PRIVACY PRESERVING FOR MOBILE SOCIAL NETWORKS USING CENTRALIZED NETWORK MODEL

*Divya Paunikar, *Sami Sayed, *Sakshi Singh, **K.S.Charumathi
Department of Information Technology, Pillai College of Engineering, New Panvel

Abstract:

In this project, we propose a privacy-preserving data retrieval program for mobile social networks. The program enables users to retrieve data from other users who are interested in some topics related to a subject of interest. We define a subject to be a term that can cover many congealed topics. We propose a centralized network model. In this model users are allowed to securely outsource data to a server such that the server matches the users who are interested in the same topic(s) and have defined social attributes with privacy preservation. Users will store a topic of subject of interest and the users details will be encrypted with encryption algorithm which enables the server to match the topic and attributes without knowing any private information. Our implementation can preserve the privacy of the MSN users with high performance.

Keywords: *Social networking services; cryptography; privacy; Data Security; Data retrieval.*

I. INTRODUCTION

Mobile social networks (MSNs) are specific types of social media which consolidate the ability of omnipresent connection for mobile users/devices to share user-centric data objects among interested users. Taking advantage of the characteristics of social networks , MSNs are capable of providing an efficient and effective mobile environment for users to access, share, and distribute data. Many promising applications of MSNs require exchanging information on a subject of interest. The security and privacy in MSN applications are becoming a real concern. People are always reluctant to reveal any personal information about their interests to protect their privacy. Subjects/topics of interest may leak sensitive information such as personal health status, sexual orientation, political preferences, etc. MSN users need to privately connect with other users who have similar topics and prevent other users who do not have similar subjects from learning any information about them. Users query the server to connect to other users with certain subjects and topics of interest. The server can connect the users without knowing any information about the subjects and topics of interest. The server enforces the policy when it connects users. In order to preserve their privacy, users use a searchable encryption scheme to encrypt the topics of interests and a proposed cryptography construct to encrypt the attributes and subjects before uploading them to the server. Using these ciphertexts, the server can match the users without knowing any private information.

II. OBJECTIVES

The program aims to achieve the following:

1. Privacy-preservation: the proposed profile matching protocol can preserve the user's privacy.
2. Users should not know the other users interests that are not shared. They should not also know the related topics.
3. Security: The proposed protocol's security should not be compromised and it shall maintain the same security.

III. Centralized Model

In centralized MSN approach, the users simply depend on a server and with the knowledge of the users and attributes or interests of the users the server performs the profile matching on their behalf. Hence the server is involved in every profile matching operation. Users will be notified by the server about the related groups of his/her topic of interest subscribed by the user. Though easy to implement, not all users are willing to give their personal information to the server because of the privacy concerns. The trusted server on the other hand is likely to be crowded with many users of the application in MSN, and the one-point failure problem has to be considered. Additionally, servers learn the attributes or interests of users and also servers are generally based on the connection of the internet.

Here users' profiles are not certified in this privacy model so that a malicious user has a chance to freely choose the inputs to the protocol to get more information than intended. So this work is proposing a private matching by the server using certified attributes to defend against malicious users. This architecture is easy to manage, and effective in guaranteeing the security of the profile making. Mobile social network applications run social network applications on mobile devices and also making it possible for users to be mobile yet socially connected.

IV. PROPOSEDSYSTEM

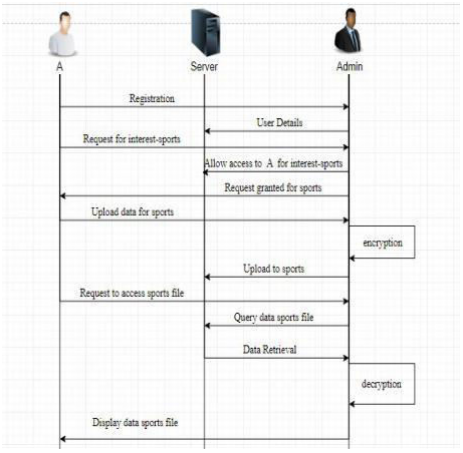

fig: System Architecture

This is a client-server architecture which exhibits several advantages of being straightforward and easy to implement, while suffering from all the drawbacks of centralized systems. This architecture is centralized and web-server-based. All functionalities, like storage, maintenance, and access to MSN services are offered by the commercial social network providers such as Facebook Inc., LinkedIn Corp. Most of the users want to find other users with similar interests, or organization. By data mining, affinity groups can be found. Data mining is very much efficient and effective in a central repository. However, with client-server architecture the complete data, directly or indirectly supplied by all users, is collected and stored permanently in the databases of the server, which potentially becomes a big problem capable of exploiting this data in many ways that can violate the privacy of individual users.

The representation of its users and their social connections in the real or virtual world, plus networking services for

communicating and socializing among its users. It also helps to forge new connections based on common interests.

V. Methodology

Enabling Privacy-Preserving for Mobile Users we use the AES Algorithm. The most popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six times faster than triple DES. The user subscribed interest is encrypted and that encrypted can be viewed only by the verifier and the server authority, even the verifier and the authority can view only in the form of encryption. After this only the user can decrypt it's credentials or subject interest. AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix.

Encryption Process:-

Here, we restrict the description of a typical round of AES encryption. Each round comprise of four sub-processes.Byte Substitution (SubBytes)

The 16 input bytes are substituted by looking up a fixed table (S-box). The result is in a matrix of four rows and four columns.

Shiftrows:-Each of the four rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of row. Shift is carried out as follows−

- First row is not shifted.
- Second row is shifted one (byte) position to the left.
- Third row is shifted two positions to the left.
- Fourth row is shifted three positions to the left.
- The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

MixColumns:-Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

Addroundkey:-The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

Decryption Process:-

The process of decryption of an AES ciphertext is similar to the encryption process in the reverse order. Each round consists of the four processes conducted in the reverse order −

- Add round key
- Mix columns
- Shift rows
- Byte substitution

Since sub-processes in each round are in reverse manner, unlike for a Feistel Cipher, the encryption and decryption algorithms needs to be separately implemented, although they are very closely related.

VI. Implementation And System Optimization

1. User Profile Domain: This is a personal space management that support a user to
    - Create an account (i.e., user registration)
    - Create/edit user profile
    - Upload/edit user generated contents (i.e., blog-like postings, status update)

A user's actions in her personal space will be reported to the server. As a result, uploading and editing user generated contents serve as a medium for important communication primitive between a user and the server. The user's credentials are kept private to the admin and then the user is able to view the content from the home page and thus can view more about the same interest. Here, the user will be asked to encrypt it's personal details while signing into the system and then the admin generates an Id which is given to the user. Thus the users will only be able to see the blogs or interests and cannot hack any user's details. Here the privacy of the user is preserved. The user also has the privilege to access the data that is uploaded by other users belonging to the same interest. All the users belonging to the same interest can share the data among themselves.

2. Server Domain: Server plays the important role to store the data about the users private information which is encrypted. In this we are using MySQL database which is most common.

Privacy of the user's credential is done using cryptographic hash algorithms which are generated automatically which becomes difficult for intruders to exploit the data.

3. Admin Controller: The admin plays the role of interpreter between the users and the database server. The responsibility of the admin in this system is to observe any authenticated user does any illegal activity against the terms and condition of the system and also give users it's personal Id. If false activity by the authenticated user is encountered then he/she is warned for maintaining the privacy terms of the system or else is removed. It is also responsible for maintaining the privacy of data and also as a login & registration portal for the user. It makes sures the connection between the database and admin is secured.

VII. Conclusion and Future Scope

This paper presents the working methodology and development of the project "Privacy preserving for mobile social networks using centralized model".

Social media apps have always been a strong part of the IT market. MSNs face various safety issues and challenges from different disciplines such as trust, security, and privacy. The Project used the centralized model to securely encrypt and upload the data to a central server where other users who have the same subject and topics can query the server for subject or topic matching. For providing safety in MSNs trust, security and privacy are the things which are needed. In this program encryption algorithm is used for security of data in a centralized way.

Thus, several performance metrics have been proposed and the proposed program extensively evaluated and the results indicated that the proposed program can preserve privacy with high performance and low overhead. Although there are limitations which will be considered for improvement in future work.

VIII. REFERENCES

[1] Vigneysh Aravindh, "Stamp: Enabling Privacy preserving location proofs for mobile users" International Journal of Scientific & Engineering Research Volume 8, Issue 8, August-2017 ISSN 2229-5518.

[2] Mohamed Mahmoud, Member, IEEE, Khaled Rabieh, Ahmed Sherif, Enahoro Oriero, Muhammad Ismail, Erchin Serpedin, and Khalid Qaraqe, "Privacy-Preserving Fine-Grained Data Retrieval Schemes For Mobile Social Networks" https://www.researchgate.net/publication/317487422

[3] Yashar Najaflou, Behrouz Jedari, Feng Xia, Senior Member, IEEE, Laurence T. Yang, and Mohammad S. Obaidat, "Safety Challenges and Solutions in Mobile Social Networks" Article in IEEE Systems Journal · September 2015.

[4] Kan Yang, Qi Han, Hui Li, Kan Zheng, Senior Member, IEEE, Zhou Su, Member, IEEE, and Xuemin Shen, "An Efficient and Fine-Grained Big Data Access Control Scheme With Privacy-Preserving Policy" IEEE INTERNET OF THINGS JOURNAL, VOL. 4, NO. 2, APRIL 2017.

[5] Xiping Hu, Terry H. S. Chu, Victor C. M. Leung, Fellow, IEEE, Edith C.-H. Ngai, Member, IEEE, Philippe Kruchten, Senior Member, IEEE, and Henry C. B. Chan, "A Survey on Mobile Social Networks: Applications, Platforms, System Architectures, and Future Research Directions" IEEE COMMUNICATION SURVEYS & TUTORIALS, VOL. 17, NO. 3, THIRD QUARTER 2015.

[6] JIALE ZHANG , BING CHEN, YANCHAO ZHAO , XIANG CHENG , AND FENG HU, "Data Security and Privacy-Preserving in Edge Computing Paradigm: Survey and Open Issues" Received February 7, 2018, accepted March 20, 2018, date of publication March 28, 2018, date of current version April 23, 2018.

[7] Leucio Antonio Cutillo∗ Refik Molva∗ Thorsten Strufe † ∗Institut Eurécom Sophia Antip, TU Darmstadt Darmstadt Germany, "Safebook: a Privacy Preserving Online Social Network Leveraging on Real-Life Trust " funded by the EC FP7-ICT-2007-8.2 for Pervasive Adaptation.

[8] B.Sony, V.Mahitha, "A NOVEL STRATEGY IN PROFILE MATCHING PROTOCOLS TO ACHIEVE CONFIDENTIALITY IN SOCIAL NETWORK", International Journal of Advanced Scientific Technologies, Engineering and Management (IJASTEMS-ISSN:2454-356X) Volume.3,Special Issue.1, March.2017.

[9] danah m. boyd , "Facebook's privacy trainwreck," Convergence: The International Journal of Research into New Media Technologies, vol. 14(1), pp. 13 – 20, 2008.

[10] Z. Zhu and G. Cao, "Towards privacy-preserving and colluding-resistance in location proof updating system," IEEE Trans. Mobile Comput., vol. 12, no. 1, pp. 51–64, Jan. 2011.

[11] kathu lanaga, mahesh,syed akthar, syed abdulha novel privacy-preserving anonymous profile matching protocols in mobile social networks. international journal of advances in applied science and engineering(ijaeas) issn(p):2348- 1811;issn(e): 2348-182x vol-1,iss.-4,september 2014,168-176.

[12] Maddali dhanesh, prakash jordan jency.j. an approach towards exploitation of social communications in mobile systems. (ijitr) international journal of innovative technology and research volume no.2, issue no. 1, december – january 2014, 773 - 775.

[13] Yashar Najaflou, Behrouz Jedari, Feng Xia, Laurence T.Yang, and Mohammad S. Obaidat. Safety Challenges and Solutions in Mobile Social Networks.

[14] Enahoro Oriero. "PRIVACY-PRESERVING FINE-GRAINED DATA RETRIEVAL SCHEMES FOR MOBILE SOCIAL NETWORKS" Master of Science in Electrical and Computer Engineering.

[15] Mehdi Sookhak, F. Richard Yu, Muhammad Khurram Khan, Yang Xiang,

Rajkumar Buyya, “Attribute-based data access control in mobile cloud computing” September 2016.

[16] Jiangang Shu, Ximeng Liu, Xiaohua Jia, Kan Yang, and Robert H. Deng, “Anonymous Privacy-Preserving Task Matching in Crowdsourcing” Article · April 2018.

[17] Mehdi Sookhaka, F. Richard Yu, Muhammad Khurram Khan, Yang Xiang, Rajkumar Buyya, “Attribute-based data access control in mobile cloud computing: Taxonomy and open issues” Future Generation Computer Systems 72 (2017) 273–287.