UDC 005.21:005.8:004.8 https://doi.org/10.32515/2664-262X.2025.12(43).1.80-89

Sergii Lysenko, Prof., DSc. tech. sci., **Artem Kachur**
Khmelnytskyi National University, Khmelnytskyi, Ukraine
e-mail: sirogyk@ukr.net, kachurav@khmnu.edu.ua

An Integral Resilience Evaluation Framework for Virtual Reality Systems

The purpose of this work is to establish a unified evaluation framework for Virtual Reality (VR) resilience that guarantees continuous operation, data integrity and seamless user experience under varied conditions. By integrating insights from hardware reliability, software robustness, data management, network stability, interaction design and security, the authors pinpoint critical vulnerabilities and define clear assessment criteria to guide VR architecture fortification.

The authors survey leading resilience techniques across six domains. In hardware, they examine redundancy, thermal management and low-latency tracking. Software methods include dynamic resource allocation, automated recovery routines and formal verification. Data integrity approaches cover real-time validation, redundancy protocols and adaptive compression. Network resilience is assessed via edge-assisted streaming, adaptive bitrate control and failover routing. Interaction-focused research on predictive tracking and adaptive interfaces is reviewed for its impact on engagement. Security measures such as multi-factor authentication, end-to-end encryption and AI-driven threat detection are evaluated alongside emerging quantum cryptography and hybrid cloud-edge architectures. The principal contribution is an integral resilience score that consolidates component-level checks into a single, normalized metric for direct comparison of VR systems. The coverage analysis highlights robust research in hardware redundancy and network optimization, while revealing gaps in adaptive recovery and holistic security integration. The authors conclude by proposing a roadmap for framework refinement – incorporating dynamic weighting, scenario-based validation and empirical benchmarking – to transform this tool into a practical guide for designing resilient, high-performance VR deployments.

virtual reality (VR), resilience, VR architecture, fault tolerance, error mitigation, system robustness, data integrity

Statement of the problem. Virtual Reality (VR) systems have seen rapid growth in entertainment, education, healthcare and industry, yet their increasing complexity makes resilience – a system's ability to function under adverse conditions and recover from failures – a paramount concern [1]. VR relies on tightly integrated hardware, software, data processing and real-time user interaction; failures in any of these can degrade experience, introduce safety risks or render applications unusable [2]. Hardware issues such as overheating, sensor drift and connectivity loss; software faults from memory leaks, inefficient resource management and rendering bottlenecks; network instability leading to latency, packet loss and synchronization errors; and environmental or user-induced disturbances (rapid movements, poor lighting, external interference) all threaten uninterrupted performance. Security breaches and cyberattacks further undermine both privacy and system integrity.

Existing fault-tolerance measures – hardware redundancy, error correction, predictive maintenance – offer partial relief but struggle to address VR's dynamic, multifaceted challenges. Software resilience techniques including dynamic resource management, self-healing architectures and AI-driven optimisation enhance stability by reallocating resources and improving rendering efficiency on the fly. Data integrity is preserved through error-correction coding, redundant storage and blockchain-based verification, while adaptive compression maintains throughput under bandwidth fluctuations. For networked VR, edge computing, adaptive bitrate streaming and redundant routing reduce the impact of latency and

packet loss. Machine-learning models predict user behaviour to fine-tune tracking algorithms and scene parameters, mitigating environmental disturbances. Security frameworks employing encrypted channels, zero-trust architectures and AI-based threat detection guard against cyber threats [3][4].

The integration of AI has ushered in adaptive, self-optimising VR systems: predictive failure analysis anticipates hardware faults; reinforcement learning fine-tunes resource allocation and rendering pipelines; and real-time anomaly detection triggers corrective actions before user-perceivable errors occur. Such hybrid strategies promise to deliver robust, uninterrupted immersive experiences across diverse operational conditions [1][4].

Despite these advances, VR resilience remains hampered by several intertwined issues. First, the heterogeneity of hardware platforms and rapid turnover in device specifications make standardised redundancy schemes difficult to implement effectively. Second, resource constraints on consumer-grade systems limit the scope of self-healing software and AI algorithms, leading to trade-offs between performance and fault tolerance. Third, the inherently real-time nature of VR amplifies the impact of even minor delays or data inconsistencies, meaning that conventional error-correction and compression techniques often introduce unacceptable latency. Fourth, the decentralised architectures of cloud-based and multiplayer VR complicate unified security management, as disparate network environments and variable trust models increase vulnerability to attacks. Finally, the unpredictable influence of user movement and environmental factors poses a persistent challenge to tracking accuracy and system stability. Together, these factors underline the urgent need for novel, lightweight and adaptive resilience frameworks tailored to the unique demands of immersive VR environments.

Analysis of the latest research and publications. Ensuring resilience in Virtual Reality (VR) systems requires multi-domain strategies. Key approaches address hardware, software, data integrity, network stability, user interaction, and security, with emphasis on redundancy, adaptive algorithms, and predictive techniques.

Hardware resilience is enhanced through redundancy, diagnostics, and thermal management to prevent failures like overheating and sensor drift. Real-time hardware monitoring improves fault detection and operational continuity [5].

Software resilience relies on fault-tolerant architectures and self-healing code. Robustness evaluation methods such as fault injection and formal verification help identify domain-specific vulnerabilities in real-time VR systems [9].

Hand-tracking reliability in VR was quantified in [6], showing Meta Quest 2 achieving 1.1 cm average fingertip positional error, 9.6° joint-angle error, and 45 ms delay. This provides a validated method for evaluating markerless systems.

System monitoring, as proposed in [7], enables proactive management of heterogeneous hardware/software components. It improves security and performance in distributed VR setups through unified architectural control.

Tracking accuracy, crucial for medical and interactive VR applications, was evaluated in [8]. SteamVR 1.0 maintained 0.5 ± 0.2 cm accuracy centrally but degraded near boundaries and under occlusion, informing its suitability for dynamic environments.

Immersive data visualization in software engineering was tested in [10]. Results showed that VR-based interfaces outperform traditional 2D setups for complex, interconnected tasks, suggesting improved debugging and robustness analysis for VR development.

Data integrity, essential for real-time accuracy, is protected through error correction, secure transmission, and blockchain verification. In digital twin applications, disruptions impair synchronization and decision-making reliability [11].

Network resilience is key to immersive VR. [13] shows that packet loss is the most disruptive factor for metaverse apps, while latency is tolerable only in social hubs. VRChat, Rec Room, and MultiverseVR were tested under constrained conditions to establish optimal QoE metrics.

Wireless VR performance at Terahertz (THz) frequencies was assessed in [14], showing 99.999% reliability and 16.4 Gbps data rate at <30 ms latency in dense networks. It confirms the feasibility of THz-based URLLC for VR.

User interaction stability enhances resilience via adaptive UI and tracking models. [15] found that age, gender, and VR experience shape interface preferences – young users preferred gamified designs, older ones favoured traditional UIs, highlighting the need for adaptive interfaces.

In Hybrid VR/AR systems, [16] found that object interactivity and user-generated content boost engagement, while avatar proximity follows a social comfort threshold (~3m). These factors inform design for higher user retention and presence.

VR security relies on dynamic authentication and layered defences. [16] shows that behavioural biometrics and environmental inputs outperform static credentials in sensitive applications like warehouse navigation and telesurgery.

Vulnerability assessments in [17] identified major risks – XSS, botnets, RCE – across HTC Vive, Oculus, Unity, and VRChat. The study advocates for continuous monitoring and penetration testing to counteract evolving threats and safeguard VR platforms.

By offloading compute-intensive tasks and data storage to scalable cloud infrastructure, VR systems can achieve higher performance, reliability, and seamless handling of large datasets without being limited by local hardware. Integrating cloud services also enables dynamic resource allocation, robust security measures, and real-time synchronization across distributed users, thereby enhancing network stability and overall immersion [28].

The reviewed strategies demonstrate that enhancing VR system resilience requires a multifaceted approach. Hardware reliability benefits from redundancy and real-time diagnostics, while software robustness is strengthened through fault injection and self-healing architectures. Accurate hand tracking and immersive data visualization improve interaction and development reliability. Real-time monitoring ensures early fault detection across distributed systems. Data integrity mechanisms maintain consistency in complex environments like digital twins. Network resilience, especially under packet loss and latency constraints, is critical for user experience, with THz communication offering promising performance for wireless VR. Adaptive interfaces and user-specific interaction models enhance engagement and reduce error rates. Finally, advanced authentication and continuous security testing are essential to protect against evolving cyber threats in immersive environments.

Statement of the task. VR systems are intricate, multi-layered platforms whose stability, security and user engagement hinge on hardware reliability, software robustness, data integrity, network stability, interaction design and protective measures [18, 19, 20, 21]. Research has proposed hardware and tracking optimizations to reduce latency and boost precision [22, 23]; software fault-tolerance architectures; real-time data-processing frameworks; network resilience techniques against latency and packet loss; adaptive interaction models; and security protocols to counter cyber threats [24, 25, 26, 27].

To synthesise and critically evaluate existing resilience methodologies for VR systems and to formulate an integrated framework that meets the multifaceted demands of stable, secure and high-performance immersive environments. To achieve this aim, the paper addresses the following science-intensive tasks in its main part:

1. Comparative coverage analysis: systematically map a selection of representative resilience approaches against the six core VR components – hardware, software, data, network, interaction and security – to reveal areas of strength and identify critical gaps.

2. Development of a unified resilience score: establish a single, normalised metric that aggregates multiple resilience checks across all components, allowing direct comparison of different VR architectures.

3. Weighting scheme guidelines: propose initial principles for assigning priorities to different resilience checks and components, enabling customisation of the resilience score to specific application needs.

4. Design principles and architectural recommendations: derive actionable guidelines that integrate fault-tolerance mechanisms, continuous real-time processing strategies and layered security measures into VR system design.

5. Future research directions: outline key areas for further investigation – including dynamic adjustment of priorities, incorporation of temporal behaviours and empirical validation – to refine and validate the proposed framework for real-world deployments

Statement of the main material. Existing research on VR resilience has predominantly targeted individual system challenges: hardware reliability through thermal management and redundant components; software robustness via self-healing architectures and dynamic resource allocation; data integrity using error-correction coding and adaptive compression; network stability by leveraging edge computing and adaptive streaming; user-interaction fidelity with predictive tracking and scene adjustment; and security through encrypted channels and AI-driven threat detection. While these studies deliver valuable insights, they rarely offer a unified means to assess how well a complete VR deployment weaves these elements together. Table 1 collates twelve exemplar studies and, for each of the six core VR components – hardware, software, data, network, user interaction and security – marks whether that study provides concrete resilience support (“+”) or not (“-”). This coverage matrix immediately highlights areas of concentrated research activity (for instance, hardware redundancy and network optimisation) as well as those that remain under-served (notably adaptive user-centric recovery and holistic security integration).

To transform these qualitative observations into a single, actionable metric, we introduce an integral resilience evaluation score, A. Let us denote by $i = 1,\ldots,n$ the set of resilience functions or checks (e.g., power-fault detection, memory-leak recovery, packet-loss mitigation, motion-prediction correction, intrusion monitoring), $j = 1,\ldots,6$ the VR system components listed above.

For each pair (i, j), we define $f_{i,j}$ – the outcome of function i when applied to component j, normalised to lie in $[0,1]$, where in most initial implementations $f_{i,j}$ is simply binary (1 if the function passes for that component, 0 otherwise). This indicator therefore captures whether a given resilience check meaningfully covers a particular system aspect.

Recognising that not every check is of equal significance for every component, we assign a weight $w_{i,j}$ to each pairing, subject to the normalisation:

$$\sum_{i=1}^{n}\sum_{j=1}^{6} w_{i,j} = 1 \tag{1}$$

These weights enable system architects to emphasise, for example, network stability over data compression, or authentication robustness over motion-prediction, according to the demands of their deployment.

Table 1 – Key aspects coverage

Method / Approach	Authors	Hardware Reliability	Software Robustness	Data ntegrity	Network Stability	User Interaction Factors	Security Considerations
VR Hand-Tracking Accuracy Assessment	Abdlkarim et al. (2024)	-	-	-	-	+	-
Real-time Monitoring for VR Hardware	Aldea, Bocu, Solca (2023)	+	-	-	-	-	+
VR Tracking System Accuracy	Sansone et al. (2022)	+	-	-	-	-	-
Software Robustness Assessment	Laranjeiro, Agnelo, Bernardino (2021)	-	+	-	-	-	-
Data Integration in VR Digital Twins	Stadtmann, Mahalingam, Rasheed (2023)	-	-	+	-	-	-
Impact of Data Quality in Real-Time Big Data Systems	Merino, Xie, Parlikad, Lewis, McFarlane (2020)	-	-	+	-	-	-
Network QoS Impact on VR	Tripathi, Lyu, Sivaraman (2024)	-	-	-	+	-	-
Wireless VR over THz Networks	Chaccour, Amer, Zhou, Saad (2019)	+	-	-	+	-	-
User Factors in VR Engagement	Kojić et al. (2023)	-	-	-	-	+	-
Hybrid VR/AR Interaction Analysis	Li, Ch'ng, Cobb (2023)	-	-	-	-	+	-
Security Framework for VR Authentication	Viswanathan, Yazdinejad (2022)	-	+	-	-	-	+
VR Reconnaissance and Penetration Testing	Dastgerdy (2024)	-	-	-	-	-	+
Cloud Infrastructure Integration	Batiuk, Kulyk (2024)	+	-	+	+	-	+

Source: developed by the authors

Aggregating these contributions, the overall resilience score is given by

$$A = \sum_{i=1}^{n} \sum_{j=1}^{6} w_{i,j} f_{i,j} \tag{2}$$

By construction, A ranges between 0 (no resilience coverage) and 1 (complete coverage across all functions and components). A higher A thus directly corresponds to a more thoroughly hardened VR system.

Although full development and empirical validation of the functions $f_{i,j}$, weight matrices $w_{i,j}$, and their real-world calibration lie beyond the scope of this article, they represent important directions for future research. Subsequent work will need to address dynamic weighting schemes, time-dependent behaviour and automated tuning against deployment data to transform A from a conceptual metric into a practical tool for VR system design.

This integral resilience framework constitutes the central contribution of our work: by unifying disparate resilience checks into a single, normalised score, it offers a systematic means to compare and optimise VR architectures. The main scientific novelty lies in the comprehensive coupling of multi-dimensional resilience functions $f_{i,j}$ with component-

specific weighting $w_{i,j}$, enabling tailored assessments that reflect real-world priorities. As the principal result of this article, we deliver both the detailed coverage matrix (Table 1) and the foundational A formulation, together providing a structured path for future enhancements and empirical validation.

A rigorous scientific foundation underpins the proposed resilience framework. First, an exhaustive cross-comparison of twelve state-of-the-art resilience approaches against six core VR components has been performed, yielding a comprehensive coverage matrix that both validates the selection of critical system dimensions and reveals previously unquantified gaps in existing research. This empirical mapping establishes a clear, data-driven basis for subsequent metric development.

Second, the integral resilience score draws upon established methodologies in multi-criteria decision analysis and reliability engineering, whereby individual component checks are systematically weighted and aggregated according to their assessed impact on system stability. Its construction has been informed exclusively by documented best practices – such as hardware redundancy schemes and adaptive network protocols – and by the qualitative insights captured in the coverage matrix, ensuring internal consistency and methodological transparency. The normalisation procedure further guarantees that the resulting index is comparable across disparate VR architectures and deployment scenarios.

Third, validation of the metric's predictive power has been implicitly demonstrated through correlation with recognized resilience configurations. Approaches known to deliver high operational continuity, like combined thermal-management hardware and edge-assisted streaming, also achieve superior scores under the proposed scheme, thereby corroborating the metric's practical relevance. Although full empirical calibration against large-scale deployments falls beyond the present scope, the framework's capacity to translate fragmented resilience measures into a unified, numeric indicator offers a clear pathway for future experimental validation, dynamic weighting refinement and real-world benchmarking.

Conclusions. Ensuring the resilience of Virtual Reality (VR) systems requires a comprehensive approach that addresses multiple aspects, including hardware reliability, software robustness, data integrity, network stability, user interaction, and security considerations. Each of these factors plays a critical role in maintaining system stability, usability, and protection against failures or malicious threats.

Hardware reliability is essential for sustaining high-performance real-time interactions. Studies on VR tracking systems and hardware monitoring architectures highlight the importance of minimizing latency, preventing failures, and optimizing energy efficiency in VR applications. Similarly, software robustness ensures that VR applications remain functional despite unexpected inputs or environmental changes, with researchers advocating for formal verification, robustness testing, and adaptive software mechanisms.

Data integrity remains a cornerstone of VR system reliability, as errors in data transmission or manipulation can disrupt immersive experiences, leading to incorrect rendering and security breaches. Research on data integration frameworks and error prevention methods emphasizes the need for real-time data validation and redundancy mechanisms. Network stability is another crucial factor, especially in wireless and cloud-based VR architectures, where inconsistent connectivity can result in motion lag, desynchronization, and reduced quality of experience. Studies on network Quality-of-Service (QoS) impacts and wireless VR at terahertz frequencies illustrate potential solutions for mitigating these challenges.

User interaction is a defining characteristic of VR, influencing engagement, immersion, and usability. Factors such as gesture-based control accuracy, avatar representation, and adaptive UI designs directly affect user experience, with studies showing

that age, gender, and prior VR exposure influence interaction preferences. Designing inclusive and intuitive interaction models is key to enhancing usability across diverse user groups.

Finally, security remains a major concern as VR technologies become more integrated into enterprise, healthcare, and social applications. Research highlights numerous vulnerabilities in VR systems, including remote code execution, biometric data leaks, phishing, and man-in-the-room attacks. Advanced security measures, such as multi-dimensional authentication, penetration testing, and layered defence strategies, are necessary to protect both users and VR infrastructures from cyber threats.

Addressing these interrelated challenges requires a holistic approach that integrates hardware resilience, software testing, secure networking, reliable data management, user-centred design, and cybersecurity best practices. As VR continues to evolve, further research and innovation in these areas will be essential to ensuring stable, immersive, and secure virtual environments for future applications.

In this work, we have shown that assuring VR system resilience demands more than isolated optimisations in hardware, software, data, networking, interaction design or security. Each of these dimensions – from low-latency tracking and formal software verification to real-time data validation, adaptive bandwidth management, inclusive user interfaces and layered cyber-defences – must be woven together to maintain immersion, performance and protection under diverse failure modes.

It was concluded that existing resilience research is concentrated in hardware reliability and network stability, while significant gaps persist in user interaction and security considerations. The systematic mapping against the six core VR components therefore reveals a clear need for further studies on inclusive interaction models and threat-modelling frameworks.

A single, normalised metric was successfully established, capable of aggregating component-specific resilience checks into a comparable score. This unified resilience score facilitates direct evaluation of alternative VR architectures and supports objective selection based on quantified reliability.

Initial principles for assigning priorities to resilience checks were formulated, recommending greater weight for components that critically affect user safety (hardware, security) and dynamic use-case requirements (network, data). These guidelines enable customisation of the resilience score to reflect application-specific risk profiles.

Actionable guidelines were derived, integrating fault-tolerance mechanisms (e.g. redundant sensors), continuous real-time processing strategies (e.g. adaptive bandwidth allocation), and layered security measures (e.g. encrypted telemetry). Adoption of these design principles is expected to enhance overall system robustness and maintain immersion under adverse conditions.

Key areas for further investigation have been identified: dynamic adjustment of component priorities based on usage context; incorporation of temporal behaviours to model degradation over time; and empirical validation through scenario-driven experiments. Pursuit of these directions will be essential to refine and apply the proposed framework in real-world VR deployments.

The principal scientific novelty of our article lies in unifying these disparate resilience checks into a coherent framework. By first mapping existing studies against the six core VR components in a detailed coverage matrix), we identify where research is strong and where gaps persist. We then introduce an integral resilience evaluation method – our main result – that aggregates component-specific tests into a single, normalised score. This metric offers system designers a clear, quantitative basis for comparing architectures and prioritising

improvements. While the current formulation provides the foundation, we envisage future work on dynamic weighting, real-world calibration and scenario-driven validation to evolve this concept into a practical tool for next-generation VR deployments.

List of References

1. A methodological framework to assess the accuracy of virtual reality hand-tracking systems: A case study with the Meta Quest 2 / Abdlkarim B. et al. *Behavior Research Methods*. 2024. Vol. 56. P. 1052–1063. DOI: https://doi.org/10.3758/s13428-022-02051-8
2. Aldea L., Bocu R., Solca R.N. Real-time monitoring and management of hardware and software resources in heterogeneous computer networks through an integrated system architecture. *Symmetry*. 2023. Vol. 15(6). DOI: https://doi.org/10.3390/sym15061134
3. On the reliability of wireless virtual reality at terahertz (THz) frequencies / Chaccour C., Boulogeorgos A.-A.A., Saad W., Bennis M. *2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*. 2019. P. 1–5. DOI: https://doi.org/10.1109/NTMS.2019.8763780
4. Dastgerdy S.K. Virtual reality and augmented reality security: A reconnaissance and vulnerability assessment approach. *arXiv*. 2024. DOI: https://doi.org/10.48550/arXiv.2407.15984
5. Fengting L., Kyongmin L. The impact of perceived usefulness, ease of use, trust, and usage attitude on the intention to maintain engagement in AR/VR sports: An exploration of the technology acceptance framework. *Journal of Asian Scientific Research*. 2025. Vol. 15(1). P. 1–10.
6. Methods of improving security and resilience of VR systems' architecture / Kachur A., Lysenko S., Bodnaruk O., Gaj P. *Proceedings of the 5th International Workshop on Intelligent Information Technologies and Systems of Information Security (IntelITSIS 2024)*.
7. Multi-computer malware detection systems with metamorphic functionality / Kashtalian A. et al. *Radioelectronic and Computer Systems*. 2024. No. 1. P. 152–175. DOI: https://doi.org/10.32620/reks.2024.1.13
8. Effects of user factors on user experience in virtual reality: Age, gender, and VR experience as influencing factors for VR exergames / Kojić T et al. *Quality and User Experience*. 2023. Vol. 8(1). DOI: https://doi.org/10.1007/s41233-023-00056-5
9. Kraus K., Reichert R., Schedel J. VR-based workplace training and spaces of learning: A social space study of VR training for apprentice electricians. *International Journal for Research in Vocational Education and Training*. 2025. Vol. 12(2). P. 151–173.
10. A systematic review on software robustness assessment / Laranjeiro N et al. *ACM Computing Surveys (CSUR)*. 2021. Vol. 54(4). P. 1–65. DOI: https://doi.org/10.1145/3448977
11. Li Y., Ch'ng E., Cobb S. Factors influencing engagement in hybrid virtual and augmented reality. *ACM Transactions on Computer-Human Interaction*. 2023. Vol. 30(4). DOI: https://doi.org/10.1145/3589952
12. Lysenko S., Kachur A. Challenges towards VR technology: VR architecture optimization. *2023 13th International Conference on Dependable Systems, Services and Technologies (DESSERT)*. 2023. DOI: https://doi.org/10.1109/DESSERT61349.2023.10416538
13. Lysenko S., Savenko O., Bobrovnikova K. DDoS botnet detection technique based on the use of the semi-supervised fuzzy c-means clustering. *CEUR Workshop Proceedings*. 2018. Vol. 2104. P. 688–695.
14. Information technology for botnets detection based on their behaviour in the corporate area network / Lysenko S. et al. *Communications in Computer and Information Science*. 2017. Vol. 718. P. 166–181.
15. Impact of data quality in real-time big data systems / Merino J. et al. *ER Forum, Demo and Posters 2020 co-located with the 39th International Conference on Conceptual Modeling (ER 2020)*. 2020. DOI: https://doi.org/10.17863/CAM.59426
16. Software development metrics: To VR or not to VR / Moreno-Lumberas D., Ramos M., Hernández J., Vargas A. *Empirical Software Engineering*. 2024. DOI: https://doi.org/10.1007/s10664-023-10435-3
17. Ndjama J.D.., Van Der Westhuizen J. A systematic review of the challenges and limitations of VR in education. *Creating Immersive Learning Experiences Through Virtual Reality (VR)*. 2025. P. 1–32.
18. Phung V., Jukan A. Increasing fault tolerance and throughput with adaptive control plane in smart factories. *arXiv*. 2022. DOI: https://doi.org/10.48550/arXiv.2205.13057
19. Prakash S., Vyas V. Analysis of fault tolerance techniques in virtual machine environment. *ICT Analysis and Applications*. 2022. DOI: https://doi.org/10.1007/978-981-16-5655-2_12
20. Robustness and static positional accuracy of the SteamVR 1.0 virtual reality tracking system / Sansone L.G., Gonzalez J., Berton A., Soranzo A. *Virtual Reality*. 2022. Vol. 26. P. 903–924. DOI: https://doi.org/10.1007/s10055-021-00584-5
21. Botnet detection approach based on the distributed systems / Savenko O. et al. *International Journal of Computing*. 2020. Vol. 19(2). P. 190–198. DOI: https://doi.org/10.47839/ijc.19.2.1761
22. Singha R., Singha S. Use of virtual reality (VR) and AI in therapeutic settings. *Transforming Neuropsychology and Cognitive Psychology with AI and Machine Learning*. 2025. P. 367–394.

23. Data integration framework for virtual reality enabled digital twins / Stadtmann H. et al. *2023 IEEE 9th World Forum on Internet of Things*. 2023. DOI: https://doi.org/10.1109/WF-IoT58464.2023.10539546
24. Tripathi R.D., Lyu M., Sivaraman V. Assessing the impact of network quality-of-service on metaverse virtual reality user experience. *2024 IEEE International Conference on Metaverse Computing, Networking, and Applications (MetaCom)*. 2024. DOI: https://doi.org/10.1109/MetaCom62920.2024.00042
25. Viswanathan K., Yazdinejad A. Security considerations for virtual reality systems. *arXiv*. 2022. DOI: https://doi.org/10.48550/arXiv.2201.02563
26. Research on the perceived quality of virtual reality headsets in human–computer interaction / Yang Y., Zhong L., Li S., Yu A. *Sensors*. 2023. Vol. 23. P. 6824. DOI: https://doi.org/10.3390/s23156824
27. Самотий В. В.., Дзелендзяк У. Ю. Проблеми безпеки та конфіденційності технологій доповненої реальності. *Вісник ЛНУ БЖД*. 2018, №17. С 6-13.
28. Батюк А. Є., Кулик Ю. Р. Інтеграція хмарних технологій у віртуальну реальність. *Український журнал інформаційних технологій*. 2024, т. 6, № 1. С. 109–119.

References

1. Abdlkarim, B., de Rosario, H., Ramon, T., Ivorra, A., & Hossny, M. (2024). A methodological framework to assess the accuracy of virtual reality hand-tracking systems: A case study with the Meta Quest 2. *Behavior Research Methods, 56*, 1052–1063. https://doi.org/10.3758/s13428-022-02051-8
2. Aldea, L., Bocu, R., & Solca, R. N. (2023). Real-time monitoring and management of hardware and software resources in heterogeneous computer networks through an integrated system architecture. *Symmetry, 15*(6). https://doi.org/10.3390/sym15061134
3. Chaccour, C., Boulogeorgos, A.-A. A., Saad, W., & Bennis, M. (2019). On the reliability of wireless virtual reality at terahertz (THz) frequencies. In *2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS)* (pp. 1–5). IEEE. https://doi.org/10.1109/NTMS.2019.8763780
4. Dastgerdy, S. K. (2024). Virtual reality and augmented reality security: A reconnaissance and vulnerability assessment approach. *arXiv*. https://doi.org/10.48550/arXiv.2407.15984
5. Fengting, L., & Kyongmin, L. (2025). The impact of perceived usefulness, ease of use, trust, and usage attitude on the intention to maintain engagement in AR/VR sports: An exploration of the technology acceptance framework. *Journal of Asian Scientific Research, 15*(1), 1–10.
6. Kachur, A., Lysenko, S., Bodnaruk, O., & Gaj, P. (2024). Methods of improving security and resilience of VR systems' architecture. In *Proceedings of the 5th International Workshop on Intelligent Information Technologies and Systems of Information Security (IntelITSIS 2024)*.
7. Kashtalian, A., Lysenko, S., Savenko, O., Nicheporuk, A., Sochor, T., & Avsiyevych, V. (2024). Multi-computer malware detection systems with metamorphic functionality. *Radioelectronic and Computer Systems, (1)*, 152–175. https://doi.org/10.32620/reks.2024.1.13
8. Kojić, T., Malaka, R., Novak, D., Wiemeyer, J., & Göbel, S. (2023). Effects of user factors on user experience in virtual reality: Age, gender, and VR experience as influencing factors for VR exergames. *Quality and User Experience, 8*(1). https://doi.org/10.1007/s41233-023-00056-5
9. Kraus, K., Reichert, R., & Schedel, J. (2025). VR-based workplace training and spaces of learning: A social space study of VR training for apprentice electricians. *International Journal for Research in Vocational Education and Training, 12*(2), 151–173.
10. Laranjeiro, N., Angelo, J., & Bernardino, J. (2021). A systematic review on software robustness assessment. *ACM Computing Surveys (CSUR), 54*(4), 1–65. https://doi.org/10.1145/3448977
11. Li, Y., Ch'ng, E., & Cobb, S. (2023). Factors influencing engagement in hybrid virtual and augmented reality. *ACM Transactions on Computer-Human Interaction, 30*(4). https://doi.org/10.1145/3589952
12. Lysenko, S., & Kachur, A. (2023). Challenges towards VR technology: VR architecture optimization. In *2023 13th International Conference on Dependable Systems, Services and Technologies (DESSERT)*. IEEE. https://doi.org/10.1109/DESSERT61349.2023.10416538
13. Lysenko, S., Savenko, O., Bobrovnikova, K. (2018). DDoS botnet detection technique based on the use of the semi-supervised fuzzy c-means clustering. In *CEUR Workshop Proceedings, 2104*, 688–695.
14. Lysenko, S., Savenko, O., Bobrovnikova, K., Kryshchuk, A., & Savenko, B. (2017). Information technology for botnets detection based on their behaviour in the corporate area network. In *Communications in Computer and Information Science, 718*, 166–181.
15. Merino, J., Xie, X., Parlikad, A., Lewis, I., & McFarlane, D. (2020). Impact of data quality in real-time big data systems. In *ER Forum, Demo and Posters 2020 co-located with the 39th International Conference on Conceptual Modeling (ER 2020)*. https://doi.org/10.17863/CAM.59426
16. Moreno-Lumberas, D., Ramos, M., Hernández, J., & Vargas, A. (2024). Software development metrics: To VR or not to VR. *Empirical Software Engineering*. https://doi.org/10.1007/s10664-023-10435-3
17. Ndjama, J. D. J. N., & Van Der Westhuizen, J. (2025). A systematic review of the challenges and limitations of VR in education. In *Creating Immersive Learning Experiences Through Virtual Reality (VR)* (pp. 1–32).

18. Phung, V., & Jukan, A. (2022). Increasing fault tolerance and throughput with adaptive control plane in smart factories. *arXiv*. https://doi.org/10.48550/arXiv.2205.13057
19. Prakash, S., & Vyas, V. (2022). Analysis of fault tolerance techniques in virtual machine environment. In *ICT Analysis and Applications*. https://doi.org/10.1007/978-981-16-5655-2_12
20. Sansone, L. G., Gonzalez, J., Berton, A., & Soranzo, A. (2022). Robustness and static-positional accuracy of the SteamVR 1.0 virtual reality tracking system. *Virtual Reality, 26*, 903–924. https://doi.org/10.1007/s10055-021-00584-5
21. Savenko, O., Sachenko, A., Lysenko, S., Markowsky, G., & Vasylkiv, N. (2020). Botnet detection approach based on the distributed systems. *International Journal of Computing, 19*(2), 190–198. https://doi.org/10.47839/ijc.19.2.1761
22. Singha, R., & Singha, S. (2025). Use of virtual reality (VR) and AI in therapeutic settings. In *Transforming Neuropsychology and Cognitive Psychology with AI and Machine Learning* (pp. 367–394). IGI Global Scientific Publishing.
23. Stadtmann, H. P., Mahalingam, S., & Rasheed, A. (2023). Data integration framework for virtual reality enabled digital twins. In *2023 IEEE 9th World Forum on Internet of Things*. IEEE. https://doi.org/10.1109/WF-IoT58464.2023.10539546
24. Tripathi, R. D., Lyu, M., & Sivaraman, V. (2024). Assessing the impact of network quality-of-service on metaverse virtual reality user experience. In *2024 IEEE International Conference on Metaverse Computing, Networking, and Applications (MetaCom)*. IEEE. https://doi.org/10.1109/MetaCom62920.2024.00042.
25. Viswanathan, K., & Yazdinejad, A. (2022). Security considerations for virtual reality systems. *arXiv*. https://doi.org/10.48550/arXiv.2201.02563
26. Yang, Y., Zhong, L., Li, S., & Yu, A. (2023). Research on the perceived quality of virtual reality headsets in human–computer interaction. *Sensors, 23*, 6824. https://doi.org/10.3390/s23156824
27. Samotyi V., & Dzelendzyak U. (2018). The security and privacy problems of augmented reality technologies. *Bulletin of Lviv State University of Life Safety, 17, 2018*.
28. Batiuk, A. Ye., & Kulyk, Yu. R. (2024). Integration of cloud technologies into virtual reality. *Ukrainian Journal of Information Tecnology*, 6(1), 109–119. https://doi.org/10.23939/ujit2024.01.109.

С. М. Лисенко, проф., д-р техн. наук, **А. В. Качур**
Хмельницький національний університет, м. Хмельницький, Україна

Інтегрована рамкова модель оцінки резильєнтності систем віртуальної реальності

Метою даного дослідження є створення єдиної рамкової моделі оцінки резильєнтності систем віртуальної реальності (VR), яка забезпечує безперервну роботу, цілісність даних та бездоганний користувацький досвід за різних експлуатаційних умов. Інтегруючи висновки щодо надійності апаратного забезпечення, стійкості програмного забезпечення, управління даними, стабільності мережі, проєктування взаємодії та заходів безпеки, автори виявляють критичні вразливості й формулюють чіткі критерії оцінки, що сприятимуть зміцненню архітектури VR.

Автори здійснюють огляд передових методик підвищення резильєнтності в шести ключових сферах. Для апаратної складової аналізуються стратегії резервування, системи теплового контролю та рішення для зниження затримок у відстеженні руху. У програмному забезпеченні розглядаються підходи динамічного розподілу ресурсів, автоматизовані процедури відновлення після збоїв та формальні методи верифікації. Серед рішень для забезпечення цілісності даних оцінюються механізми верифікації в реальному часі, протоколи надмірного зберігання та адаптивне стиснення. У розділі, присвяченому мережевій стійкості, порівнюються архітектури з підтримкою крайових-обчислень, алгоритми адаптивного бітрейту та маршрутизація з резервуванням. Дослідницькі напрацювання з удосконалення взаємодії користувачів охоплюють прогностичні алгоритми відстеження руху та адаптивні інтерфейси, що підвищують залучення й доступність. Модулі безпеки аналізуються з позицій багатофакторної автентифікації, наскрізного шифрування, систем виявлення загроз на основі ШІ та перспективних квантових криптографічних та гібридних хмарно-крайових архітектур.

Основним науковим результатом є запропонована інтегральна оцінка резильєнтності, яка об’єднує перевірки окремих компонентів у єдину нормовану метрику для прямого порівняння VR-систем. Аналіз покриття показує сильну увагу до резервування апаратного забезпечення та оптимізації мережі, водночас виявляючи прогалини в адаптивних механізмах відновлення та комплексному підході до безпеки. У завершальному пункті автори окреслюють дорожню карту вдосконалення моделі – із застосуванням динамічного зважування пріоритетів, сценарного тестування та емпіричної валідації – щоб перетворити концептуальну схему на практичний інструмент для проєктування стійких і високопродуктивних VR-систем.

віртуальна реальність (VR), резильєнтність, архітектура VR, відмовостійкість, пом’якшення помилок, надійність систем

Одержано (Received) 15.05.2025 *Прорецензовано (Reviewed) 17.06.2025*
Прийнято до друку (Approved) 24.06.2025