10th International Conference on Cyber Warfare and Security (ICCWS), Kruger National Park, South Africa, 24 - 25 March 2015

Fingerprint Match-on-Card: Review and Outlook

Meshack B. Shabalala, Terrence Moabalobelo and Johannes van der Merwe Modelling and Digital Science (MDS), Information Security
Council for Scientific and Industrial Research (CSIR)
Pretoria, South Africa
{mshabalala, tmoabalobelo, jvdmerwe3}@csir.co.za

Abstract

As cybercrime is on the rise, individuals would like to rest assured that their authentication information cannot be stolen, and then used to gain access to their privileged information. Smart cards can and have played a pivotal role in lowering the statistics on identity theft. This has been achieved by predominantly implementing biometrics matching algorithms inside smart card technology. The biometric matching inside a smart card is known as Match-on-Card/On-Card comparison. However compared to traditional biometric systems implemented on PCs' and servers, smart cards are resource constrained. In addition smart cards do not implement mathematical functions such as trigonometry since they are mainly meant for secure data storage and simple processing. The current state of the On-Card biometric comparison technology is limited in that data for On-Card comparison either has to be pre-calculated outside the card at runtime or fetched from a look-up table. This is because of the limited mathematical operations available inside a smart card. The pre-calculation of data outside the smart card compromises the security offered by the card and the look-up table limits the accuracy of the biometric comparison. The paper reviews the techniques and challenges of implementing fingerprint On-Card comparison algorithms in a smart card environment. Approaches of overcoming the On-Card comparison challenges are also discussed.