of network-connected devices and the expansion of the Internet of Things require the improvement of algorithmic means of network security and protection of web resources through the use of Industry 4.0 technologies, such as artificial intelligence, machine learning, data analytics, blockchain, and the Internet of Things, which will allow the development of more efficient algorithms, detect and prevent cyberattacks, and ensure the protection of users' personal data. In the future, it is advisable to investigate the possible connection between the identified trends in the future development of algorithmic digital security tools in the general paradigm of the next iteration of Industry 5.0.

Bibliographic references

Akhtar, M. S., & Feng, T. (2023). Evaluation of Machine Learning Algorithms for Malware Detection. Sensors, 23(2), 946. https://doi.org/10.3390/s23020946

Alemami, Y., Al-Ghonmein, A. M., Al-Moghrabi, K. G., & Mohamed, M. A. (2023). Cloud data security and various cryptographic algorithms. International Journal of Electrical and Computer Engineering, 13(2), 1867-1879. https://doi.org/10.11591/ijece.v13i2.pp1867-1879

Al-Juboori, S. A. M., Hazzaa, F., Jabbar, Z. S., Salih, S., & Gheni, H. M. (2023). Man-in-the-middle and denial of service attacks detection using machine learning algorithms. Bulletin of Electrical Engineering and Informatics, 12(1), 418-426. https://doi.org/10.11591/eei.v12i1.4555

Alzahrani, N. M., & Alfouzan, F. A. (2022). Augmented reality (AR) and cyber-security for smart cities—A systematic literature review. Sensors, 22(7), 2792. https://doi.org/10.3390/s22072792

Bhagat, V., Kumar, S., Gupta, S. K., & Chaube, M. K. (2023). Lightweight cryptographic algorithms based on different model architectures: A systematic review and futuristic applications. Concurrency and Computation: Practice and Experience, 35(1), e7425. https://doi.org/10.1002/cpe.7425

Bhuvaneshwari, K. S. (2023). Smart System and Services Using Artificial Intelligence and Machine Learning Algorithms: Sky of AI. In P. Raj, K. Saini, & V. Pacheco (Eds.), Applying Drone Technologies and Robotics for Agricultural Sustainability (pp. 140-154). IGI Global. https://doi.org/10.4018/978-1-6684-6413-7.ch009

Birrane, E. J., Heiner, S., & McKeever, K. (2023). Using Security Contexts. In eds E.J. Birrane, S. Heiner, & K. McKeever (Eds.), Securing Delay-Tolerant Networks with BPSec (pp.178-198). Wiley. https://doi.org/10.1002/9781119823513.ch10

Brogan, J., Barber, N., Cornett, D., & Bolme, D. (2023). VDiSC: An Open Source Framework for Distributed Smart City Vision and Biometric Surveillance Networks, Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision (WACV) Workshop. https://acortar.link/dL5s9l

Chauhan, J. A., Patel, A. R., Parikh, S., & Modi, N. (2022). An Analysis of Lightweight Cryptographic Algorithms for IoT-Applications. In S. Rajagopal, P. Faruki, & K. Popat (Eds.), Advancements in Smart Computing and Information Security (pp. 201-216). ASCIS 2022. Communications in Computer and Information Science (Vol. 1760). Springer, Cham. https://doi.org/10.1007/978-3-031-23095-0_15

Chen, J. I.-Z., & Lee, C.-Y. (2023). Algorithms Based on Block-Chain Applied to Develop the IoT Applications [Preprint]. Research Square. https://doi.org/10.21203/rs.3.rs-2331906/v1

Comparitech Limited (2023). Cybersecurity vulnerability statistics and facts of 2023. https://acortar.link/nCgpFD

Diaba, S. Y., & Elmusrati, M. (2023). Proposed algorithm for smart grid DDoS detection based on deep learning. Neural Networks, 159, 175-184. https://doi.org/10.1016/j.neunet.2022.12.011

Dupont, S., Yautsiukhin, A., Ginis, G., Iadarola, G., Fagnano, S., Martinelli, F., Ponsard, C., Legay, A., & Massonet, P. (2023, February). Product Incremental Security Risk Assessment Using DevSecOps Practices. In S. Katsikas et al. (Eds.), Computer Security. ESORICS 2022 International Workshops: CyberICPS 2022, SECPRE 2022, SPOSE 2022, CPS4CIP 2022, CDT&SECOMANE 2022, EIS 2022, and SecAssure 2022, Copenhagen, Denmark, September 26–30, 2022, Revised Selected Papers (pp. 666-685). Cham: Springer International Publishing.

https://doi.org/10.1007/978-3-031-25460-4_38

Edgescan. (2023). Vulnerability Stats Report. https://www.edgescan.com/intel-hub/stats-report

Erondu, U. I., Asani, E. O., Arowolo, M. O., Tyagi, A. K., & Adebayo, N. (2023). An Encryption and Decryption Model for Data Security Using Vigenere With Advanced Encryption Standard. In A. Tyagi (Ed.), Using Multimedia Systems, Tools, and Technologies for Smart Healthcare Services (pp. 141-159). IGI Global. https://doi.org/10.4018/978-1-6684-5741-2.ch009

Evdokimov, V., & Polukhin, A. (2022). Income optimization of market participants in the day ahead market by modeling of processes of price determination for day ahead market. Electronic modeling, 44(4), 121-129. https://doi.org/10.15407/emodel.44.04.121

Ferencz, K., Domokos, J., & Kovacs, L. (2021). Review of industry 4.0 security challenges, IEEE 15th international symposium on applied computational intelligence and informatics (SACI). Timisoara, Romania: IEEE. https://doi.org/10.1109/SACI51354.2021.9465613

Fernando, Y., Tseng, M.-L., Wahyuni-Td, I. S., de Sousa Jabbour, A. B. L., Chiappetta Jabbour, C. J., & Foropon, C. (2023). Cyber supply chain risk management and performance in industry 4.0 era: information system security practices in Malaysia. Journal of Industrial and Production Engineering, 40(2), 102-116. https://doi.org/10.1080/21681015.2022.2116495

Gazdag, S.-L., Grundner-Culemann, S., Heider, T., Herzinger, D., Schärtl, F., Cho, J. Y., Guggemos, T., & Loebenberger, D. (2023). Quantum-Resistant MACsec and IPsec for Virtual Private Networks. In F. Günther, & J. Hesse (Eds.), Security Standardisation Research (pp. 1-21). SSR 2023. Lecture Notes in Computer Science (Vol. 13895). Springer, Cham. https://doi.org/10.1007/978-3-031-30731-7_1

Gheni, H. Q., & Al-Yaseen, W. L. (2023). Using Ensemble Techniques Based on Machine and Deep Learning for Solving Intrusion Detection Problems: A Survey. Karbala International Journal of Modern Science, 9(1), 5. https://doi.org/10.33640/2405-609X.3277

Harris, D., Miknis, M., Smith, C., & Wilson, I. (2023). Metrics for Evaluating Cyber Security Data Visualizations in Virtual Reality. PRESENCE: Virtual and Augmented Reality, 29, 223-240. https://doi.org/10.1162/pres_a_00363

Hasan, M. K., Habib, A. A., Shukur, Z., Ibrahim, F., Islam, S., & Razzaque, M. A. (2023). Review on the cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations. Journal of Network and Computer Applications, 209, 103540. https://doi.org/10.1016/j.jnca.2022.103540

Herbert, B., Wigley, G., Ens, B., & Billinghurst, M. (2022). Cognitive load considerations for Augmented Reality in network security training. Computers & Graphics, 102, 566-591. https://doi.org/10.1016/j.cag.2021.09.001

Hrynchyshyn, Y. (2021). The infrastructure of the Internet services market of the future: analysis of the problems of formation. Futurity Economics & Law, 1(2), 12–16.

IBM (2023). Cost of a data breach 2022. A million-dollar race to detect and respond. https://www.ibm.com/reports/data-breach

Jabbar, A. A., & Bhaya, W. S. (2023). Security of private cloud using machine learning and cryptography. Bulletin of Electrical Engineering and Informatics, 12(1), 561-569. https://doi.org/10.11591/eei.v12i1.4383

Jose, J., & Jose, D. V. (2023). Deep learning algorithms for intrusion detection systems in internet of things using CIC-IDS 2017 dataset. International Journal of Electrical and Computer Engineering (IJECE), 13(1), 1134-1141. https://doi.org/10.11591/ijece.v13i1.pp1134-1141

Khobragade, P., & Turuk, A.K. (2023). Blockchain Consensus Algorithms: A Survey. In J. Prieto, F.L. Benítez Martínez, S. Ferretti, D. Arroyo Guardeño, & P. Tomás Nevado-Batalla (Eds.), Blockchain and Applications, 4th International Congress (pp. 198-210). BLOCKCHAIN 2022. Lecture Notes in Networks and Systems (Vol. 595). Springer, Cham. https://doi.org/10.1007/978-3-031-21229-1_19

Lakshmi Narayanan, K., & Naresh, R. (2023). An efficient key validation mechanism with VANET in real-time cloud monitoring metrics to enhance cloud storage and security. Sustainable Energy Technologies and Assessments, 56, 102970. https://doi.org/10.1016/j.seta.2022.102970

Li, T., & Zalialetdzinau, K. (2022). Attemps of scientific reflection on the role of e-learning of the future in the area of digital transformation: new opportunities and

experiences with DevSecOps. Futurity Education, 2(4), 52–63. https://doi.org/10.57125/FED.2022.25.12.06

Martelleur, J., & Hamza, A. (2022). Security Tools in DevSecOps: A Systematic Literature Review. [File PDF]. http://urn.kb.se/resolve?urn=urn%3Anbn%3Ase%3Alnu%3Adiva-118400

Monika, D., Singh, S., & Wason, A. (2023). Performance investigations on data protection algorithms in generalized multi protocol label switched optical networks. Scientific Reports, 13(1), 425. https://doi.org/10.1038/s41598-022-26942-0

Montasari, R. (2023). Artificial Intelligence and the Internet of Things Forensics in a National Security Context. In R. Montasari (Eds.), Countering Cyberterrorism: The Confluence of Artificial Intelligence, Cyber Forensics and Digital Policing in US and UK National Cybersecurity (pp. 57-80), Vol. 101. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-21920-7_4

Mughaid, A., AlZu'bi, S., Alnajjar, A., AbuElsoud, E., Salhi, S. E., Igried, B., & Abualigah, L. (2023). Improved dropping attacks detecting system in 5g networks using machine learning and deep learning approaches. Multimedia Tools and Applications, 82(9), 13973-13995. https://doi.org/10.1007/s11042-022-13914-9

National Institute of Standards and Technology (2023). National Vulnerability Database (NVD) Dashboard. (2023). https://nvd.nist.gov/general/nvd-dashboard#

Pawełoszek, I., Kumar, N., & Solanki, U. (2022). Artificial intelligence, digital technologies and the future of law. Futurity Economics & Law, 2(2), 22–32. https://doi.org/10.57125/FEL.2022.06.25.03

Pradhan, D., Sahu, P. K., Rajeswari, Tun, H. M., & Wah, N. K. S. (2023). Integration of AI/Ml in 5G Technology toward Intelligent Connectivity, Security, and Challenges. In P. Chatterjee, M. Yazdani, F. Fernández-Navarro, & J. Pérez-Rodríguez (Eds.), Machine Learning Algorithms and Applications in Engineering. CRC Press. https://doi.org/10.1201/9781003104858-14

Priyanka, K., Skandan, S., Shakthi Saravanan, S., Chandramohanan, R., Darshan, M., & Raswanth, S.R. (2023). Unique and Secure Account Management System Using CNN and Blockchain Technology. In J. Singh, D. Das, L. Kumar, & A. Krishna (Eds.), Mobile Application Development: Practice and Experience. Studies in Systems, Decision and Control (pp. 131-140), Vol. 452. Singapore: Springer. https://doi.org/10.1007/978-981-19-6893-8_11

Sagu, A., Gill, N. S., Gulia, P., Singh, P. K., & Hong, W.-C. (2023). Design of Metaheuristic Optimization Algorithms for Deep Learning Model for Secure IoT Environment. Sustainability, 15(3), 2204. https://doi.org/10.3390/su15032204

Saura, J. R., Ribeiro-Soriano, D., & Palacios-Marqués, D. (2022). Evaluating security and privacy issues of social networks based information systems in Industry 4.0. Enterprise Information Systems, 16(10-11), 1694-1710. https://doi.org/10.1080/17517575.2021.1913765

Seh, A. H., Yirgaw, H., Ahmad, M., Faizan, M., Pathak, N., Zaman, M., & Agrawal, A. (2023). A Cybersecurity Perspective of Machine Learning Algorithms. In S. A. Khan, R. Kumar, O. Kaiwartya, R. A. Khan, & M. Faisal (Eds.), Computational Intelligent Security in Wireless Communications (pp. 221-240). CRC Press. https://doi.org/10.1201/9781003323426

Shalini, P. (2023). Multimodal biometric decision fusion security technique to evade immoral social networking sites for minors. Applied Intelligence, 53(3), 2751-2776. https://doi.org/10.1007/s10489-022-03538-9

Shalini, S., Selvi, M., Kannan, A., & Santhosh Kumar, S.V.N. (2023). Review of Security Methods Based on Classical Cryptography and Quantum Cryptography. Cybernetics and Systems. https://doi.org/10.1080/01969722.2023.2166261

Sharma, D., Mittal, R., Sekhar, R., Shah, P., & Renz, M. (2023). A bibliometric analysis of cyber security and cyber forensics research. Results in Control and Optimization, 10, 100204. https://doi.org/10.1016/j.rico.2023.100204

Shiau, W. L., Wang, X., & Zheng, F. (2023). What are the trend and core knowledge of information security? A citation and co-citation analysis. Information & Management, 60(3), 103774. https://doi.org/10.1016/j.im.2023.103774

Statista. (2023). Number of common IT security vulnerabilities and exposures (CVEs) worldwide from 2009 to 2023 YTD. https://www.statista.com/statistics/500755/worldwide-common-vulnerabilities-and-exposures

Upreti, K., Syed, M. H., Khan, M. A., Fatima, H., Alam, M. S., & Sharma, A. K. (2023). Enhanced algorithmic modelling and

architecture in deep reinforcement learning based on wireless communication Fintech technology. Optik, 272, 170309. https://doi.org/10.1016/j.ijleo.2022.170309

Vulnera (2023) The Vulnerability Stats, Data and Trends to Know in 2023. https://vulnera.com/2023/01/03/vulnerability-statistics-for-2023

WPScan. (2023) WordPress Vulnerability Statistics. https://wpscan.com/statistics

Yadav, P., Chaurasia, N., Gola, K. K., Semwan, V. B., Gomasta, R., & Dubey, S. (2023). A Robust Secure Access Entrance Method Based on Multi Model Biometric Credentials Iris and Finger Print. In Doriya, R., Soni, B., Shukla, A., Gao, XZ. (Eds.), Machine Learning, Image Processing, Network Security and Data Sciences. Lecture Notes in Electrical Engineering (pp. 315-331). (Vol. 946). Springer, Singapore. https://doi.org/10.1007/978-981-19-5868-7_24

Yang, A., Lu, C., Li, J., Huang, X., Ji, T., Li, X., & Sheng, Y. (2023). Application of meta-learning in cyberspace security: A survey. Digital Communications and Networks, 9(1), 67-78. https://doi.org/10.1016/j.dcan.2022.03.007

Yarmoliuk, O. (2022). Information support of enterprises: problems, challenges, prospects. Futurity Economics & Law, 2(1), 12–22. https://doi.org/10.57125/FEL.2022.03.25.02

Yi, H. (2023). Machine Learning Method with Applications in Hardware Security of Post-Quantum Cryptography. Journal of Grid Computing, 21(2), 19. https://doi.org/10.1007/s10723-023-09643-4

Zoppi, T., Ceccarelli, A., Puccetti, T., & Bondavalli, A. (2023). Which Algorithm can Detect Unknown Attacks? Comparison of Supervised, Unsupervised and Meta-Learning Algorithms for Intrusion Detection. Computers & Security, 127, 103107. https://doi.org/10.1016/j.cose.2023.103107

Zubaydi, H. D., Varga, P., & Molnár, S. (2023). Leveraging Blockchain Technology for Ensuring Security and Privacy Aspects in Internet of Things: A Systematic Literature Review. Sensors, 23(2), 788. https://doi.org/10.3390/s23020788