Enhancing IoT systems through Cloud-Fog-Edge architectures challenges and opportunities

Anna Kalyashina[1,2*], *Yuri* Smirnov[2], *Valeriy* Esov[3], *Maxim* Kuznetsov[4,5], and *Oksana* Dmitrieva[4]

[1]Kazan National Research Technical University named after A. N. Tupolev – KAI, Kazan, Russia
[2]Kazan State Power Engineering University, Kazan, Russia
[3]Bauman Moscow State Technical University, Moscow, Russia
[4]Kazan National Research Technological University, Kazan, Russia
[5]Kazan State Agrarian University, Kazan, Russia

Abstract. This article examines the deployment and implications of Cloud-Fog-Edge architectures in Internet of Things (IoT) systems, highlighting their significance in enhancing data management and system security across diverse sectors. As IoT ecosystems expand, the necessity for architectures that efficiently handle large volumes of data and ensure real-time processing capabilities becomes paramount. The Cloud-Fog-Edge architecture addresses these needs by distributing computing resources across three layers—cloud, fog, and edge—each optimized for specific tasks within the IoT workflow. We discuss the challenges and solutions associated with interoperability in such multi-layered systems, emphasizing the need for standardized communication protocols and data formats to facilitate seamless interactions between heterogeneous devices and platforms. Furthermore, the article delves into the critical aspects of security within these architectures, outlining strategies for robust data encryption, access management, regular security updates, and comprehensive network activity monitoring to safeguard against unauthorized access and cyber threats. The integration of Cloud-Fog-Edge architectures not only promises enhanced operational efficiency and scalability but also significantly boosts the adaptability of IoT systems to meet evolving technological and operational demands. By providing a detailed analysis of the functionalities, integration challenges, and security practices associated with each architectural layer, this article contributes to a deeper understanding of how Cloud-Fog-Edge frameworks can be optimized to bolster the reliability, efficiency, and security of modern IoT environments.

1 Introduction

The Internet of Things, a linchpin in the era of digital transformation, profoundly influences multiple sectors by revolutionizing smart cities, industrial operations, healthcare, and more. As IoT expands, the burgeoning number of connected devices coupled with escalating demands for quick data processing necessitates innovative architectural solutions. Among

* Corresponding author: anna_vik@mail.ru

these solutions, the Cloud-Fog-Edge architecture stands out, providing a unique mechanism for efficient data handling. This architecture not only enhances system performance and scalability but also fortifies security—a critical concern amidst the rising tide of cyber threats.

Traditional cloud computing architectures struggle to meet the latency and processing needs at the network's edge, particularly as IoT devices proliferate globally. The latency in data transfer from IoT devices to the cloud and back can hinder real-time data analysis and operational responsiveness. This lag is untenable in sectors where real-time data processing is crucial, such as in automated manufacturing processes or emergency healthcare services [1,2].

The Cloud-Fog-Edge architecture addresses these challenges by decentralizing data processing. In this tri-layered architecture, data tasks are distributed strategically across the cloud, intermediate fog nodes, and edge devices [3]. This structure reduces the distance data must travel for processing, thereby decreasing latency significantly.

The Cloud-Fog-Edge architecture's efficacy is further enhanced through the integration of advanced technologies like Software-Defined Networking (SDN) and Network Functions Virtualization (NFV). SDN provides flexible control over network resources, allowing for real-time adjustments based on data flow needs [4,5]. NFV contributes by virtualizing network functions, which were traditionally bound to hardware, thus reducing costs and improving scalability and agility.

Security in IoT systems is paramount, given the sensitivity of data and the potential repercussions of breaches. The Cloud-Fog-Edge architecture leverages its distributed nature to enhance security protocols [6,7]. By processing data locally on edge devices or fog nodes, the architecture minimizes the amount of data transmitted over the network, thus reducing exposure to cyber threats [8]. Furthermore, SDN and NFV enable more granular security controls, improving the ability to detect and respond to anomalies at different network layers.

The Cloud-Fog-Edge architecture facilitates new models of data management where all levels—from the edge to the cloud—collaborate to perform data processing tasks. This collaborative approach not only minimizes latency but also optimizes resource usage, enhancing the efficiency and responsiveness of IoT systems [9,10].

The Cloud-Fog-Edge architecture represents a transformative approach to managing the data deluge in IoT environments. By reducing latency, enhancing security, and improving scalability, this architecture equips IoT platforms to be more adaptive and capable of meeting the diverse needs of modern industries [11]. As this architecture continues to evolve, it promises to unlock new potentials in IoT applications, from industrial internet applications to smart city infrastructures and beyond.

2 Detailed exploration of Cloud-Fog-Edge architectures in IoT systems

This research delves deeply into the architectures known as Cloud-Fog-Edge, which are instrumental in managing data efficiently within Internet of Things systems. These architectures are crucial for addressing the complexities associated with large-scale, real-time data processing across various IoT applications [12,13]. The study is specifically focused on understanding the interactions among the different architectural layers, evaluating their functionality, scalability, adaptability, and overall impact on the performance and security of IoT systems [14].

The cloud layer functions as the central repository for data storage and conducts intensive computational processes. It is essential for supporting advanced analytics, long-term data management, and other resource-intensive tasks that are impractical at the edge. However, this layer often struggles with issues like latency and high bandwidth costs due to its physical distance from the data sources [15,16]. Centralized data processing also raises significant concerns regarding privacy and data sovereignty.

Moving closer to the data source, the fog layer acts as an intermediary, offering semi-localized processing capabilities. This layer provides services such as local data aggregation, preliminary analytics, and temporary storage, which helps reduce the load on the cloud and decreases response times. Despite its benefits, the fog layer introduces complexity in managing the semi-distributed fog nodes and poses challenges in ensuring security and consistency across these nodes [17,18].

At the closest point to the data source, the edge layer processes data directly at or near where it is generated. This is crucial for supporting real-time applications by providing immediate insights and actions, which is especially important in latency-sensitive applications such as autonomous driving and industrial automation. However, the edge layer has its limitations, including lesser processing power and storage capacity compared to the cloud and fog layers [19]. Additionally, securing the numerous edge devices can be problematic due to their accessibility and exposure to local environments.

The interaction and integration of these layers provide a cohesive system architecture that is examined in this study. The research looks into how data moves between layers and how processing tasks are allocated based on the nature of the data and the required response times. It also analyzes the mechanisms in place for scaling resources and balancing the load between the cloud, fog, and edge layers to optimize performance and cost efficiency. The adaptability of the system to changes in network connectivity, device mobility, and fluctuations in data volume and velocity is another critical area of focus [20,21].

The study assesses how the architecture supports high throughput and low latency, which are essential for the effective functioning of IoT applications. Additionally, the security measures implemented across the layers, including data encryption, access control, and threat detection strategies, are thoroughly examined [22]. The research pays particular attention to maintaining security when data is processed and stored across multiple, potentially unsecured, nodes.

The theoretical contributions of this study provide deeper insights into distributed computing paradigms, enhancing the understanding of decentralized data processing frameworks. Practically, the study offers guidelines for designing IoT systems that require robust, scalable, and secure architectures, which are applicable in diverse fields such as healthcare, industrial IoT, and smart cities [23].

This comprehensive analysis aims to shed light on the operational dynamics of Cloud-Fog-Edge architectures, highlighting their potential to enhance the efficiency, scalability, and security of IoT systems. By detailing the functionalities, integration challenges, and security practices of each layer, the research contributes valuable knowledge to the field of IoT architecture development.

3 Enhancing IoT systems through layered integration

The Cloud-Fog-Edge architecture introduces a nuanced, three-tiered framework specifically engineered to amplify the data processing and management capabilities within Internet of Things systems. This architecture is strategically designed to foster enhanced system flexibility, scalability, and efficiency through its distinct operational layers: the cloud, the fog, and the edge [24,25]. Each layer is integral to the architecture, playing a unique role in handling data and operational processes which collectively improve the overall performance and security of IoT infrastructures.

At the pinnacle of this architecture sits the cloud layer, which provides the foundational computing and storage facilities necessary for extensive data analysis and long-term data retention. The cloud serves as a central node that synthesizes and manages data coming from all connected devices. Its robust infrastructure is designed to support high-volume data processing and complex computational demands, ensuring data is handled securely and efficiently. Moreover, the cloud's powerful analytics engines help in deriving valuable insights from vast amounts of data, which are crucial for strategic decision-making and long-term planning in IoT operations [26].

The fog layer acts as an essential intermediary, positioned between the edge devices and the cloud. This layer provides a crucial buffer that processes data incoming from the edge, thus alleviating the burden on the cloud by pre-processing data before it reaches the central servers. This not only reduces latency but also optimizes network and computational resources [27,28]. The fog layer is capable of performing significant analytics and making decisions in near-real time, which is vital for operations requiring swift responses. By processing data closer to the source, the fog enhances the responsiveness and agility of IoT systems, enabling more dynamic and efficient operational workflows.

Directly interfacing with the physical world through IoT devices, the edge layer represents the front line of data processing. Located at or near the data source, the edge processes data in real time, crucial for immediate decision-making and action. This capability is particularly important in environments where even minimal delays can lead to critical failures, such as in manufacturing automation or emergency response systems [29]. The edge layer's primary function is to filter and process data locally, which significantly reduces the data transmission requirements and bandwidth usage, thereby minimizing the latency further.

The seamless integration of cloud, fog, and edge layers forms a comprehensive system that optimizes data flow across different levels, enhancing the overall performance and scalability of IoT systems [30,31]. This integration allows for a more refined control over data processing tasks, distributing them across the layers based on complexity and urgency. For example, simple data validation and filtering can occur at the edge, more complex data aggregation and initial analysis can happen in the fog, and intensive data processing and long-term storage can be managed in the cloud.

This layered approach not only improves data management efficiency but also strengthens the security posture of the entire IoT ecosystem. By decentralizing the data processing points, the architecture reduces the risk of systemic failures and security breaches. Each layer can implement tailored security measures suitable for its operational scope and risk profile, thereby enhancing the overall system's resilience against cyber threats [32].

The Cloud-Fog-Edge architecture represents a strategic evolution in how data is processed and managed in IoT systems. By effectively distributing computing tasks across three distinct layers, this architecture addresses the critical challenges of latency, system scalability, and security in IoT environments. It ensures that IoT platforms are not only more responsive and efficient but also better equipped to handle the increasing complexities of modern digital ecosystems [33,34]. This layered architectural model is set to play a pivotal role in shaping the future of IoT deployment across various industries, enhancing capabilities in real-time data processing and decision-making.

4 SDN and NFV technologies in IoT

The integration of Software-Defined Networking and Network Functions Virtualization technologies significantly advances the management and efficiency of multi-layered Cloud-Fog-Edge architectures in Internet of Things systems. These innovative technologies enable crucial approaches to network resource management, which are essential for ensuring high performance and adaptability in modern IoT systems [35,36].

Software-Defined Networking represents a transformative approach to network management that emphasizes flexibility and centralized control. By decoupling the network's control functions from the physical hardware, SDN allows network managers to dynamically

 https://doi.org/10.1051/e3sconf/202458306012

adjust network behavior from a centralized console (see Fig.) [37]. This capability is instrumental in optimizing network resource usage and reducing response times across vast and complex IoT networks. With SDN, real-time traffic management becomes feasible, enabling the network to reroute traffic based on current conditions and priorities, which significantly reduces latency and enhances the performance of critical IoT applications. Moreover, the centralized control model of SDN enables quicker responses to security threats [38,39], allowing immediate deployment of security measures and network-wide policy updates. SDN simplifies network operations and reduces operational costs by automating tasks that traditionally require manual configuration [40], allowing networks to scale effectively and adapt to changing traffic patterns or application requirements with minimal human intervention.

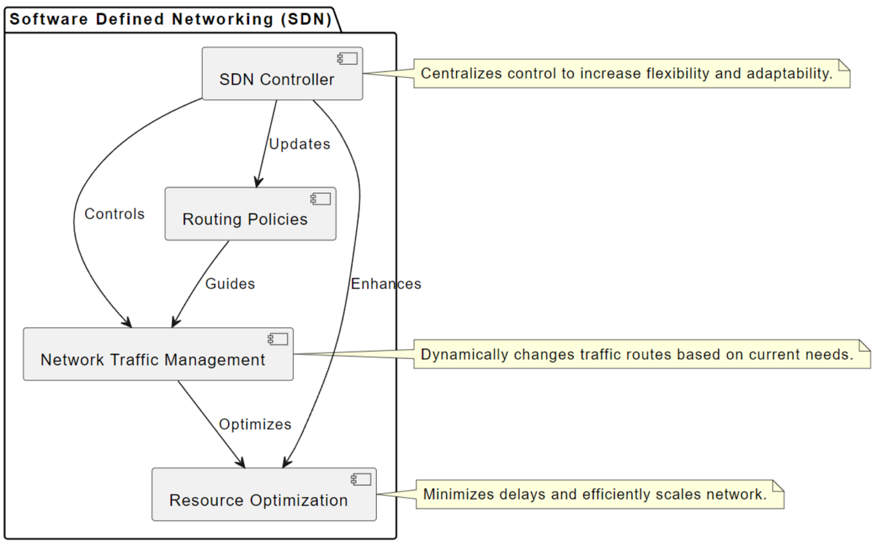

Fig. Component diagram of software-defined networks.

Network Functions Virtualization enhances network scalability and agility by virtualizing network services that were traditionally carried out on dedicated hardware. This shift facilitates the deployment of network services such as firewalls, load balancers, and network address translation on virtual machines running on standard commercial hardware. The virtualization of network functions through NFV reduces the capital and operational expenditures associated with purchasing and maintaining proprietary equipment. It increases flexibility and scalability as virtualized functions can be rapidly adjusted to meet changing demand without physical alterations to the network infrastructure. NFV also enables network managers to deploy new services quickly, adapt to new business requirements, and innovate with fewer constraints imposed by physical network configurations.

The combination of NFV with SDN can further enhance network management in IoT environments by providing a comprehensive and flexible approach to handling network traffic and services dynamically. This integration optimizes resource allocation and operational efficiency by using SDN to intelligently route traffic and NFV to efficiently manage network functions. Enhanced reliability and service continuity are also benefits of NFV's ability to replicate network functions across multiple virtualized environments, ensuring that network services can remain operational even if individual components fail [41,42].

SDN and NFV are cornerstone technologies that significantly enhance the operational capabilities of Cloud-Fog-Edge architectures in IoT systems. By offering unparalleled control, flexibility, and efficiency in network management, these technologies are essential for supporting the increasingly complex and dynamic nature of IoT environments. As IoT systems continue to expand and evolve, the strategic deployment of SDN and NFV will be crucial in ensuring these systems are both resilient and capable of adapting to new technological challenges and operational demands.

5 Interoperability challenges in Cloud-Fog-Edge architectures

Interoperability is a critical challenge in the implementation of Cloud-Fog-Edge architectures within the Internet of Things ecosystems. This issue arises from the need to integrate numerous devices and systems that span multiple layers—cloud, fog, and edge—which often come from different manufacturers and use diverse technologies. Achieving interoperability involves enabling these various elements to communicate and coordinate seamlessly without human intervention, which is essential for the functionality [43], efficiency, and scalability of IoT systems. Without strong interoperability, the IoT ecosystem risks fragmentation, which can disrupt the seamless flow of information, reduce system performance, and expose the network to security vulnerabilities [44,45].

The challenge intensifies due to the inherent diversity in device hardware, operating systems, and application environments within each architectural layer. The cloud layer is designed for heavy data processing and storage, the fog layer provides mid-level processing and quicker response times, and the edge layer handles immediate, real-time processing close to data sources [46]. Ensuring that these diverse layers work together effectively requires a concerted effort to standardize communication protocols and data formats across the entire system.

Standardization is crucial for overcoming these interoperability issues. It entails setting universal specifications that all devices, regardless of their origin or technology, can adhere to. By standardizing communication protocols, we ensure that messages sent from one device are accurately received and understood by another, facilitating coherent and reliable data exchange [47,48]. Similarly, standardizing data formats ensures that data shared across systems is interpretable and usable by all entities involved, which is vital for analytics and decision-making processes.

To achieve effective standardization, several steps are necessary. Developing universal protocols requires the involvement of industry consortia and standards organizations that can create and enforce guidelines that dictate how devices should communicate. These protocols must be robust, secure, and adaptable to future technological advancements. Alongside communication standards, it is also necessary to establish common data formats that allow for the accurate aggregation and interpretation of data from various sources. This standardization of data requires a collaborative approach to define data schemas that are universally acceptable and capable of handling the diverse range of data types generated by IoT devices [49].

Moreover, standardization includes the development of common security protocols that protect the integrity and confidentiality of data across all layers of the architecture. Given that IoT systems often manage sensitive information, maintaining high standards of security and privacy across a range of devices is crucial. Finally, promoting cross-vendor collaboration is essential for the widespread adoption of these standards. Manufacturers and developers must work together to ensure their products comply with these standards, which can be facilitated through certification programs and regular audits [50,51].

Achieving interoperability in Cloud-Fog-Edge architectures is fundamental to creating a seamless, efficient, and secure IoT environment. By focusing on the standardization of communication protocols and data formats, we can enhance system stability, improve security, and facilitate the integration of diverse technologies [52,53]. This approach not only reduces costs by decreasing the need for customized integration efforts but also accelerates the deployment of new IoT solutions. As the IoT landscape continues to evolve, interoperability will remain a cornerstone of technological progress, requiring ongoing collaboration and innovation from all stakeholders involved.

6 Security in Cloud-Fog-Edge architectures

In the Internet of Things ecosystem, where systems and data are constantly exposed to risks such as unauthorized access and cyber-attacks, ensuring robust security across all layers of the Cloud-Fog-Edge architecture is critically necessary. The architecture's dynamic and distributed nature introduces unique security challenges that require comprehensive strategies to protect data integrity, maintain privacy, and ensure system availability.

Security in multi-layered IoT architectures involves a variety of measures tailored to address the specific vulnerabilities associated with each layer: cloud, fog, and edge. Data encryption is central to securing any IoT system and must be implemented at every stage—from the edge devices through the fog nodes to the cloud. This ensures that data remains encrypted during both transmission and storage, safeguarding it against eavesdropping and tampering by malicious entities. Utilizing modern encryption algorithms and protocols is essential to maintain data confidentiality and integrity across different networks.

Effective management of access to IoT systems is crucial for preventing unauthorized entry and data breaches. This involves implementing rigorous authentication mechanisms and detailed authorization protocols to control who can access specific data and when. Employing multi-factor authentication, role-based access control, and the use of complex, regularly updated passwords helps minimize the risk of unauthorized access. Additionally, policies must be regularly reviewed and updated to adapt to new security challenges and compliance requirements.

Regular updates and patches are essential to counteract the exploitation of software vulnerabilities. IoT devices and systems often have longer operational lifetimes, making continuous software support and frequent security patches critical. Automating these updates where possible can reduce the burden on system administrators and decrease the likelihood of human error.

Monitoring network traffic for unusual or suspicious patterns is critical for the early detection of potential security threats. Continuous surveillance using Intrusion Detection Systems and Intrusion Prevention Systems, along with advanced Security Information and Event Management systems, provides a proactive security posture. These systems analyze data flows and can automatically respond to threats by alerting administrators and, if necessary, isolating affected systems to prevent the spread of an attack.

Security measures in a Cloud-Fog-Edge architecture require an integrated approach that addresses the distinct characteristics of each layer. Devices at the edge are often the most vulnerable, being physically accessible and typically equipped with limited processing power and storage. Security measures at this level include strong local authentication mechanisms, data encryption, and minimal data retention policies to reduce exposure in case of physical tampering.

As a mediator between edge devices and the cloud, the fog layer must enforce security policies that include data authentication and threat analysis. This layer can also perform additional security functions such as local firewalls, antivirus programs, and network segmentation to further protect data before it moves to the cloud.

Given its role in storing large volumes of data and performing significant processing tasks, the cloud layer's security is paramount. Cloud security encompasses robust encryption practices, comprehensive access management systems, and extensive network monitoring.

Additionally, cloud providers must ensure compliance with regulatory requirements and standards to protect data privacy and integrity.

Maintaining security in IoT architectures involves regular training for all personnel in cybersecurity practices. Developing a security-conscious culture within an organization is crucial for preventing security lapses and ensuring rapid response to incidents. Regular audits and penetration tests should be conducted to evaluate the effectiveness of the security infrastructure and identify potential improvements.

Securing Cloud-Fog-Edge architectures is an ongoing challenge that requires constant vigilance and adaptation to emerging threats. By implementing a layered security approach that integrates comprehensive measures across all components of the architecture, organizations can protect their valuable data and maintain the trust of their users and clients. This proactive security strategy not only defends against current threats but also prepares IoT systems for future vulnerabilities.

7 Conclusion

Throughout this article, we have explored the multifaceted Cloud-Fog-Edge architecture and its critical role in enhancing data management and security within the Internet of Things ecosystems. As we delved into various aspects of this architecture, from interoperability to security, it became evident that the integration of Cloud-Fog-Edge frameworks offers substantial benefits to IoT systems, particularly in handling large volumes of data across distributed environments.

The Cloud-Fog-Edge architecture not only facilitates efficient data processing by bringing computation closer to data sources but also significantly reduces latency and enhances responsiveness. Through the strategic deployment of cloud, fog, and edge layers, this architecture supports scalable, efficient, and flexible IoT applications. We discussed how these layers interact to create a cohesive system that dynamically adapts to changing conditions and demands.

Interoperability emerged as a key challenge, necessitating standardized protocols and data formats to ensure seamless communication between diverse devices and systems. Addressing this challenge is essential for achieving the full potential of IoT systems, enabling them to operate harmoniously across varied technological landscapes [54].

Security within the Cloud-Fog-Edge architecture was highlighted as a paramount concern, given the constant threat of unauthorized access and cyber attacks. We examined comprehensive security measures, including data encryption, access management, regular updates, and network activity monitoring, which are crucial for protecting data integrity and privacy at every layer of the architecture.

In conclusion, the Cloud-Fog-Edge architecture represents a transformative approach for managing the complexity of IoT systems. By enhancing interoperability and fortifying security, this architecture not only improves current IoT deployments but also paves the way for future advancements. It stands as a robust framework that can accommodate the rapid growth and evolving demands of the IoT landscape, ensuring that IoT systems are not only more efficient and responsive but also more secure and resilient against emerging challenges. As IoT continues to expand its influence across industries, the strategic importance of Cloud-Fog-Edge architectures will undoubtedly grow, playing a pivotal role in shaping the future of digital infrastructure.

References

1. A. Mijuskovic, 2021 IEEE 25th International Enterprise Distributed Object Computing Workshop (EDOCW), Gold Coast, Australia, 349-355 (2021)
2. V. Kuchukov, A. Nazarov, I. Vashchenko, 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), St. Petersburg and Moscow, Russia, 374-376 (2020)
3. N. V. Andreyanov, A. S. Sytnik, M. P. Shleymovich, IOP Conference Series: Earth and Environmental Science **988(3)**, 032002 (2022)
4. G. Mingaleeva, O. Afanaseva, P. Zunino, D. T. Nguen, D. N. Pham, Energies **13(21)**, 5848 (2020)
5. G. R. Mingaleeva, M. F. Nabiullina, D. N. Pham, 2023 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM), 233-238 (2023)
6. Y. Smirnov, A. Kalyashina, R. Zaripova, International Russian Automation Conference (RusAutoCon), 913-917 (2022)
7. Z. Gizatullin, R. Gizatullin, 2023 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM), Sochi, Russian Federation, 261-265 (2023)
8. Z. M. Gizatullin, M. P. Shleimovich, Russ. Aeronaut **66**, 154-161 (2023)
9. S. Lyasheva, R. Safina, M. Shleymovich, 2023 International Conference on Industrial Engineering, Applications and Manufacturing, 797-802 (2023)
10. M. Shleymovich, R. Safina, 2022 International Russian Automation Conference, 289-293 (2022)
11. R. M. Shakirzyanov, A. A. Shakirzyanova, 2021 International Russian Automation Conference (RusAutoCon), 714-718 (2021)
12. Y. I. Soluyanov, A. I. Fedotov, D. Y. Soluyanov, A. R. Akhmetshin, IOP Conference Series: Materials Science and Engineering **860(1)**, 012026 (2020)
13. A. V. Chupaev, R. S. Zaripova, R. R. Galyamov, A. Y. Sharifullina, E3S Web of Conferences **124**, 03013 (2019)
14. L. V. Plotnikova, R. R. Giniyatov, S. Y. Sitnikov, M. A. Fedorov, R. S. Zaripova, IOP Conference Series: Earth and Environmental Science **288**, 012069 (2019)
15. M. Tyurina, A. Porunov, A. Nikitin, R. Zaripova, G. Khamatgaleeva, Lecture Notes in Mechanical Engineering, 391-402 (2022)
16. E. I. Gracheva, O. V. Naumov, Journal of Pharmacy and Technology **8**, 4, 26763-26770 (2016)
17. D. D. Micu, I. V. Ivshin, E. I. Gracheva, O. V. Naumov, A. N. Gorlov, E3S Web of Conferences **124**, 02013 (2019)
18. Z. Gizatullin, R. Gizatullin, M. Nuriev, 2024 International Russian Smart Industry Conference (SmartIndustryCon), Sochi, Russian Federation, 356-360 (2024)
19. M. Nuriev, A. Kalyashina, Y. Smirnov, G. Gumerova, G. Gadzhieva, E3S Web of Conferences **515**, 04008 (2024)
20. R. F. Gibadullin, N. S. Marushkai, 2021 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM), 404-409 (2021)
21. V. O. Kozelkova, G. A. Ovseenko, V. I. Karachin, T. Van Tung, N. C. Kien, R. S. Kashaev, 4th International Youth Conference on Radio Electronics, Electrical and Power Engineering (REEPE), 1-4 (2022)

22. R. F. Gibadullin, I. S. Vershinin, R. Sh. Minyazev, 2017 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM), 1-6 (2017)
23. T. Petrov, A. Safin, E3S Web of Conferences **178**, 01049 (2020)
24. V. O. Kozelkova, G. A. Ovseenko, V. I. Karachin, N. C. Kien, T. Van Tung, O. V. Kozelkov, 4th International Youth Conference on Radio Electronics, Electrical and Power Engineering (REEPE), 1-5 (2022)
25. R. F. Gibadullin, G. A. Baimukhametova, M. Yu. Perukhin, 2019 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM), 1-7 (2019)
26. G. R. Rakhmatullina, E. A. Pankova, O. V. Fukina, M. Khayytov, L. V. Chapaeva, Journal of Physics: Conference Series **2270(1)**, 012056 (2022)
27. V. A. Gerasimov, M. G. Nuriev, D. A. Gashigullin, 2022 International Russian Automation Conference (RusAutoCon), 75-79 (2022)
28. S. R. Khasanov, E. I. Gracheva, M. I. Toshkhodzhaeva, S. T. Dadabaev, D. S. Mirkhalikova, E3S Web of Conferences **178**, 01051 (2020)
29. Z. M. Gizatullin, R. M. Gizatullin, M. G. Nuriev, 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), 120-123 (2020)
30. S. Lyasheva, M. Shleymovich, R. Shakirzyanov, 2019 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon), 1-6 (2019)
31. E. Gracheva, M. Toshkhodzhaeva, O. Rahimov, S. Dadabaev, D. Mirkhalikova, S. Ilyashenko, V. Frolov, International Journal of Technology **11**, 8 (2020)
32. M. Shakirzyanov, R. Gibadullin, M. Nuriyev, E3S Web of Conferences **419**, 02029 (2023)
33. T. Petrov, A. Safin, E3S Web of Conferences **178**, 01016 (2020)
34. J. Yoqubjonov, R. Gibadullin, M. Nuriev, E3S Web of Conferences **431**, 07011 (2023)
35. I. Viktorov, R. Gibadullin, E3S Web of Conferences **431**, 05012 (2023)
36. R. F. Gibadullin, I. S. Vershinin, M. M. Volkova, 2020 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon), 1-7 (2020)
37. R. F. Gibadullin, M. Yu. Perukhin, B. I. Mullayanov, 2020 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon), 1-6 (2020)
38. S. N. Cherny, R. F. Gibadullin, 2022 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM), 965-970 (2022)
39. V. A. Raikhlin, I. S. Vershinin, R. F. Gibadullin, Journal of Physics: Conference Series **2096**, 012160 (2021)
40. R. F. Gibadullin, I. S. Vershinin, R. Sh. Minyazev, 2018 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM), 1-6 (2018)
41. V. A. Raikhlin, R. F. Gibadullin, I. S. Vershinin, Lobachevskii Journal of Mathematics **43**, 2, 455-462 (2022)
42. G. A. Ovseenko, R. S. Kashaev, O. V. Kozelkov, T. K. Filimonova, T. S. Evdokimova, A. M. Mardanova, 5th International Youth Conference on Radio Electronics, Electrical and Power Engineering (REEPE) **5**, 1-5 (2023)
43. R. Zaripova, A. Nikitin, Y. Hadiullina, E. Pokaninova, M. Kuznetsov, E3S Web of Conferences **288**, 01072 (2021)

44. I. N. Madyshev, V. V. Kharkov, N. Z. Dubkova, M. G. Kuznetsov, AIP Conference Proceedings **2647**, 1 (2022)
45. Z. M. Gizatullin, M. S. Shkinderov, R. R. Mubarakov, Proceedings of the 2022 Conference of Russian Young Researchers in Electrical and Electronic Engineering, 1350-1353 (2022)
46. Z. Gizatullin, M. Shkinderov, 2019 International Russian Automation Conference, 8867761 (2022)
47. A. G. Ilyin, A. S. Mahdi Khafaga, V. Yunusova, 2021 Systems of Signals Generating and Processing in the Field of on Board Communications, 1-4 (2021)
48. M. Galimov, R. Burnashev, A. Gatiatullin, 2023 8th International Conference on Computer Science and Engineering (UBMK), Burdur, Turkiye, 382-386(2023)
49. N. Andreyanov, M. Shleymovich, A. Sytnik, 2022 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM), 880-885 (2022)
50. E. Kozlov, R. Gibadullin, E3S Web of Conferences **474**, 02031 (2024)
51. R. M. Petrova, E. Gracheva, 2023 5th International Conference on Control Systems, Mathematical Modeling, Automation and Energy Efficiency (SUMMA), Lipetsk, Russian Federation, 1049-1055 (2023)
52. R. M. Petrova, E. Gracheva, 2023 5th International Conference on Control Systems, Mathematical Modeling, Automation and Energy Efficiency (SUMMA), Lipetsk, Russian Federation, 1056-1061 (2023)
53. G. Uteyev, R. F. Gibadullin, 2024 International Russian Smart Industry Conference (SmartIndustryCon), Sochi, Russian Federation, 350-355 (2024)
54. N. A. Sabirov, R. F. Gibadullin, 2024 International Russian Smart Industry Conference (SmartIndustryCon), Sochi, Russian Federation, 344-349 (2024)