181. PREVENTING SHOULDER SURFING ATTACK FOR SECURE TRANSACTION

S.Jayasakthiya1, R.Deepa2
1II M.E. Department of Computer Science & Engineering, St. Peter's College of Engineering & Technology,
2Assistant Professor, Department of Computer Science & Engineering, St. Peter's College of Engineering & Technology,
r.deepame@gmail.com, shakthi.senthilvel.ss@gmail.com

In real-time processing, when the user enters the Personal Identification Number (PIN) as a numeric password in mobile or stationary system, including smart phones, tablet computers, Automated Teller Machines (ATM), and Point Of Sale (POS) terminals, a direct observation attack based on shoulder surfing becomes a great concern. The PIN entry can be observed by nearby adversaries, more effectively in a crowded place. The same PIN is usually chosen by a user for various purposes and PIN may cause the user a great risk. To cope with this problem, developing an application which is between the user and the system, in each round a regular numeric keypad is coloured at random, half of the keys in black and the other half in white, which is called as BW method. A user who knows the correct PIN digit can answer its colour by pressing the separate colour key below. Secondly improved BW method, split every numeric key into two halves, so as to be filled with two district colours simultaneously each colour fills half of the available keys i.e., five out of ten keys. So there exist four colour groups on the numeric keypad and user needs to either of the two colours that his/her PIN digit in each round. Thirdly, session key entry method users have to choose any one of the symbol from the digits in the given array. Authentication is also provided by these methods.

Keywords-Personal Identification Number, Shoulder-surfing attack, User authentication.

ISBN 978-81-904760-6-5