**Bring your own device: security challenges and a theoretical framework for two-factor authentication**


## ABSTRACT

In this paper, the security challenges of BYOD are discussed, including existing security solutions which often are too restrictive. Data leakage is one of the security challenges confronting BYOD. Data leakage can occur as a result of stolen, lost or compromised employee devices. When an employee device is stolen, lost or comprised, an attacker can obtain access directly to the enterprise data on the employee device if a strong authentication technique is not in place. The traditional means of authenticating employees when connecting to an enterprise server in a traditional network environment which relies on either knowledge or ownership is too weak for the BYOD environment. In such a traditional enterprise network, employees obtain access to an enterprise server using their respective stationary desktop, while in a BYOD environment access to an enterprise server is from anywhere, making it easy for an attacker in possession of an employee device and password to gain unauthorised access. To address this problem, there is need for a strong authentication technique. This study proposes a theoretical framework for a two-factor authentication method that combines knowledge-based (Password) and biometric-based (Keystroke dynamic) features for authentication of mobile devices in a BYOD environment. Technical details on how the framework can be implemented are presented. It is the belief of the authors that proper implementation of the proposed potential future application framework will go a long way in addressing the problem of data leakage in a BYOD environment.



**Keyword:** BYOD; Mobile device; Authentication; Biometric; Keystroke dynamic