Abstract

The emergence of computer has greatly fuelled the advancement of Science and Technology and drastically changed the way human live. Beside these advancements is increasing sense of insecurity and apprehension. Security issues, particularly those relating to users, which include identification, authentication, authorization and accountability, have always been a challenge to banking transactions. As the number of customers in banking system increases, the banking channel becomes a target for criminals to carry out their activities. Series of security challenges in automatic teller machine (ATM) transactions are: Identity Theft, Impersonation, Skimming, Entrapping of smartcard, personal identification number (PIN) theft, Phishing, Insider attacks and physical attack. The existing ATM authentication method involves PIN and smartcard usage for customer privacy protection and fraud prevention. Hence, this research is focused on developing a model that allows Iris recognition into an automated teller machine authentication processes.
Iris authentication combine with PIN were adopted for authentication in ATM transaction in this study due to its accuracy, relatively low cost, small size, and ease of integration into different programming language. Window based application (IriSoft) was developed using NetBeans 8.0 IDE and Wamp Server 2.4 x86 to build database application package. In the iris recognition approach, to implement iris localization, segmentation and normalization VeriEye Software Development Kit (SDK) version 10.0 extended SDK which contain iris extractor and iris comparism component were utilized. The process involves a pre-enrolment of users with PIN and irises in the database. While during verification, user will stand in front of camera attached to the computer for scanning of the iris, after which the comparism of the sample iris image would be matched with the sample feature which had been stored up in database.

The model developed was tested and verification exercise was successfully carried out. The new system was found out to be more efficient when compared with the existing PIN authentication method. The verification time was very small and measured in seconds. Furthermore, the program (IriSoft) was subjected to standard indicator for checking the effectiveness, accuracy and performance of iris pattern matching. The Fake Acceptance Rate (FAR) was 0% while Fake Rejection Rate (FRR) was found to be 99.94% implying that it was not possible for any fraudster, to match the identity of another individual in the database; whereas there was a chance of 1.6% of an authentic user to be denied access which is very minimal. ATM users should be security conscious while withdrawing money to prevent forced withdrawal. Banks should also ensure end-to-end encryption is in place to protect data as it travels from users through internet to bank servers. Government should be involved in awareness campaign. Having realized the importance of iris recognition authentication in ATM, a holistic approach is recommended that individual users, bank and government play their role; bearing in mind that no security systems can be wholly full proof.

References

Multi-Factor Authentication Model for Integrating Iris Recognition into an Automated Teller Machine

14-17.


Index Terms

Computer Science Security

Keywords

Automatic Teller Machine (ATM), Fake Acceptance Rate (FAR), Fake Rejection Rate (FRR), Iris Recognition, Multi-Factor Authentication (MFA).