Security is provided to grant access to a legal user and to prevent the system from an illegal or non-authorized person. SHOULDER ATTACK is one of the latest weapons that are used by hackers or adversaries to hack an account or to authenticate in a secure zone. When a user uses a Chip+PIN credit card at a POS terminal, the POS machine will ask for PIN to be entered then on entering PIN in the terminal the transaction gets completed. To complete the
transaction user need to provide four digit PIN number on that device. While providing PIN in front of friends, relative or unknown person, it is affected by "Shoulder Surfing attack". In a shoulder surfing attack, password can be easily obtained by simply looking at the fingers of the user or by making video while user enters the password. So there is a need to develop a secure system for credit/debit card transactions that will avoid the SS and another similar type of attacks. The proposed system must contain minimum hardware changes and secure algorithms. The approach is to divert the flow of current system in such a way that whenever the user needs to put PIN code, he will be using his mobile phone to type that pin-code. The user will get the request to enter the pin code on his/her phone itself. The project proposes the technology of secure authentication system to avoid shoulder surfing (SS) attack and also the problem of identity theft is resolved to increase the faith of users in the system.

References

- Bogdan Hoanca, Kenrick Mock 2006. "Secure graphical password-a system for high traffic public areas," ETRA '06

Index Terms

Computer Science  Security

Keywords

Shoulder Surfing (ss)  Point Of Sale (pos)  Personal Identification Number (pin).