Journal of computer science and software applications
https://www.mfacademia.org/
ISSN:2377-0430
Vol. 3, No. 2, 2023

Data Encryption for Privacy Protection in Social Apps

Daniel Lewis

Radford University

Daiellewis@radford.edu

Abstract:

The advent of the big data era has brought the issue of privacy leakage during data release and transmission to the forefront of information security research. Among the prevalent privacy protection techniques are anonymization, data encryption, and differential privacy. This study employs data encryption technology to simulate the development of a social application. The application encrypts user-released information and implements a password protection mechanism. Only individuals with the correct password can access the encrypted data, thereby safeguarding user privacy and preventing the exposure of personal information in textual content and images.

Keywords:

Big data, privacy protection, data encryption, social app.

1. Introduction

Today is the era of rapid development of the Internet, the use of the Internet has become an indispensable part of people's lives. In the process of using the Internet, many platforms often need to publish and release some data information to facilitate the use of relevant data. [1] However, the disclosure of data will also bring the risk of privacy disclosure. Generally, public data contains a lot of personal information. Once the information is mastered by criminals, it is possible to use this information to do some illegal things. This is due to the disclosure of personal privacy in the environment of big data. Therefore, it is very important to study privacy protection in big data environment.

2. Development Status

The research on privacy protection technology is usually realized by mining algorithms, improving and improving some association rules, and carrying out the related work of privacyprotection before the publication of privacy data, so as to realize the protection of privacy information.[2]

Data encryption mainly includes homomorphic encryption, symmetric encryption, asymmetric encryption, secure multi-party computing, ciphertext retrieval and other commonly used cryptography technologies. The main function of data encryption is to solve the security of data storage, analysis and application and data communication.[3] However, homomorphic encryption scheme is not suitable for privacy protection in big data environment. AES algorithm is the representative of symmetric encryption technology.[4] RSA algorithm is the traditional encryption method of asymmetric encryption technology. K-anonymity (k-anonymity) is a data encryption method first proposed by samarati and Sweeney in 1998. [5]It uses the sensitive attributes in the original data to protect against leakage. Differential privacy is a provable and strict privacy protection model.

3. Implementation of Social App with Privacy Protection Function

The emergence of social software has broken the boundaries of geography and time. Users can share some good times and life insights in their lives in various social apps by publishing dynamic information, which broadens the channels for relatives and friends to understand themselves and shortens the distance between people. However, the dynamic information released on social app

faces the risk of personal privacy disclosure. Once the information is used by criminals, it will have a great impact on people's lives. Therefore, to achieve privacy protection in the big data environment, it is necessary to encrypt the data and set the password for the information released in the social app. When publishing some information that may involve personal privacy, the password should be set and then released. Only the password should be told to the trusted friends, while other strangers and illegal attackers can not access the released information without knowing the password, so as to realize the function of privacy protection.

3.1. Function Design of Social App Client with Privacy Protection Function

The app has the functions of user registration, user login, user release information (encryptionrelease can be selected), user view released information, user modify personal information, user modify personal password, log out and other functions.

Social App needs users to register reasonably before they can log in to their accounts, and it should ensure that users can modify their personal information and password to improve the work of accounts. The information released by users that need privacy protection should be encrypted to ensure that legitimate users can read encrypted information and prevent illegal attackers from gaining malicious information. The function flow of the app is as follows.

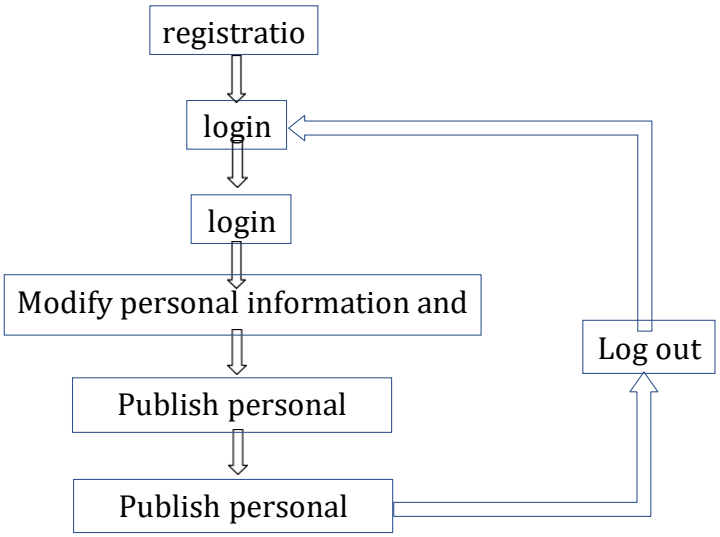

Figure 1. Function flow

After the user enters some registration information locally according to the requirements, the app will receive the return result of the registration and prompt the customer that the registration is successful or the registration information is incomplete.

The user enters the registered account and password, sends a login request to the app, and obtains the returned login result from the big data management app. If the account does not exist or the password is wrong, the user cannot log in successfully.

After the user successfully logs in, there will be "home page" interface and "my" interface in theapp. Click "my" interface to see "modify personal data", and click to modify user information.Similarly, in the "my" interface, the "change password" will be displayed. After clicking, the user's password can be modified. Only by inputting the original password and entering a new password twice can the password be successfully modified.

After clicking "log out" in the "my" interface, a request will be sent to the program to log out. After confirming to log out, you can exit the current account.

When users want to publish information that may involve personal privacy, they can choose toset a password to encrypt the publication. If the information can be made public, then there is no need to set a password.

When other users want to view the published encrypted information, they need to enter the correct password to view the details. When viewing the unencrypted information, they can directly click to

view it.

3.2. Design of Database in Social App with Privacy Protection Function

The database used in this paper is SQLite database (acid compliant relational database management system), which is a lightweight database and the most common andorid client database. This database interface is more, the operation is convenient, and the occupation of resources is less, which is suitable for mobile user clients to use.

Two databases are used in the design. The first is uesrdb, which stores the user's information. It corresponds to the user's personal data at the initial registration, including user name, password, nickname, gender, birthday, phone number, avatar and behavior. These data can be added, deleted, modified and checked in the app later. The second database is homedb, which stores the information published by users. It contains the title, content, time, password, user name and nickname of the user. These data can also be added, deleted, modified and checked in the app.

3.3. Implementation of Social App with Privacy Protection Function

3.3.1. App Development Environment and Encryption Algorithm

In the previous part, the function design of big data management app with privacy protection function has been introduced. The app client has the functions of user registration, user login, personal data modification, password modification, log out, information release (encryption) and view and release information.

In terms of app development, it is developed by using andorid Studio software, which is a new generation of Android integrated development environment developed by Google company, which is more intelligent and runs faster. The compiler language used is java language. In terms of privacy information encryption algorithm, AES encryption algorithm is adopted. At present,AES encryption algorithm cannot be cracked by exhaustive attack, with high security and high computing efficiency. Using AES encryption algorithm to realize the information encryption and release of users on social app in big data environment has better efficiency and can ensure the security of encryption and decryption.

3.3.2. Social App Core Encryption and Decryption Algorithm

The following code shows the tool class used in AES encryption algorithm to realize the subsequent key generation, encryption and decryption process.

```
public class SymmetricEncoder {
    private static final String AES_MODE = "AES/CBC/PKCS7Padding";
    private static final String CHARSET = "UTF-8";
    private static final String CIPHER = "AES";
    private static final String HASH_ALGORITHM = "SHA-256";
    private static final byte[] IV_BYTES = {0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00};
```

Figure 2. The tool class of AES encryption algorithm

Use AES encryption and decryption tool class to generate the key in AES symmetric encryption algorithm. The role of key in big data management app is to convert information into ciphertext when publishing information, and convert ciphertext into plaintext when decrypting information. Since AES algorithm is symmetric encryption algorithm, the key used in encryption and decryption is the same.

```
private static SecretKeySpec generateKey(final String password) throws NoSuchAlgorithmException, UnsupportedEncodingException {
    final MessageDigest digest = MessageDigest.getInstance(HASH_ALGORITHM);
    byte[] bytes = password.getBytes(CHARSET);
    digest.update(bytes, offset: 0, bytes.length);
    byte[] key = digest.digest();

    return new SecretKeySpec(key, CIPHER);
}
```

Figure 3. Generate key algorithm

In the social app with privacy protection function, AES encryption algorithm is used for users to set passwords and encrypt them symmetrically when publishing information related to personal privacy. It generates ciphertext and protect users' personal privacy. In the process of encryption, first assign the value of the password set to the key in the algorithm, convert the input information into byte array, call AES encryption mode, and then pass in the encryption mode, encryption key and byte array to be encrypted, and return the result after encryption.

```
public static String encrypt(final String password, String message)
        throws GeneralSecurityException {

    try {
        final SecretKeySpec key = generateKey(password);
        byte[] cipherText = encrypt(key, IV_BYTES, message.getBytes(CHARSET));
        //NO_WRAP is important as was getting \n at the end
        return Base64.encodeToString(cipherText, Base64.NO_WRAP);
    } catch (UnsupportedEncodingException e) {
        throw new GeneralSecurityException(e);
    }
}
```

Figure 4. Codes encrypting

In the social app with privacy protection function, the function of AES decryption algorithm is that when a user wants to access the information that other users have published containing personal privacy information, they need to input the correct password, that is, the key used for decryption. When the password is correct, the ciphertext can be decrypted. In the process of decryption, it is necessary to assign the password value to the key, convert the ciphertext into a byte array, call the decryption mode of AES, and then pass in the decryption mode, decrypt the key and the byte array to be decrypted, and return the final decryption result.

```
public static String decrypt(final String password, String base64EncodedCipherText)
        throws GeneralSecurityException {

    try {
        final SecretKeySpec key = generateKey(password);
        byte[] decodedCipherText = Base64.decode(base64EncodedCipherText, Base64.NO_WRAP);
        byte[] decryptedBytes = decrypt(key, IV_BYTES, decodedCipherText);
        return new String(decryptedBytes, CHARSET);
    } catch (UnsupportedEncodingException e) {
        throw new GeneralSecurityException(e);
    }
}
```

Figure 5. Codes decrypting

4. Conclusion

Privacy protection in big data environment cannot be ignored. According to the current situation that people use social app to publish some personal information, this paper uses data encryption technology to simulate the design of a social app, which can realize user registration, login, release of dynamic information and information encryption and decryption, which can better ensure that the privacy information released by users will not be obtained and used by attackers, and corresponding measures are taken Test.

This paper only designs and realizes the privacy protection in the big data environment from the perspective of social app. To truly achieve the privacy protection in the big data environment, the government needs to improve the corresponding laws and regulations, relevant departments to strengthen supervision, Internet companies to increase investment in scientific research, relevant industries to strengthen self-discipline, and citizens to improve the awareness of privacy protection. Only in this way can we ensure that the personal privacy of citizens in the big data environment will

not be violated, and people can enjoy the convenience brought by big data to life.

References

[1] Shaomin Zhang, Jieqi Rong, Baoyi Wang: A Privacy Protection Scheme of Smart Meter for Decentralized Smart Home Environment Based on Consortium Blockchain, International Journal of Electrical Power and Energy Systems, 2020, 121-124.

[2] Yiping Wen, Jianxun Liu, Wanchun Dou, Xiaolong Xu, Buqing Cao, Jinjun Chen: Scheduling Workflows with Privacy Protection Constraints for Big Data Applications on Cloud, Future Generation Computer Systems, 2020, 108-115.

[3] Yang Xiaopeng: Research on Prediction Service Mechanism of Privacy Protection in Big Data Environment, 2017.

[4] Fang Binxing, Jia Yan, Li Aiping, Jiang Rong: Overview of Big Data Privacy Protection Technology, Big Data, 2016, vol2 (01), 1-18.

[5] Li Shengliang: Research on The Encryption Algorithm based on AES, 2015.