UDC 004.056:004.75
DOI https://doi.org/10.32782/IT/2024-4-9

Serhii DOROZHYNSKYI
PhD, Associate Professor at the Department of Cybersecurity, Information Technology and Economics, Dean of the Faculty of Information Technology and Social Sciences and Humanities, Kyiv University of Intellectual Property and Law of the National University «Odessa Law Academy», 210, Kharkivske highway, Kyiv, Ukraine, 02121, dorozhun1706@gmail.com
***ORCID:** 0000-0002-5395-6423*
***Scopus author ID:** 57222147991*

Vitaliy TUPKALO
Doctor of Technical Sciences, Professor, Professor at the Department of Cybersecurity, Information Technologies and Economics, Kyiv University of Intellectual Property and Law of the National University «Odessa Law Academy», 210, Kharkivske highway, Kyiv, Ukraine, 02121
***ORCID:** 0000-0002-6594-530X*

Yuriy SHCHERBYNA
Candidate of Technical Sciences, Associate Professor at the Department of Information Technologies, National University «Odessa Law Academy», Odessa, Ukraine, shcherbyna@onua.edu.ua
***ORCID:** 0000-0003-3885-6747*

To cite this article: Dorozhynskyi, S., Tupkalo, V., Shcherbyna, Yu. (2024). Vazhlyvi pytannia obrobky ta zakhystu danykh u dystrybutovanykh systemakh [Important issues of data processing and protection in distributed systems]. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 4, 68–74, doi: https://doi.org/10.32782/IT/2024-4-9

IMPORTANT ISSUES OF DATA PROCESSING AND PROTECTION IN DISTRIBUTED SYSTEMS

The purpose *of this article is to explore the critical aspects of big data processing in distributed networks as a contemporary challenge in ensuring cybersecurity. Special attention is given to issues of confidentiality, integrity, and availability of data in multi-user environments with high interaction complexity.*

The methodology *of the study involves a comprehensive approach, including the analysis of threats and vulnerabilities specific to distributed architectures such as cloud technologies, peer-to-peer networks, and decentralized infrastructures. Key issues such as asynchronous data access, limited computational resources, operation synchronization complexity, and risks of data interception during transmission are examined. The study evaluates modern cryptographic approaches, including homomorphic encryption, distributed key management mechanisms, and privacy-preserving protocols. Additionally, the application of machine learning and deep learning algorithms is explored for anomaly detection in system behavioral models in real-time.*

The scientific novelty *of the research lies in the systematization of threats and vulnerabilities inherent to distributed data processing systems and the development of effective approaches to neutralize them. For the first time, a comprehensive approach to the use of blockchain technologies is proposed as a means of ensuring transparent auditing of events and tracking transactions in distributed environments.*

The conclusions *provide practical recommendations for integrating modern cryptographic methods, distributed key management mechanisms, blockchain technologies, and machine learning algorithms to build resilient cybersecurity systems. The findings are of practical significance for ensuring the protection of big data in distributed networks and improving the effectiveness of responses to potential threats.*

Key words: *big data, distributed networks, cybersecurity, information protection, cryptography, homomorphic encryption, anomaly detection, machine learning, blockchain, risk management, privacy, data integrity, cloud technologies.*

Сергій ДОРОЖИНСЬКИЙ
PhD, доцент кафедри кібербезпеки, інформаційних технологій та економіки, декан факультету інформаційних технологій та соціально-гуманітарних наук, Київський університет інтелектуальної власності та права Національного університету «Одеська юридична академія», Харківське шосе, 210, м. Київ, Україна, 02121
***ORCID:** 0000-0002-5395-6423*
***Scopus Author ID:** 57222147991*

Віталій ТУПКАЛО
доктор технічних наук, професор, професор кафедри кібербезпеки, інформаційних технологій та економіки, Київський університет інтелектуальної власності та права Національного університету «Одеська юридична академія», Харківське шосе 210, м. Київ, Україна, 02121
***ORCID:** 0000-0002-6594-530X*

Юрій ЩЕРБИНА
кандидат технічних наук, доцент кафедри інформаційних технологій, Національний університет «Одеська юридична академія», Одеса, Україна, 02121
***ORCID:** 0000-0003-3885-6747*

Бібліографічний опис статті: Дорожинський, С., Тупкало, В., Щербина, Ю. (2024). Важливі питання обробки та захисту даних у дистрибутованих системах. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 4, 68–74, doi: https://doi.org/10.32782/IT/2024-4-9

ВАЖЛИВІ ПИТАННЯ ОБРОБКИ ТА ЗАХИСТУ ДАНИХ У ДИСТРИБУТОВАНИХ СИСТЕМАХ

***Метою статті** є дослідження критичних аспектів обробки великих даних у розподілених мережах як сучасного виклику забезпечення кібербезпеки. Особлива увага приділена проблемам конфіденційності, цілісності та доступності даних у багатокористувацьких середовищах із високим рівнем складності взаємодії.*

*У **методології** роботи застосовано комплексний підхід, що включає аналіз загроз і вразливостей, характерних для розподілених архітектур, таких як хмарні технології, однорангові мережі та децентралізовані інфраструктури. Розглянуто ключові проблеми, зокрема асинхронний доступ до даних, обмежені обчислювальні ресурси, складність синхронізації операцій і ризики перехоплення інформації під час передачі. Проведено аналіз сучасних криптографічних підходів, включаючи гомоморфне шифрування, механізми розподіленого управління ключами та протоколи збереження конфіденційності. Додатково досліджено алгоритми машинного та глибинного навчання для виявлення аномалій у поведінкових моделях систем у режимі реального часу.*

***Наукова новизна** роботи полягає у систематизації загроз та вразливостей, притаманних розподіленим системам обробки даних, і розробці ефективних підходів для їх нейтралізації. Вперше запропоновано комплексний підхід до використання блокчейн-технологій як засобу забезпечення прозорості аудиту подій і відстеження транзакцій у розподілених середовищах.*

*У **висновках** наведено практичні рекомендації щодо інтеграції сучасних криптографічних методів, механізмів розподіленого управління ключами, блокчейн-технологій та алгоритмів машинного навчання для побудови стійких до загроз кібербезпекових систем. Результати дослідження мають практичне значення для забезпечення захисту великих даних у розподілених мережах та підвищення ефективності реагування на потенційні загрози.*

***Ключові слова:** великі дані, розподілені мережі, кібербезпека, захист інформації, криптографія, гомоморфне шифрування, виявлення аномалій, машинне навчання, блокчейн, управління ризиками, конфіденційність, цілісність даних, хмарні технології.*

Introduction. In today's era of digital transformation, big data has become a key resource for organizations across industries. Distributed networks, such as cloud computing, peer-to-peer networks, and decentralized platforms, provide scalability, accessibility, and efficiency in processing this data. However, the growth in the volume of information and its criticality is accompanied by the emergence of new threats to its security, due to the dynamism of distributed environments, asymmetry of computing power, and the complexity of integrating various system components.

Cyberattacks aimed at compromising the confidentiality, integrity and availability of data pose a particular danger. Vulnerabilities in network infrastructure, unreliable data transmission protocols, and flaws in data access systems create favorable conditions for attacks. In particular, attackers use the specifics of distributed networks to launch denial-of-service (DDoS) attacks, steal data and unauthorized modification. In addition, the problem is complicated by the requirements for real-time data processing speed, which imposes restrictions on the use of traditional security methods that are too resource-intensive. In this context, it is critical to develop effective, scalable and adaptive security mechanisms that take into account the specifics of big data and distributed network architectures.

The purpose of the article is to identify, analyze, and develop effective methods and approaches to ensuring the protection of big data in distributed networks that take into account the

specifics of such environments, in particular their dynamism, asynchrony, and scalability.

To achieve this goal, the following **main tasks** have been set:

1. To review and systematize the current threats arising from the processing of big data in distributed networks, with a focus on the problems of confidentiality, integrity and availability of information.

2. Investigate existing cryptographic security methods, their effectiveness and adaptability to distributed environments.

3. To develop and analyze threat detection algorithms using machine learning technologies, in particular deep learning, to identify anomalies in real time.

4. Evaluate the potential of blockchain technologies to ensure the security of big data in distributed networks, in particular for event auditing and transaction tracing.

One of the key challenges in securing big data in distributed networks is the need to balance the efficiency of information processing with its protection. Multi-user environments are often characterized by high dynamic data access, which makes it difficult to manage access rights, ensure transparency of operations, and prevent unauthorized interference. In addition, the nature of big data processing requires the integration of various technologies, such as containerization, compute orchestration, and workflow automation, which increases the number of possible vulnerabilities.

Of particular importance are the problems of ensuring data integrity, when changing even a small part of the information can lead to significant disruptions in the system's functioning or to the appearance of unreliable results. At the same time, the need for fast real-time data processing makes it difficult to implement comprehensive security checks at every stage of computing.

Modern challenges also relate to the unification of security protocols and standards in the context of the globalization of the information space. Distributed networks often span multiple jurisdictions with different laws and regulatory requirements, making it difficult to create universal approaches to data protection. The issue of system compatibility and ensuring their uninterrupted functioning in the event of threats or attacks is another important aspect.

Another challenge is the development of decentralized platforms where data processing takes place without clear centralized control. In such systems, there is a growing risk of disagreements between participants, distrust in the results of data processing, and the spread of manipulation in transactions. These challenges emphasize the need to develop not only technical solutions but also regulatory and organizational approaches that ensure comprehensive protection of big data in distributed environments.

Threats to big data in distributed networks can be categorized into three main aspects: confidentiality, integrity, and availability, which form the basic triad of cybersecurity – the CIA model. Each of these aspects has its own specific threat characteristics and consequences.

Confidentiality means ensuring that only authorized entities have access to data. The formalization of a confidentiality breach can be described by the formula:

$$B(C) = P(U_i \in U_a),$$

where U_i – access subject, U_a – set of authorized entities, P – the possibility of unauthorized access. The main types of privacy attacks are information interception and metadata analysis, including man-in-the-middle attacks and attacks on encrypted data channels.

Integrity ensures the integrity and accuracy of data during its processing, storage, or transmission. A breach of integrity can be expressed by the following formula:

$$B(I) = \exists x_i, x_j \in D, x_i \neq x_j, h(x_i) \neq h(j),$$

where D – dataset, $h(x)$ – a hash function used for data verification. Integrity threats include unauthorized data modification and data injection. In particular, data overwriting attacks affect critical systems, reducing their reliability.

Availability means ensuring that data and resources can be legally accessed at any time. An availability violation is described by the following formula:

$$B(A) = \frac{D_t}{T_t} > \delta,$$

where δ – acceptable level of downtime, D_t – system unavailability time, T_t – total system operation time.

Classification of threats by sources and methods of attack

Threats to big data in distributed networks can be categorized according to various attributes, including attack sources and methods. Defining these categories allows you to create more accurate models for protecting and responding to threats. The main sources of threats are internal and external attacks, as well as unauthorized use of resources. Attack methods can be divided into attack and exploitation methods used to violate each of the security aspects: confidentiality, integrity, and availability.

This classification allows us to take into account not only the types of attacks, but also their sources, which allows us to create more flexible and effective defense strategies. For example, to combat internal threats, it is necessary to apply strict control over access to data and monitor user activity. For external threats, such as DDoS attacks, it is necessary to use traffic filtering and network-level protection methods. In addition, developing methods to quickly identify fake certificates or attack verification mechanisms will be an important step in ensuring security in the face of the constant development of attack techniques.

To effectively protect big data in distributed networks, it is necessary to implement comprehensive methods focused on ensuring confidentiality, integrity, and availability. These methods should take into account the specifics of distributed environments, such as decentralized access, a large number of entry points, and high volumes of data to be processed.

Confidentiality protection is aimed at protecting information from unauthorized access. The main methods are:

1. Data encryption, where symmetric (AES) and asymmetric algorithms (RSA, ECC) are used to protect confidentiality. The encryption process can be described by the formula:

$$C = E_k(P),$$

where C – ciphertext, P – plain text, E_k – encryption function with a key.

2. Data anonymization, where techniques such as differential privacy add noise to the data to preserve user privacy.

3. Access control, where multi-level policies, such as Role-Based Access Control, are implemented.

Data integrity ensures that information remains unchanged and reliable. The main methods:

- Hashing – uses algorithms such as SHA-256 to verify changes to data.
- Digital signatures – provide authentication of the data source using asymmetric encryption.
- Version control – storing previous versions of data to ensure that it can be restored after modification.

Data availability guarantees continuous access to information, even in the event of a threat. The main methods:

- Distributed storage – the use of systems such as RAID or decentralized networks that guarantee data redundancy:
- Protection against DDoS attacks – the use of traffic filtering mechanisms, for example, through content delivery networks (CDNs).
- Backup automation – regular backups for quick recovery in case of loss.

These methods should interact in a single system to provide a full range of data protection. For example, encryption guarantees confidentiality, but digital signatures or hashing are required to verify data.

Distributed networks that process large amounts of data are characterized by a number of specific features that significantly affect the implementation and effectiveness of information security methods. These features include a geographically distributed structure, high dynamics of the network topology, a large amount of processed data, and a multi-user environment.

Table 1

Classification of threats by sources and methods of attack

Threat category	Threat source	Attack methods	Attack goals	Attack example
Internal threats	Employees or users of the system	1.Illegal access to data 2.Modification of data without authorization	Confidentiality Integrity	Insider attacks Data leakage
External threats	External attackers or organizations	Man-in-the-middle or distributed denial of service attacks	Confidentiality Integrity Availability	DDoS attacks Data interception
Threats from technology	Software and hardware vulnerabilities	Exploitation of OS or software vulnerabilities; Exploitation of flaws in network protocols	Confidentiality Integrity Availability	Database hacking; Network attacks
Variable threats	Attacks on verification mechanisms	Fake certificates or metadata tampering; Attacks on identity systems	Confidentiality Integrity	Forgery of digital signatures; Use of fake certificates
Threats caused by external factors	**Unforeseen circumstances**	**Natural disasters; Energy losses**	**Availability**	**Loss of access to data due to natural disasters**

One of the key features is **decentralization**, which creates additional challenges for access control and security monitoring. Distributed networks do not have a single data center, which makes it difficult to use traditional centralized security systems. In such conditions, it is necessary to use methods that allow you to dynamically adapt access policies depending on changes in the network topology. For example, role-based and attribute-based access control systems should provide a quick response to changes in user roles or resource status in real time. It is also important to ensure effective protection in terms of scalability. Big data processing requires computing resources that far exceed the capabilities of traditional cybersecurity approaches. Therefore, modern security methods must take into account the limitations of computing power, network bandwidth, and processing delays. This leads to a growing demand for lightweight cryptographic algorithms, data compression methods, and traffic flow optimization that minimize the impact on system performance. Another feature is the increased vulnerability to attacks due to the multi-user environment. The interaction of numerous users and devices in a distributed network creates risks to data confidentiality and integrity. These risks can be mitigated by using multi-level encryption, mandatory multi-factor authentication, and integrating intrusion detection systems with machine learning to analyze anomalies in user behavior. An important challenge is to ensure uninterrupted data availability in distributed storage networks. In such systems, any damage or failure of individual nodes should not affect the functioning of the entire network. This is achieved through data redundancy, regular backups, and the implementation of auto-checking and self-healing mechanisms.

Distributed computing is the fundamental basis for working with big data, as it provides parallel processing of information, optimized resource utilization, and scalability of systems. However, this architecture imposes significant requirements and creates new challenges for building data protection systems. They are characterized by a large number of nodes that can be geographically distributed. This requires the implementation of decentralized security systems that can operate without centralized control. In particular, such systems use blockchain, which provides reliable verification of transactions, or cryptographic algorithms that allow the exchange of keys without the need for centralized trusted parties.

The second critical aspect is the scalability of the security architecture. Security systems must be able to dynamically expand to handle growing data volumes and the number of requests. In such an environment, traditional encryption and authentication methods may not be effective due to processing delays. This requires the use of lightweight protocols, such as elliptic curve cryptography, as well as the integration of artificial intelligence-based threat detection methods. In addition, distributed computing creates risks associated with infrastructure heterogeneity. In most cases, distributed systems consist of nodes running on different platforms and using different technologies. This increases the likelihood of exploiting compatibility vulnerabilities in system components. To solve this problem, it is necessary to implement standardized security protocols and mutual authentication mechanisms between nodes. It is also important to manage access to resources in a distributed architecture. Due to the large number of users and requests, there is a risk of system overload and an increased likelihood of attacks such as DDoS. To prevent this, access restriction policies, load balancing between nodes, and dynamic resource scaling are used. Another challenge is to ensure transparency and control over security in distributed computing. Дntegrated monitoring systems are used to analyze the behavior of nodes and requests in real time. Such systems are able to automatically detect anomalies that may indicate a possible attack and take measures to neutralize it.

Effective protection of big data in distributed networks requires the implementation of modern monitoring and threat detection systems that can operate in real time, given the dynamic nature of such networks. These systems are based on analyzing large volumes of traffic, detecting anomalies in the behavior of users and network nodes, and being able to respond quickly to security incidents.

One of the main components of modern monitoring systems is mechanisms for collecting and analyzing telemetry data from all network nodes. In distributed networks, these mechanisms must be decentralized and scalable to process data from many sources simultaneously. Streaming data processing technologies, such as Apache Kafka or Apache Flink, play an important role in this, allowing for efficient real-time processing of events. Threat detection systems, in turn, use machine learning and artificial intelligence algorithms to analyze anomalies. For example, clustering methods or neural networks to detect complex patterns in behavior. These algorithms allow not only to identify threats that match known attack patterns, but also to predict potentially new types of attacks that have no historical analogues.

Integrating monitoring with incident response tools is also an important aspect. Systems such as SIEM automate detection and response processes,

providing analytical information for security operators. For example, if suspicious activity is detected in network traffic, the system can automatically isolate the host or block access, preventing the threat from spreading. Another critical component is ensuring transparency of the monitoring system's actions for administrators. This is achieved by building a multi-level data visualization system that allows you to get an idea of the network status and possible threats. The use of graphical interfaces, for example, based on systems such as Kibana, facilitates data analysis even on a large scale. The importance of protecting the monitoring systems themselves, which also become a target for attackers, should be noted separately. For this purpose, methods of protection against man-in-the-middle attacks, multi-level encryption of telemetry data, and the use of containerization technologies to isolate components are being implemented.

Integrating security into the architecture of distributed networks is a key aspect of big data security. This process requires taking into account the specifics of distributed environments, such as decentralization, infrastructure heterogeneity, and the dynamic nature of data flows. An integrated approach to integration should provide protection at all levels of the architecture, including the infrastructure, network, and application layers.

At the infrastructure level, isolation and segmentation technologies are implemented to minimize the risks of threats spreading in the event of compromise of individual nodes. For example, the use of virtualization and containerization (Docker, Kubernetes) provides logical isolation of processes and execution environments. This makes it impossible for an attacker to access other system components even if an attack on a single node is successful.

At the network level, the integration of security means involves the implementation of mechanisms for encrypting data transmission channels (for example, TLS/SSL protocols) and protection against attacks at the routing level (for example, BGP-Sec). It is also important to use network segmentation using virtual local area networks (VLANs) to limit the interaction between different groups of nodes. Distributed systems are increasingly using software-defined networks (SDN), which provide centralized control and adaptation of security policies to dynamic changes in the network.

At the application level, integration includes the implementation of multi-factor authentication, role-based and attribute-based access control models, as well as control and audit tools. The uniqueness of distributed environments requires these mechanisms to be highly adaptive: they must take into account the distribution of resources and ensure policy consistency across different nodes. For example, when a user's role changes, the access policy should be automatically updated across all system components.

Automation is of particular importance for security integration. In distributed networks, large amounts of data and high process dynamics make manual security management difficult. Therefore, the integration of automated systems, such as SOAR (Security Orchestration, Automation, and Response), allows you to automatically respond to security incidents. For example, if abnormal activity is detected on a particular node, the system can initiate isolation of that node, change access policies, or redirect traffic to other nodes. Another important component is the integration of self-diagnostic and self-healing mechanisms. This allows the system to proactively detect vulnerabilities, check the compliance of settings with modern security standards, and automatically restore functionality in the event of a failure. For example, the use of data replication and consensus mechanisms (RAFT, Paxos) in distributed data warehouses guarantees their availability even if some nodes are lost.

Conclusions. The article investigates the critical aspects of big data processing in distributed networks, taking into account the challenges associated with ensuring their protection. By analyzing modern methods of data processing, monitoring and protection, it is established that distributed systems are an important component of big data infrastructure, but their decentralization, scalability and dynamic nature significantly complicate the construction of effective security systems. In particular, the structure of distributed networks, characterized by geographical remoteness of nodes, heterogeneity of execution environments, and high traffic intensity, imposes additional requirements for security tools. The study determined that traditional approaches to ensuring the confidentiality, integrity, and availability of information are becoming insufficient, especially in the context of system scaling. In this regard, it is proposed to use lightweight cryptographic algorithms, in particular elliptic curve cryptography, and blockchain technologies for decentralized data storage and transaction verification. Threat monitoring and incident management are critical to protecting big data in distributed networks. We propose to integrate real-time data analysis mechanisms, use artificial intelligence to detect anomalies, and automate response processes. Systems such as SIEM and SOAR, which are focused on automatically performing threat prevention operations, have proven effective in reducing response times and minimizing the impact of

incidents on system functionality. Integration of security tools into the architecture of distributed networks should take into account a multi-level approach. At the infrastructure level, it is recommended to use node isolation through virtualization and containerization. At the network level, the use of software-defined networks (SDN) allows you to dynamically adapt security policies to changes in topology. At the application level, it is important to implement multi-factor authentication, adaptive access control, and audit mechanisms. A high level of automation of security processes is a mandatory component of modern systems. The introduction of self-healing technologies and self-diagnostic mechanisms allows for a proactive approach to eliminating threats. Data replication and consensus tools, such as RAFT and Paxos, ensure data availability and integrity even in the event of the loss of individual nodes. The study results confirm that effective protection of big data in distributed networks is only possible with the use of innovative technologies, adaptive methods, and an integrated approach to security. Integration of advanced technologies such as blockchain, artificial intelligence, software-defined networks, and automated incident management systems are key to creating resilient and dynamic security systems that meet the demands of modern information environments.

BIBLIOGRAPHY:

1. M. S. Rahman and H. Reza, «A Systematic Review Towards Big Data Analytics in Social Media,» in Big Data Mining and Analytics, vol. 5, no. 3, pp. 228–244, September 2022, doi: 10.26599/BDMA.2022.9020009.

2. D. Syed, A. Zainab, A. Ghrayeb, S. S. Refaat, H. Abu-Rub and O. Bouhali, «Smart Grid Big Data Analytics: Survey of Technologies, Techniques, and Applications,» in IEEE Access, vol. 9, pp. 59564–59585, 2021, doi: 10.1109/ACCESS.2020.3041178.

3. X. Sun, Y. He, D. Wu and J. Z. Huang, «Survey of Distributed Computing Frameworks for Supporting Big Data Analysis,» in Big Data Mining and Analytics, vol. 6, no. 2, pp. 154–169, June 2023, doi: 10.26599/BDMA.2022.9020014.

4. J. Liao and J. Lin, «A Distributed Deep Reinforcement Learning Approach for Reactive Power Optimization of Distribution Networks», в IEEE Access, vol. 12, p. 113898–113909, 2024, doi: 10.1109/ACCESS.2024.3445143.

5. D. Park, S. Kang and C. Joo, «A learning-based distributed algorithm for scheduling in multi-hop wireless networks,» *Journal of Communications and Networks*, vol. 24, no. 1, pp. 99–110, Feb. 2022, doi: 10.23919/JCN.2021.000030.

6. M. W. S. Atman and A. Gusrialdi, «Finite-Time Distributed Algorithms for Verifying and Ensuring Strong Connectivity of Directed Networks,» in IEEE Transactions on Network Science and Engineering, vol. 9, no. 6, pp. 4379–4392, 1 Nov. -Dec. 2022, doi: 10.1109/TNSE.2022.3200466.

7. T. Lenard, A. Collen, M. Benyahya, N. A. Nijdam and B. Genge, «Exploring Trust Modeling and Management Techniques in the Context of Distributed Wireless Networks: A Literature Review,» in IEEE Access, vol. 11, pp. 106803–106832, 2023, doi: 10.1109/ACCESS.2023.3320945.

REFERENCES:

1. Rahman, M. S., & Reza, H. (2022). A systematic review towards big data analytics in social media. Big Data Mining and Analytics, 5(3), 228–244. https://doi.org/10.26599/BDMA.2022.9020009

2. Syed, D., Zainab, A., Ghrayeb, A., Refaat, S. S., Abu-Rub, H., & Bouhali, O. (2021). Smart grid big data analytics: Survey of technologies, techniques, and applications. IEEE Access, 9, 59564–59585. https://doi.org/10.1109/ACCESS.2020.3041178

3. Sun, X., He, Y., Wu, D., & Huang, J. Z. (2023). Survey of distributed computing frameworks for supporting big data analysis. Big Data Mining and Analytics, 6(2), 154–169. https://doi.org/10.26599/BDMA.2022.9020014

4. Liao, J., & Lin, J. (2024). A distributed deep reinforcement learning approach for reactive power optimization of distribution networks. IEEE Access, 12, 113898–113909. https://doi.org/10.1109/ACCESS.2024.3445143.

5. Park, D., Kang, S., & Joo, C. (2022). A learning-based distributed algorithm for scheduling in multi-hop wireless networks. *Journal of Communications and Networks*, 24(1), 99–110. https://doi.org/10.23919/JCN.2021.000030

6. Atman, M. W. S., & Gusrialdi, A. (2022). Finite-time distributed algorithms for verifying and ensuring strong connectivity of directed networks. IEEE Transactions on Network Science and Engineering, 9(6), 4379–4392. https://doi.org/10.1109/TNSE.2022.3200466

7. Lenard, T., Collen, A., Benyahya, M., Nijdam, N. A., & Genge, B. (2023). Exploring trust modeling and management techniques in the context of distributed wireless networks: A literature review. IEEE Access, 11, 106803–106832. https://doi.org/10.1109/ACCESS.2023.3320945