Project Title: Additional security for user sign in

Research Question: How can we implement an additional security component to overcome the cybercrimes for user authentication?

Context: In regard to the current situation, the usage of online applications has augmented in all the sectors because of the lockdown. This increased usage has given rise to more cybercrimes. The necessity to increase the security on user authentication could reduce the cybercrimes. So, the aim of this project is to implement the security component as a plugin which can easily couple with any existing application. By integrating this security component, it will add an additional security layer for the user actions.

Problem: Chances of unauthorized access to the secured application with the legacy user authentication (Username & Password). The solution is to introduce second factor authentication in the form of one-time passcode (OTP) sent to their mobile or other devices.

Comparison: The comparison is made between the application with additional security component developed (Username, Password & OTP) against legacy application (Username & Password).

|  |  |
| --- | --- |
| **Advanced security authentication** | **Legacy authentication** |
| More secure because of two levels of authentication | Less secure because of single layer authentication |
| Less chances of hacking due to dynamic one-time passwords at the second level of authentication | More chances of hacking due to static passwords |

Outcome: We can avoid cybercrimes in user authentication by introducing an additional layer of security in the form of dynamic one-time passcode sent to their authorized mobile or other devices.