Abstract

Smartphones and other mobile computing devices are being widely adopted globally [1]. The increasing popularity of smart devices has led users to perform all their day to day activities using these devices [2]. Hence, M-banking has become more convenient, effective and reliable [3]. It is extremely necessary to provide the security services including; confidentiality, integrity, and authentication between the financial institutions' servers and the mobile device used by the customer, as their communications are through unsecured networks such as the Internet [4]. Users' confidential information may be at risk due to fixed values-based security schemes, one level authentication, separate hard token-based authentication, hardware stealing, and Android-Based attacks. This paper specifies a comprehensive sought of how M-banking schemes can be assessed. Also it introduces a solution to mitigate most of these
Secure Android-based Mobile Banking Scheme

risks.

References

- Narendiran, Rajendran and Albert, "PUBLIC KEY INFRASTRUCTURE FOR MOBILE BANKING SECURITY".
- Analysis for Vetting Undesirable; IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 11, NOVEMBER 2014.
- Jinseong, Micinski, Jeffrey, Nikhilesh, Foster, Fogel, and Millstein, "Dr. Android and Mr. Hide: Fine-grained Permissions in Android Applications"; SPSM&apos;12, October 19, 2012, Raleigh, North Carolina, USA.
- Backes, Gerling Hammer, and Styp-Rekowski, "AppGuard - Enforcing User Requirements on Android Apps A"; Saarland University, Saarbrücken, Germany.
- Sangram Ray and G. P. Biswas, "Design of Mobile Public Key Infrastructure
- Chang-Lung Tsai Chun-Jung Chen and Deng-Jie Zhuang, "Secure OTP and Biometric Verification Scheme for Mobile Banking; Third FTRA international conference on mobile, Ubiquitous and intelligent computing, 2012.
- Morris Dworkin, "Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices; NIST Special Publication 800-38E, January 2010.

**Index Terms**

Computer Science 

Security

**Keywords**

Dynamic Initialization vector 
Overlaid AES modes 
Multi-Layer Authentication 
Variable keys