# An Analytical Study of Attacks on Remote User Authentication Schemes

Trupil Limbasiya
Department of Computer Science & Engineering,
NIIT University, Rajasthan, India
trupil.limbasiya@niituniversity.in

## Abstract

In this digital era, any two or more individuals can transfer the talks over the internet even though they are not near each other. Before transferring the talks, they have to draw the prevalent session key based on the verification of each other through any authentication scheme called remote user authentication scheme. In 1981, Leslie Lamport proposed remote user authentication system centred on one way function for encoding password in unconfident communication first time. Many researchers have proposed the various remote user authentication schemes using the various features like text password, smart card, biometric identity, etc. Motivated by this, in this paper we prepared the state-of-art survey on the possible attacks based on the remote user authentication schemes from their inception. In addition, we have discussed distinct attacks that can be possible on remote user authentication schemes. Our aim is not only doing history finding on remote user authentication schemes, but also familiarize researchers with list of attacks that are identified till this date on these schemes. When any researchers are interested in developing a new model for authenticity at the same time, they must have to take care of certain situations as well as different challenges.