International Journal of Computer Science and Engineering (IJCSE)
ISSN (P): 2278–9960; ISSN (E): 2278–9979
Vol. 12, Issue 2, Jul – Dec 2023; 401–430

International Academy of Science, Engineering and Technology
Connecting Researchers; Nurturing Innovations

IMPLEMENTING ADAPTIVE AUTHENTICATION USING RISK BASED ANALYSIS IN FEDERATED SYSTEMS

Srinivasulu Harshavardhan Kendyala[1], Ashvini Byri[2], Ashish Kumar[3], Dr Satendra Pal Singh[4], Om Goel[5] & Prof.(Dr) Punit Goel[6]

[1]Scholar, University of Illinois, Hyderabad, Telangana, India

[2]Scholar, University of Southern California, Parel, Mumbai, India

[3]Scholar, Tufts University, DMW Colony Patiala, 147003, Punjab India

[4]Ex-Dean, Gurukul Kangri University, Haridwar, Uttarakhand, India

[5]Independent Researcher, ABES Engineering College Ghaziabad, India

[6]Research Supervisor, Maharaja Agrasen Himalayan Garhwal University, Uttarakhand, India

ABSTRACT

In an era of increasing cybersecurity threats, traditional authentication methods often fall short of ensuring secure access to sensitive resources, particularly in federated systems. This paper proposes an adaptive authentication framework utilizing risk-based analysis to enhance security measures dynamically. By leveraging contextual data, such as user behavior, device characteristics, and access patterns, the proposed approach assesses the risk level associated with each authentication attempt.

The framework employs machine learning algorithms to analyze historical data, enabling the system to adaptively adjust authentication requirements based on real-time risk assessments. High-risk scenarios may prompt additional verification steps, such as multi-factor authentication, while low-risk situations allow for seamless access. This adaptability not only strengthens security but also enhances the user experience by minimizing unnecessary friction during the authentication process.

Furthermore, the paper discusses the implementation of this adaptive authentication mechanism within federated identity management systems, highlighting the challenges and considerations for integrating risk-based analysis into existing architectures. By balancing security and usability, the proposed solution aims to mitigate unauthorized access while maintaining a smooth user experience across federated environments.

The effectiveness of the adaptive authentication framework is validated through a series of experiments, demonstrating its ability to significantly reduce security risks without compromising user convenience. This research contributes to the field of cybersecurity by providing a scalable and flexible authentication solution that aligns with the evolving threat landscape in federated systems.

KEYWORDS: *Adaptive Authentication, Risk-Based Analysis, Federated Systems, Cybersecurity, Multi-Factor Authentication, User Behavior, Machine Learning, Identity Management, Unauthorized Access, Security Framework.*

Article History

***Received:** 05 Nov 2023 | **Revised:** 10 Nov 2023 | **Accepted:** 16 Nov 2023*