

METHODS FOR RELIABLE USER AUTHENTICATION IN VIRTUAL REALITY NETWORKS

Umarov Bekzod Azizovich

ORCID ID: 0009-0007-9366-7195 Associate Professor, Department of Applied Mathematics and Informatics, PhD in Pedagogical Sciences, Fergana State University.

umaumarov@mail.ru

Ergashaliyeva Dilzodaxon Alisherjon qizi

ORCID ID: 0009-0008-3768-1854 Student in the Applied Mathematics program, Fergana State University.

dilzodaergashaliyeva2007@gmail.com

<https://doi.org/10.5281/zenodo.23632191>

Abstract. *This article analyzes user authentication methods in virtual reality (VR) networks, focusing on their security characteristics and privacy limitations. Password-based, multifactor, device-based, and behavioral biometric authentication methods are compared. The use of head movements, hand gestures, gaze direction, and voice data processed by VR devices expands authentication capabilities but also introduces privacy-related risks. Based on a review of the scientific literature, an adaptive conceptual model is proposed that combines initial session verification, continuous risk assessment during the session, and additional authentication when necessary.*

Keywords: *Virtual reality, metaverse, authentication, multifactor authentication, biometrics, continuous authentication, Zero Trust, identification.*

Introduction

In VR systems, user profiles, virtual assets, and access rights to services are managed over networks. If the identification mechanism is not adequately protected, an attacker may take over an account, act on behalf of the user, or gain unauthorized access to restricted resources.

Therefore, authentication is a critical security component of the VR ecosystem.

Traditional password-based verification may confirm a user's identity at the beginning of a session; however, it does not guarantee security throughout the session if the device subsequently falls into another person's hands. The sensors available in VR devices enable the use of behavioral biometrics, but such methods are associated with risks of errors, spoofing, and privacy violations. The aim of this article is to compare authentication methods used in VR networks and substantiate an adaptive approach that balances security and usability.

Literature Review and Methodology

In a review of the literature on VR security and privacy, Giaretta identifies authentication as one of the actively researched areas. Huynh-The and co-authors analyze authentication, access control, and data privacy issues within the broader context of metaverse security. A systematic review by Rahartomo and co-authors also identifies authentication as one of the most extensively studied aspects of metaverse security [3]. These studies establish the need to consider VR authentication not only at the initial access stage but also in relation to session continuity and data privacy.

This study employs comparative analysis and conceptual modeling. Password-based, multifactor, device-based, and behavioral biometric authentication methods are compared according to security, privacy, usability, and computational cost.

The proposed model integrates three stages: initial identification at the beginning of a session, monitoring of risk indicators throughout the session, and requiring additional verification when risk increases. The possibility of processing biometric data locally on the device and transmitting only the necessary results to the server is also considered. Since this is a conceptual study, no FAR, FRR, or EER values that have not been experimentally measured are reported.

Results

The comparative analysis indicates that password-based authentication is a simple and widely used method, but it is vulnerable to threats such as phishing and password reuse.

Multifactor authentication can reduce the risk of account compromise by combining independent verification factors, although additional steps may affect the user experience.

Device-based or cryptographic-key-based verification can help protect sessions, but the devices themselves must be securely managed. Behavioral biometrics can provide an additional trust signal based on users' movements or interaction patterns; however, relying on it as the sole authentication factor is risky.

Based on the analysis, an adaptive authentication model is proposed. The model initially verifies the user through trusted account credentials or a cryptographic mechanism. At the next stage, the session's risk level is assessed based on device status, connection characteristics, and indicators of unusual activity. When the risk exceeds a predefined threshold, additional verification is required. Biometric data are used only when necessary, in accordance with the principles of informed consent and data minimization. Rather than continuously monitoring all user behaviors, this model adopts a risk-based verification approach.

Discussion

The effectiveness of authentication in VR networks depends on balancing security and usability. Verifying every action may provide additional protection, but it can also introduce latency and excessive monitoring. An adaptive approach makes it possible to reduce unnecessary verification in low-risk situations while triggering additional checks in suspicious circumstances.

Because behavioral biometrics can change over time and may reveal information about users' personal characteristics, they should be used in combination with other authentication factors.

To validate the practical effectiveness of the proposed model, future research should experimentally evaluate it across different VR devices. The evaluation should measure false acceptance rates, false rejection rates, authentication latency, energy consumption, and user convenience.

Conclusion

Reliable authentication in VR networks is an essential requirement for protecting user accounts, virtual assets, and personal information. This article compares various authentication approaches and proposes an adaptive conceptual model that combines initial session verification, continuous risk assessment, and additional authentication when necessary.

The scientific and practical significance of the model lies in integrating risk-based security adaptation with the principle of minimizing the use of biometric data. Future work should experimentally test the proposed model and evaluate its performance using quantitative metrics.

References:

1. Umarov, Bekzod. "RAQAMLI TEXNOLOGIYALAR VOSITASIDA PEDAGOGLARNING PROFESSIONAL KOMPETENTLIGINI RIVOJLANTIRISH MAZMUNI." *Евразийский журнал математической теории и компьютерных наук* 3.5 (2023): 87-93.
2. Azizovich, Umarov Bekzod. "THE DEVELOPMENT OF PROFESSIONAL COMPETENCY OF TEACHERS IN EDUCATIONAL TECHNOLOGY BASED ON DIGITAL TECHNOLOGIES." *Eurasian Journal of Mathematical Theory and Computer Sciences* 4.7 (2024): 11-14.
3. Azizovich, Umarov Bekzod. "PEDAGOGICAL-PSYCHOLOGICAL PRINCIPLES OF THE FORMATION OF PROFESSIONAL COMPETENCE." *Confrencea* 6.6 (2023): 204-212.
4. Umarov, B. "THEORETICAL FOUNDATIONS OF THE ORGANIZATION OF PROFESSIONAL PRACTICE THAT DEVELOPS PROFESSIONAL COMPETENCE BY MEANS OF DIGITAL TECHNOLOGIES." *Science and innovation* 3.B8 (2024): 107-109.
5. Azizovich, Umarov Bekzod. "LOKAL TARMOQLARDA MONITORING VA TAHLIL JARAYONLARINI TASHKIL ETISHNING SAMARALI USULLARI." *World Scientific Research Journal* 46.2 (2025): 375-379.
6. Azizovich, Umarov Bekzod. "LOKAL KOMPYUTER TARMOQLARIDA AXBOROTNI UZATISH." *PEDAGOGIK TADQIQOTLAR JURNALI* 8.1 (2025): 308-309.
7. Umarov, Bekzod. "RAQAMLI TEXNOLOGIYALAR VOSITASIDA BO'LAJAK O'QITUVCHILARNING KASBIY KOMPETENTLIGINI RIVOJLANTIRISHNING MAZMUNI VA MALAKAVIY AMALIYOTNI TASHKIL ETISH BOSQICHLARI." *Scientific journal of the Fergana State University* 4 (2025): 25-25.