Abstract

Due to advancements and improvements in internet and communication systems, more people are relying on internet to store their confidential information. Earlier the idea of Static passwords was being used but most of the users try to use easily guessable, weak passwords or keywords from their personal information, which makes it easy for the intruders to guess their passwords in few combinations using Brute Force attack. Thus idea of using Multi-Factor Authentication has been introduced in the world of internet to harden the security of network and make it difficult for the attackers to crack systems. In this mechanism, users are required to provide some extra information along with their login Id and password. Most popular is using One-Time Passwords that are generated randomly and valid only for single login and even for short duration of time (usually 30 to 60 seconds). One-Time Passwords can be generated either online or offline via various mechanisms. In this paper, review of various Multi-step Authentication schemes has been performed to compare various authentication mechanisms.


Index Terms

Computer Science Security
Keywords

Multi-factor Authentication, One-Time Passwords (OTP), Static Passwords, Short Message Service (SMS), Time-based One-Time Passwords (TOTP) and Image-based Authentication.