Chapter 30
A Perspective on Using Blockchain for Ensuring Security in Smart Card Systems

Ankur Lohachab
https://orcid.org/0000-0002-5291-7860
Kurukshetra University, India

ABSTRACT

Due to the momentous growth in the field of Internet of Things (IoT), various commercial and government organizations are exploring possibilities of mass issuance of smart cards in different applications. Widespread deployment of smart card-based systems in heterogeneous environment would facilitate card holders to participate in these applications in a personalized manner. Despite the security features, valuable data and access to decisive services make these systems prime target for attackers. These systems can be subjected to a range of security attacks – from hardware exploitation to exploitation of software bugs, from unauthorized data access to social engineering, and so forth. In the future, where many sectors will be trying to adopt the concept of Blockchain, it will create new opportunities for benefiting citizens with enhanced security over their data. In this chapter, the author performs in-depth analysis over the role of Blockchain in securing the smart card ecosystem.

INTRODUCTION

Introduction of the concept of smartness in technology is bringing more promising solutions to the modern digital world. Wireless Sensor Networks (WSNs) are taking the form of Internet of Things (IoT), chip cards are getting transformed into smart cards, and so forth. By addressing the issues of advanced underlying technologies like WSN, IoT further extends the idea of inter-connected networks by embedding networking features into physical world objects. In a similar fashion, smart cards also extend the concept of chips cards by making them more resourceful. Although magnetic-stripe enabled cards remained popular for around 30 years, industries over time have realized the need of storing more static data over the card itself. However, due to certain limitations as given in Table 1, magnetic-stripe cards are not considered as a reliable choice.

DOI: 10.4018/978-1-7998-5351-0.ch030

Table 1. Magnetic-stripe cards and limitations

Parameter	Description
Security	These cards provide minimal level of security because it is easy to read and write data from these cards very easily. Hence, information can be easily stolen and the card can be easily duplicated.
Storage	These cards have limited amount of storage and thus can store only limited amount of information.
Functionality	Magnetic stripe cards support restricted functionality and thus, are not suitable for many real-time applications.
Biometric information storage and matching	These cards cannot store biometric templates of users as well as do not support on-card biometric matching.
Data diversity	These cards are not capable of storing diverse types of data.
Digital signature storage	These cards cannot store digital signature for enabling efficient auditing process.
Two-factor authentication	These cards do not support two-factor authentication.

Upon realizing these limitations, researchers are continuously putting efforts on the same-sized cards in order to make them more convenient. These cards are referred as "smart cards" as unlike chip or magnetic-stripe cards, they not only have a unique identifier, but can also participate in automated transactions in a secure manner (Jiang, Ma, & Wei, 2018). Advent of technologies like Micro-Electro-Mechanical-Systems (MEMS) makes it possible to embed more features and functionalities on the card. For instance, Radio Frequency Identification (RFID) enabled cards work in a contactless fashion that have certain level of benefits as compared to contact cards. Other points that distinguish smart cards from magnetic chip cards include difficulty of duplication, more durability, more security, more cost, and so forth. Microprocessor chips used in the smart cards are not very different from those of a modern personal computer, but they have very limited functionality. For instance, Trusted Computing Base (TCB) (the amount of code trusted by the CPU for enabling secure operations) is very limited in the smart card chips. Despite the fact that these chips are only 9 mm^2 less as compared to processors, they contain sufficient amount of memory (Rankl & Effing, 2004). However, as this memory is not suitable for executing complex algorithms, the operations are generally performed over it considering the resource constraints.

Since the applications of smart cards range from diverse payment based applications to healthcare and citizenship cards, the security features must be robust enough for ensuring the safe-keeping of end user's data. Various public and private organizations have successfully implemented or are trying to implement standards, such as Europay, MasterCard and Visa (EMV) in payment based smart cards (Mayes & Markantonakis, Smart Cards, Tokens, Security and Applications, 2008); (Degabriele, Lehmann, Paterson, Smart, & Strefler, 2012); (Ward, 2006). These smart card issuing organizations claim that their cards encompass unique features that may be advantageous to the users as shown in Figure 1 (Thornton, 2017). However, same security standards may not be able to satisfy the security requirements of heterogeneous applications. Smart card security problems can be associated with hardware and software aspects, where hardware include smart card chip and reader, and software include application programs, operating system and user interface, and all are required to be secured (Guyot, 2010). Service providers are endeavouring to protect the data which is considered as treasure in the smart world. However, attackers are somehow becoming capable of stealing the sensitive information. Although, many encryption algorithms are present in the literature, now-a-days, researchers are implementing light-weight encryption schemes on these devices due to resource constraints. Data Encryption Standard (DES) has been implemented in the smart