ABSTRACT:

TEAM 7.6

SALONI GHULE-21BCE1967

SHREYA SINGH-21BPS1435

KREET ROUT- 21BCE1482

NITIN KUMAR- 21BCE1792

In today's connected digital environment, protecting online platforms and sensitive information is becoming increasingly important. In the face of complex threats, traditional user identification methods are often inadequate and inefficient. Hereby an attempt was made to present a new approach that uses artificial intelligence (AI) to analyze user behavior to improve the security of online systems. This approach adds an extra layer of security by identifying users based on their unique

online behavior, such as keystrokes, mouse movements, and browsing habits.

This research explores the potential of machine learning algorithms and deep learning to create intelligent machines that can adapt with their users, constantly measuring and evaluating themselves. These artificial intelligence systems can detect unusual or suspicious activities by evaluating various aspects of online behavior and thus detect fraudulent activity and can improve the authentication process against access.

We discuss the potential applications of AI-based security approaches in various fields such as banking, e-commerce, healthcare and social media, as well as nature platforms where the protection of user data is very important. In addition, we highlight the ethical and privacy issues involved in collecting and analyzing online behavioral patterns.

The results of this study show that the integration of artificial intelligence-based authentication increases security, reduces dependence on traditional authentication methods, and strengthens online systems against cyber threats. This new approach holds promise against the changing challenges of user authentication as we move to a more secure and reliable digital environment.