AONT Encryption Based Application Data Management in Mobile RFID Environment*

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

[1] Department of Computer Education, Teachers College, Jeju National University,
61 Iljudong-ro, Jeju-si, Jeju Special Self-Governing Province, Korea
namjepark@jejunu.ac.kr, namjepark@gmail.com
[2] Department of Information Management, Dongguk Univertsity,
707 Seokjang-dong, Gyeongju, Gyeongsangbuk-do, 780-714, Korea
song@dongguk.ac.kr

Abstract. Mobile RFID (radio frequency identification) is a new application that allows the use of a mobile phone as a wireless RFID reader and provides new services to users by integrating RFID and the ubiquitous sensor network infrastructure with mobile communication and wireless internet services. Ensuring the security of mobile RFID's large-capacity database system by depending only on existing encryption schemes is unrealistic. In this regard, data sharing for security management has drawn 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, making it unsuitable for application to a large-scale database. To address this problem, this paper proposes secret sharing algorithms that enable efficient data security management through the use of the characteristics of the all-or-nothing transform (AONT) encryption in RFID middleware.

1 Introduction

Radio Frequency Identification (RFID) technology is being actively developed to exploit its global market potential. At the same time, it has raised fears among those who believe that it could facilitate a 'Big Brother' society. Thus, technology development efforts in areas such as tags, readers, and middleware should address not only information and market needs but also privacy and security concerns. The excessive limitations of RFID tags and readers have made it impossible to apply present codes and protocols. Technologies for information and privacy protection should address the general interconnection among elements, and their RFID characteristics should closely reflect the RFID environment.

Common RFID technologies have been used in B2B (business to business) models (e.g., supply channel, distribution, and logistics management), whereas mobile RFID technologies have been used in the RFID reader attached to an individual owner's mobile phone, through which the owner can collect and use information on objects by

* 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.

J.-S. Pan, S.-M. Chen, and N.T. Nguyen (Eds.): ICCCI 2010, Part II, LNAI 6422, pp. 142–152, 2010.

reading their RFID tags. Corporations have applied mobile RFID technologies mainly to B2C (business to customer) models for marketing. Although RFID services have been limited largely to fields requiring less security (e.g., searching for movies and providing information in galleries), such services are expected to be applied more extensively to fields that necessitate privacy and security (e.g., purchasing, healthcare, and electrical drafts).

The secure storage and management of RFID's personal data has become an important issue, leading to the encryption of data to address security threats. However, the encryption scheme requires a lot of time and memory for encoding and decoding. Because encryption schemes such as the Advanced Encryption Standard (AES) encode confidential information in its entirety, there is a risk of the outflow of entire information once the secret key is decoded; hence, the distribution and management of the key is difficult. Unlike the encryption scheme, there is no such thing as the life of a key under the secret sharing scheme; thus, secret sharing scheme presents no problems in terms of public key certificate-based authentication and can substantially reduce operational costs. By contrast, under the existing secret sharing scheme[1], if original data are separately stored, the size of share (i.e., distributed information) equals that of the original data, increasing the data volume to be stored. Recently, it has been found that transforming the plaintext (in the encryption mode) before encoding improves data security while maintaining the efficiency of the existing encryption scheme[2].

This paper proposes the secret sharing algorithms that incorporate the characteristics of the all-or-nothing transform (AONT) encryption mode for the long-term, secure, and efficient sharing, storage, and reconstruction of large-capacity data. That is, the security of the algorithms is improved using the AONT encryption mode, and XOR operations are applied to the algorithms to boost their efficiency. The proposed algorithms are expected to be used for efficiently managing the distribution of large-capacity data (including highly confidential data on customers' personal information) even when there is data leakage from the RFID tags.

The rest of this paper is organized as follows: Chapter 2 describes a secure data management in networked mobile RFID, the AONT encryption mode related to this research and XOR secret sharing scheme; Chapter 3 reviews and designs the proposed algorithms, and Chapter 4 analyzes the proposed scheme; finally, Chapter 5 presents the conclusion.

2 Related Research

2.1 Networked Mobile RFID Technology

RFID is expected to be the base technology for ubiquitous network or computing, and to be associated with other technology such as telemetric, and sensors. The mobile phone integrated with RFID can activate new markets and end-user services, and can be considered as an exemplary technology fusion. Furthermore, it may evolve its functions as end-user terminal device, or 'u-device (ubiquitous device)', in the world of ubiquitous information technology.