Security and Privacy on Personalized Multi-Agent System

M

Soe Yu Maw
University of Computer Studies, Mandalay, Myanmar

INTRODUCTION

Nowadays, the rapid growth of the mobile technologies changes the peoples' lifestyle. Mobile devices play a very important role in information and communication technology because of the easily acquisition of information from anywhere and at anytime. Personalization plays an important part in mobile services and can be considered as an added value, with mobile technologies, services can be tailored to the individual user.

Recommender system can be defined as a specific type of information filtering (IF) technique that attempts to present information items (movies, music, books, news, hotels and restaurants, interesting places and so on) those are likely of interest to the user. The recommender systems serve the personalized information to the users according to the user's interest or preference based on their profiles.

Agent-based systems are widely used for mobile and which can interact much more personally with the users. Mobile agent can migrate from one resource to another and retrieve the personalized information from the database across the Internet and gives the results to the user. A multi-agent system can manage end user requests and dynamically building a user's profile. Agents run on mobile devices and can provide personalized assistance to mobile users. Although the personalized multi-agent system provides many benefits to the mobile user, there need to consider the issues of security and privacy.

Security and privacy is a key to any system architecture and essential requirements for personalization system which primarily concerns the storage of user profiles. Cryptography is an important component of secure information and communications systems. Cryptography is a discipline that embodies principles, means, and methods for the transformation of data in order to hide its information content, establish its authenticity, prevent its undetected modification, prevent its repudiation, and/or prevent its unauthorized use.

Cryptography can be used as a key to security and privacy issues to achieve the confidentiality, data integrity, and authentication such as personal data, whether that data is in storage or in transit. Confidentiality and integrity are taken care of by the encryption algorithms. Encryption is used to secure communications and data storage, particularly authentication credentials and the transmission of sensitive information.

In this article, symmetric key primitive of block cipher is chosen to ensure the confidentiality and integrity of information. Advanced Encryption Standard (AES) is an iterated block cipher algorithm which is designed to be extremely secure. The main focus of this article is to address the security and privacy aspects on users' personal information and preferences by applying AES algorithm to ensure the confidentiality and integrity for personalized multi-agent system in a mobile application environment.

BACKGROUND: CRYPTOGRAPHY MAIN TECHNIQUES

In this section, the definition, overview of the main techniques and the literature review of the related works are presented.

Cryptography

Cryptography is the science of mapping the plaintext into ciphertext and vice versa (called encryption and decryption) by using algorithms with mathematical functions. Cryptography provides the services of confidentiality, authenticity, integrity, non-repudiation and secrecy. In general, there are three types of cryp-

DOI: 10.4018/978-1-4666-5888-2.ch567

tographic primitives: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography and un-keyed (hash functions).

Symmetric (Secret Key) Cryptography

A single key is used for both encryption and decryption which transforms plaintext into ciphertext using a secret key and an encryption algorithm. Using the same key and a decryption algorithm, the plaintext is recovered from the ciphertext (Stallings, 2006).

Symmetric key cryptography is categorized as stream cipher and block cipher. They provide data confidentiality by encryption. Stream ciphers partition the text into small blocks which operate on a single bit (byte or computer word) at a time and implement some form of feedback mechanism so that the key is constantly changing (a different key is generated for each block). A block cipher partition the text into relatively large (e.g., 128 bits) blocks and encrypts one block of data at a time using the same key on each block. Algorithms of symmetric key cryptosystems are DES, Triple DES, AES and so on.

Asymmetric (Public Key) Cryptography

Asymmetric encryption is a form of cryptosystem in which encryption and decryption are performed using the different keys (a public key and a private key). Public-key encryption algorithm transforms plaintext into ciphertext using a one of two keys. Using the paired key and a decryption algorithm, the plaintext is recovered from the ciphertext. It can be used for confidentiality, authentication, or both (Stallings, 2006). Algorithms of asymmetric key cryptosystems are RSA, Diffie-Hellman, ElGamal, Digital Signature Algorithm (DSA), Elliptic Curve Cryptography (ECC) and so on.

Hash Function

Hash function, called message digests and one-way encryption. The algorithm uses no key and a mathematical transformation to irreversibly encrypt information. A function that maps a message of any length into a fixed-length hash value, which serves as the authenticator. The purpose of a hash function is to produce a "fingerprint" of a file, message, or other block of data, to encrypt passwords and provide a measure of the integrity of a file (Stallings, 2006). Hash functions are also commonly employed by many operating systems to encrypt passwords and Message Digest (MD) algorithms, Secure Hash Algorithm (SHA), Tiger and so on.

Advantages of Cryptography Methods

Each cryptographic primitive is optimized for some specific application. Secret key cryptography is ideally suited to encrypting messages which provides privacy and confidentiality. Secret key cryptography operates about 1000 times faster than public-key cryptography. Public-key cryptography can be used for non-repudiation and user authentication. Hash functions are well-suited for ensuring data integrity with high degree of confidence.

Symmetric iterated block cipher architecture is adopted in the implementation of the proposed personalized recommendation of the multi-agent mobile system to address the security and privacy issues.

Advanced Encryption Standard (AES)

In 2001, National Institute of Standards and Technology (NIST) announced the Rijndael algorithm as Federal Information Processing Standards (FIPS) for the Advanced Encryption Standard (AES) to replace the Data Encryption Standard (DES) algorithms which specifies cryptographic algorithm that can be used to protect electronic data. The Rijndael algorithm is designed to handle additional block sizes and key lengths. However, the additional features are not adopted in the AES. The AES algorithm can be implemented in software, firmware, hardware, or any combination (FIPS PUB 197, 2001).

Figure 1 shows the overall structure of AES encryption and decryption with a single 128-bit block as input. This algorithm processes the entire data block in parallel during each round using substitutions and permutations. Each round and the initial stage require a 128-bit round key. Therefore, 11 sets of round keys are generated from the secret key. The input data