Secure RFID Application Data Management Using All-Or-Nothing Transform Encryption*

Namje Park[1] and Youjin Song[2,**]

[1] Computer Science and Engineering, Arizona State University,
699 S. Mill Avenue, Tempe, Arizona, AZ 85281, USA
namjepark@gmail.com
[2] Department of Information Management, Dongguk Univertsity,
707 Seokjang-dong, Gyeongju, Gyeongsangbuk-do, 780-714, Korea
song@dongguk.ac.kr

Abstract. Ensuring the security of RFID's large-capacity database system by depending only on existing encryption schemes is unrealistic. Therefore, data sharing for security management to supplement it is drawing attention as an extremely secure scheme. However, applying the existing secret sharing scheme to this method makes the size of the share equal to that of the original data. Thus, it is not suitable for application to large-scale database. This paper proposes secret sharing algorithms that enable efficient data sharing security management based on the characteristics of the All-Or-Nothing Transform encryption mode. The proposed algorithms enable fast sharing and reconstruction in terms of processing speed and allow the sum of shares to be equal to that of the plaintext, thereby making them suitable for large-capacity database storage.

1 Introduction

While common RFID technologies are used in B2B (Business to Business) models like supply channels, distribution, logistics management, networked mobile RFID technologies are used in the RFID reader attached to an individual owner's cellular phone through which the owner can collect and use information of objects by reading their RFID tags; in case of corporations, it has been applied mainly for B2C (Business to Customer) models for marketing [1]. Though most current RFID application services are used in fields like the search of movie posters and provision of information in galleries where less security is required, they will be expanded to and used more frequently in such fields as purchase, medical care, electrical drafts, and so on where security and privacy protection are indispensable.

With the question of secure storage and management of mobile RFID's personal data becoming an increasingly urgent matter, data is encrypted to eliminate threats to security. However, the encryption scheme requires plenty of time and memory for

* This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology(No. 2009-0087849)

** Corresponding author.

G. Pandurangan et al. (Eds.): WASA 2010, LNCS 6221, pp. 245–252, 2010.

encoding and decoding. Since the encryption scheme such as Advanced Encryption Standard (AES) encodes confidential information in its entirety, there is a risk of entire outflow of said information once the secret key is decoded; hence the difficulty of key distribution and management. Unlike the encryption scheme, there is no such thing as life of a key under the secret sharing scheme, which presents no problem in renewing the public certificate of authentication and helps reduce considerable operational expenses. In contrast, under the existing secret sharing scheme [2], if the original data are separately stored, the size of share (i.e., distributed information) becomes equal to that of the original data; thus increasing the data volume to be stored. Recently, security has been found to be improvable without reducing the efficiency of the existing encryption scheme through the appropriate transformation of plaintext (in encryption mode) before encoding it.

This paper proposes secret sharing algorithms having the characteristics of All-Or-Nothing Transform (AONT), aiming for long-term, secure, and efficient storage of large-capacity data. In other words, algorithms for the sharing and reconstruction of large-capacity data whose security is improved using the AONT encryption mode and to which XOR operations are applied to boost efficiency are suggested. The research results of this paper are expected to be utilized as algorithms that ensure availability and manage the efficient distribution of large-capacity data including highly confidential data and secrets involving customers' personal information, even though some of the data are leaked to the outside.

2 Secure Data Management in Networked Mobile RFID

Network mobile RFID middleware applications may access application tag data in three ways. The left below is a diagram of a tag being read by a mobile RFID reader to get a key [5]. This is used by an application to access database storage to get additional data. Note that key and storage contain application data, such as personal data, etc. This is at risk of theft and abuse. In the middle, tag key and data are both read by a mobile RFID reader to get the personal data, etc. In this case, no additional data is required. Note that both key and data may contain sensitive data that is at risk. On the right, RFID tag key and data are read by a mobile RFID reader to get the personal data, etc. Key also used by an application to access storage to get additional data, such as whether this person is on a specific watch list. This is the most challenging combination because key, data, and storage are all at risk.

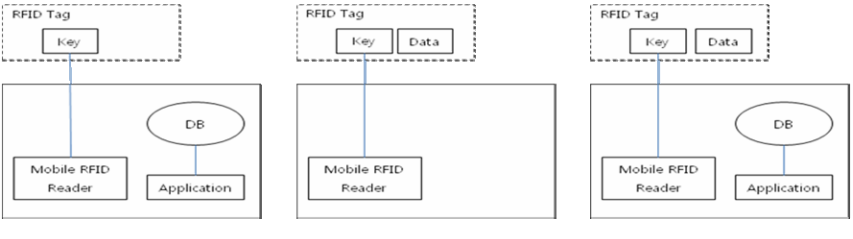

Fig. 1. Secure Data Management in Mobile RFID Environment