Abstract

In recent years, there has been a growing focus on the security of administrative access to critical systems. This is due in part to the increasing number of high-profile data breaches that have been attributed to unauthorized access by administrators. In order to address this challenge, we propose to develop a secure and context-aware multi-factor authentication system for administrative access. Our system will use a combination of machine learning and biometric behavior analysis to authenticate administrators and to prevent unauthorized access.

Our system will be designed to be highly secure and to provide a high level of user convenience. It will be based on a number of innovative technologies, including machine learning, biometric behavior analysis, and context-aware authentication. Our system will be able to authenticate administrators based on a variety of factors, including their physical location, their device type, and their behavioral patterns. This will make it much more difficult for attackers to gain unauthorized access to critical systems.

Our system will also be designed to be highly scalable and to be able to support a large number of users. It will be able to integrate with existing authentication systems and will be easy to deploy and manage. We believe that our system will be a valuable addition to the security toolkit of any organization that needs to protect its critical systems from unauthorized access.

- [1] "A Survey of Multi-Factor Authentication." *IEEE Security & Privacy*, vol. 13, no. 2, pp. 54-67, 2015.
- [2] "Biometric Behavior Analysis for User Authentication: A Survey." *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 10, pp. 2243-2257, 2016.
- [3] "Context-Aware Authentication: A Survey." *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 1464-1488, 2016.
- [4] "A Survey of Machine Learning for Biometric Authentication." *IEEE Access*, vol. 6, pp. 47268-47290, 2018.

- [5] "A Survey of Multi-Factor Authentication for Mobile Devices." *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 264-289, 2019.