Allowing Profile Matched Friend Request in Social Media using AES

Atul Jacob T  
Christian College Of Engineering & Technology.  
Oddanchatram, Dindigul

Jerin Thomas  
Christian College Of Engineering & Technology.  
Oddanchatram, Dindigul

Jiju John  
Christian College Of Engineering & Technology.  
Oddanchatram, Dindigul

Joel Joseph  
Christian College Of Engineering & Technology.  
Oddanchatram, Dindigul

Mr. Dennis Ebenezer  
Assistant Professor  
Christian College Of Engineering & Technology. Oddanchatram, Dindigul

Abstract

Mobile social networks (MSN) place an important role in our day to day life. In existing system, usually all users publish their complete profile for other people to search. In this paper, a profile matching application is implemented which helps the user to find the exact match of the profile with other peoples. We propose the security protocol which helps profiling and we have increased the privacy so that less information about the user profile is revealed. We also keep the files secured using AES algorithm.

Keywords: profile matching, secure communication, MSN, AES (Advanced Encryption Standard)

I. INTRODUCTION

Social networking is grouping of individuals into specific groups. Social media is a wide range of internet based and mobile services that allow users to participate in online communities. It is also a platform to built social relations between people who share similar interests, activities, backgrounds and real-life connections. Social media also allows individuals, companies, organizations and governments to interact with a lot of people. There are number of websites focus on particular interests which means anyone can be a member, but it does not matter what their hobbies or interests are. Once you are a member of community you can be friends with similar interests and can unfriend those friends.

What is meant by Mobile Social Network?

Mobile Social Networking is networking where individuals with similar interests connect with each other by using their mobile phone. The present trend for social networking websites is to create mobile applications to give real time access and user instant from the particular device. Face to face interaction plays an important role in our day to day life, especially for social networking purposes the initiator and its matching user directly find out and connect to each other, without knowing anything about other users profile attributes, making new connections according to personal preferences to matching user profile is an important task, while the rest of the users should also know nothing about the two users matching attributes. The web based social networks is extended for mobile access through mobile browsers and smartphone applications.

Fig. 1: System Architecture.
A. Existing System

In existing system for such services, usually all users directly publishes their complete profile for other people to search. In many applications, the user’s profile may contain personal information which are sensitive and which they doesn’t want to make public. The present system addresses the verifiable privacy preserving profile matching and secure communication [2],[5]. The profiles of all participants, should not be exposed without their consents and can reduce the barrier to participate in Mobile Social Network. The two techniques used are Private Set Intersection (PSI) and Private Cardinality of Set Intersection (PCSI).

1) Disadvantages
Possibility for hackers to launch spam and virus attacks. Increases the risk of people being victim to online scams that seems original, resulting in the theft of data and the identity. It also results in the productivity loss, especially if the employees are busy in updating their profiles.

B. Proposed System

Treat the user’s profile as multiple attributes chosen from a public set of attributes provide well designed protocols to privately match user’s profiles based on the private vector dot product. In the proposed system, the AES is used to enhance the security of the files. Here the profiles of two users are taken as two matrices and the attributes such as location and hobbies of each user which is written in their profiles are compared using private vector dot product. After the comparison of the attributes we can find the similarities of two profiles and thus we can send and accept the request. The files that we need to share should be secured, we can secure the files by the encryption and decryption of the path that the file stored by using Advanced Encryption Standard.

1) Advantages
User can get better suggestion of friends based on the profile matching technique. The security of the files is enhanced by AES.

II. MATERIALS AND METHODS

AES (Advanced Encryption Standard) algorithm:

AES is based on a principle called substitution permutation network. It is very fast in both the software and hardware. AES has a constant block size of 128 bits and key size of 128, 192, or 256 bits [10]. AES is symmetric key algorithm. It operates on a 4x4 matrix of bytes, termed as the state. AES cipher is specified as a number of repetitions of transformation rounds that converts input plain text into the final output of the cipher text. The each round consists of several processing steps, including one that depends on encryption key. A set of reverse rounds are applied to transform cipher text back into the original plain text using same encryption key.

The following are the four stages or steps in a round of AES. The sub bytes step is the first step in a round of AES. In this each byte in the matrix is updated using the 8-bit substitution box.

![SubBytes](image)

Fig. 2: Each byte replaced with its entry of 8-bit.

The shiftrows step is the second step, it operates on each of the rows of the state and it shifts in a cyclic manner [10].

![ShiftRows](image)

Fig. 3: Bytes in each row are shifted towards left in cyclic manner.
In the mixcolumns step, the four bytes present in each column are combined using the linear transformation.

![MixColumns Diagram](image)

**Fig. 4:** A fixed polynomial is multiplied with each column of the state.

In the addroundkey step, the each state is combined with the subkey. Each subkey is derived from the main key [10].

![AddRoundKey Diagram](image)

**Fig. 5:** XOR operation is used to combine each byte of the state with the byte of subkey.

### C. JAVA:
Java is a system for developing application software and developing in a cross-platform computing environment. It is used in various computing platforms from embedded devices and mobile phone to enterprise servers.

### D. SQL:
Structured query language (SQL) is a special purpose programming language developed for managing the data in the RDBMS (Relational DataBase Management System). Originally based on relational algebra and tuple relational calculations, SQL consist of a data definition language, data manipulation and a data control language.

### III. IMPLEMENTATION AND EVALUATION

There are four modules that should be implemented and they are authentication, Find friend, Recommendation and Data recognition module.

#### A. Authentication

In the authentication module we can register and login through the system using personal details. Admin and user are the two authentication modules. Admin is the main person to control all the user actions. The user can register and store all the data through the system. It is important when dynamic IP addressing is used for computers on the trusted network. user’s identity can be proved through this.
B. Find Friend
In the find friend module user can find friend, send request, accept request etc. Friends are suggested according to their attributes such as location and hobbies.

C. Recommendation
Recommendation is a module in which system recommend users matching friend. It is based on similarities of mutual friends that are described in the profile attributes values. These values are taken as the entity values. The system will match the entity values of profiles. If the two profiles share some similar entity values then it result shows two person may know each other.

D. Data Recognition
In the Data recognition module the system request the details of the user to store and perform auto friend matching and analysis of the corresponding method.

IV. EXPERIMENTATION RESULTS

The following are the experimentation results:

![Fig. 6: Authentication](image)

![Fig. 7: Finding Friend](image)

![Fig. 8: adding a friend and matching of two profiles based on certain attributes.](image)
In this paper we have evaluated and allowed the profile matched friend request in social media and thus privacy of the person is preserved from the third party. We ensure the security of the files using AES algorithm. We have seen that the security of the profile of users is the major issue in profile matching in mobile social network and thus we found a solution for this problem.

REFERENCES


