

## **Design and implementation of multi factor mechanism for secure authentication system**

### **ABSTRACT**

A secure network depends in part on user authentication and regrettably the authentication systems currently in use are not completely safe. However, the user is not the only party that needs to be authenticated to ensure the security of transactions on the Internet. Existing OTP mechanism cannot guarantee reuse of user's account by an adversary, re-use stolen user's device which is used in the process of authentication, and non-repudiation. This paper proposed mechanism of multi factor for secure electronic authentication. It intends to authenticate both of user and mobile device and guarantee non-repudiation, integrity of OTP from obtaining it by an adversary. The proposal can guarantee the user's credentials by ensuring the user's authenticity of identity and checking that the mobile device is in the right hands before sending the OTP to the user. This would require each user having a unique phone number and a unique mobile device (unique International Mobile Equipment Identity (IMEI)), in addition to an ID card number. By leveraging existing communication infrastructures, the mechanism would be able to guarantee the safety of electronic authentication, and to confirm that it demonstrates excellence in non-repudiation, authenticate user and mobile device which are used in the process of authentication, certification strength and also in comparison and analysis through experimenting with existing OTP mechanisms.

**Keyword:** Security; Non-repudiation; Multi factor authentication; IMEI