Abstract

"User Authentication Using Keystroke Dynamics." It is a method to get the user
User Authentication using Keystroke Dynamics

authentication on an android application by using the keystroke dynamics of the user using Artificial Neural Networks with the help of Error Back Propagation algorithm. In this application the user enters the password 30 times and databases are used to record 45 factors that describes a user's keystroke patterns like di-graph, dwell time, tri-graph, flight time, finger size, button pressure, coordinate values which can be seen by the user in real time. Once this is done the data is taken and put in an Artificial Neural Network and trained using Error back propagation Algorithm. This process done over time produces trained set off weights that would produces an already calculated value in the output layer. This data from the network is again stored in a separate table which is then used to check the authentication of the user typing the password.

References

- J. D. Umphress and G Williams, "Mobile Authentication Using Keystroke Dynamics", International Conference on communication, Jan 2015
- Pauli Henrique Pisani, Ana Carolina Lorena, A systematic review on key stroke Dynamics, Journal of the Brazilian Computer Society, Nov. 2013
- Fabian Monrose, Aviel D. Rubin, Keystroke dynamics as a biometric for authentication, Feb 2000
- Hyoung-jooLee,Sungzoon Cho, "Retraining a keystroke dynamics-based authenticator with impostor patterns", in ELSEVIER.

Index Terms

Computer Science  Security

Keywords

Artificial Neural Networks  Error Back Propagation Algorithm  Keystroke Dynamics
Database Systems

Mobile Phones

Passwords

Pins (personal Identification Numbers)

Android

Biometric Authentication