JES Journal of Engineering Sciences

Vol 11, Issue 4 , April/2020
ISSN NO:0377-9254

SECURE PROFILE MATCHING AND PRIVACY-PRESERVING IN SOCIAL NETWORKS

Dr.P.C.SENTHIL MAHESH[1], K.AKHILA REDDY[2], P.HYMAVATHI[3], S.MASTAN[4], P.NARENDRA REDDY[5]

[1]Professor, Dept of CSE, AITS, Rajampet, AP, India.
[2,3,4,5]Student, Dept of CSE, AITS, Rajampet, AP, India.

Abstract—We consider a scenario where a user queries a user profile database, maintained by a social networking service provider, to identify users whose profiles match the profile specified by the querying user.A typical example of this application is the online dating.Most recently, one of the online dating website, Ashley Madison, was hacked, which results in the disclosure of a large number of dating user profiles. This data breach has urged the researchers to explore the practical privacy protection for user profiles in a social network.We propose a privacy-preserving solution for profile matching in social networks by using the multiple servers.Our solution is built on the basis of homomorphic encryption and allows a user to find out matching users with the help of multiple servers without revealing to anyone the query and the queried user profiles in clear. Our solution achieves user profile privacy and the user query privacy as long as at least one of the multiple servers is honest. Our experiments demonstrate that our solution is practical.

I. INTRODUCTION

Discovering and interacting with people within a certain distance according to personal preferences is a crucial service provided by mobile social networks (MSN), which is helping us to stay connected better than ever. Let us imagine the following the two scenarios. (1)At the airport, a passenger wants to discover and connect with the nearby passengers who come from the same university. (2) In the hospital, a patient wants to find similar patients according to their disease symptoms and medications for physical or mental support. In MSN, all such requirements can be satisfied by user profile matching very quickly and accurately. Generally speaking, user profile is a set of attributes generated by users to describe themselves for special friending purpose when they join social networks. For example, in the first scenario, the user profile of a the passenger may include his/her age, sex, university from which he/she graduated, company in which he/she is working and his/her destination, etc. In the second scenario, the user profile of a patient may include his/her disease symptoms, medications being taken and his/her doctor, etc. The meaning of "matching" can be defined from different perspectives. For instance, if we consider the user profile as an attribute set, two profiles are matched when the number of their common attributes exceeds a certain threshold. If we consider the user profile as an attribute vector, the exact meaning of the "matching" can be defined as that the distance of the two attribute vectors is less than the certain threshold. Nowadays, a lot of the exciting mobile applications based on user profile matching have been the generated.Small-talks connects proximate the users are based on the their common interests. Color allows the people in close proximity (within 50 meters) to share photos automatically based on their similarity. MagnetU can automatically match one with nearby users who have the similar profile. However, such systems also raise a number of privacy concerns. Obviously, directly exchanging the user profiles without any protection may open a door to various variety of attacks. Let us take the aforementioned two scenarios for example. In the first scenario, if an adversary can access the preference-profile submitted by the initiator, he/she may pretend to be the matched one, make contact with the initiator and implement further deception. In the second scenario, if the profiles of patients are directly exchanged with each other, it will facilitate user profiling where that sensitive and private information can be easily collected by a nearby user, either in an active or passive way.

Therefore, the demand for the privacy protection motivates the people to find the privacy-preserving profile matching schemes which make the friending in MSN more secure. The most direct solution is to take advantage of a trusted central server to collect information from individual users, compute and disseminate the matching results on demand. However, this solution may be unsuitable for MSN. First, it requires the user to access the mobile Internet. But, in practice the mobile Internet may not always be available, and it may incur a high expense. Secondly the central server may become bottleneck when a failure or attack occurs. For these reasons, the distributed solution in which the users are able to well protect their personal information without the help of a trusted central server is more suitable for MSN, especially for MSN based on short-range wireless technologies such as WiFi and Bluetooth. Several distributed solutions of privacy-preserving profile matching problem have been proposed in recent years. They

based on secure multi-party computation (SMC), and can be divided into two mainstreams. The first category treats user profile as attribute set and computes the similarity between two users based on the private set intersection (PSC) and private cardinality of set intersection (PSCI). The second category describes the user profile as an attribute vector and measures the similarity by secure dot-product computation. These methods rely on the public-key cryptosystem homomorphic encryption, which results in expensive computation cost. Multiple rounds of the interactions are required to perform the presetting and the profile matching between each pair of the users, which means the higher communication cost. In these methods, both matched users and unmatched users are required to take on nearly the same expensive computation and communication cost. Furthermore, most of these methods are unverifiable, which means the some malicious adversaries may forge their profiles or return the false calculation results to deceive the initiator. In this paper, we propose a novel privacy-preserving profile matching scheme which can overcome the above disadvantages. Our scheme is based ciphertext-policy attribute-based encryption (CP-ABE). Its basic idea is very simple. When an initiator wants to search for nearby users who meet his/her preference, he/she generates a ciphertext using CP-ABE at first. His/her preference-profile is taken as the ciphertext access policy and embedded into the ciphertext. This ciphertext is sent to nearby users. Only the matched user the whose profile includes the preference-profile that can decrypt the ciphertext correctly. Then he/she can choose to communicate with the initiator. Despite a simple solution, there are two main challenges that should be carefully addressed. First, there are a lot of CP-ABE constructions, but most of them cannot be applied to our scheme. The most important reason is that the ciphertext access policies in these constructions are accessible to anyone. However, in our application context, the ciphertext access policy (preference-profile) should be hidden for privacy-preserving. In addition, among most of the CP-ABE constructions, both the size of ciphertext and decryption time increase linearly with the number of the user attributes, which cannot satisfy the requirements in terms of the communication and computation efficiency in our application context. Therefore, considering the security and efficiency, we have to find out a CP-ABE construction that provides receiver anonymity through hidden access policy while ensuring the constant size of the ciphertext and constant decryption time. Facing this the challenge, in our work, a special CP-ABE construction with hidden access policy, constant length of ciphertext and constant decryption time is chosen as the foundation of our privacy-preserving profile matching scheme. It builds on the prime order group, and relies on asymmetric decision bilinear diffie-hellman (DBDH) assumption. It was shown to be the fully secure with the respect to the standard model. Second, in the CP-ABE constructions applied in our work, the size of access policy is required to be equal to the size of the user attributes. However, in our application context, the length of the preference-profile is not the necessarily equal to the length of profile of matching user. In fact, the meaning of "matching" in our scheme means "including". That is to say, the profile of the matched user must include all the attributes in the preference-profile. Therefore, we have to design a mechanism to enable the original CP-ABE construction to satisfy such a requirement. In order to overcome this barrier, we modify the original key generation algorithm, design a data structure named reminder vector, and design the corresponding algorithm to achieve fast matching.

Based on the query, multiple servers, which secretly share the decryption key, compare the preferred user profile with each record in the database. If the dissimilarity is less than the threshold, the matching user' contact information is returned to the querying user.

Our main contributions include

1) We formally define the user profile matching model, the user profile privacy and the user query privacy.

2) We give a solution for privacy-preserving user profile matching for a single dissimilarity threshold and then extend it for multiple dissimilarity thresholds.

3) We perform security analysis on our protocols. If at least one of multiple servers is honest, our protocols achieve user profile privacy and user query privacy.

4) We conduct extensive experiments on a real dataset to evaluate the performance of our proposed protocols under different parameter settings.

II. EXISTING SYSTEM

Existing online matching services require participants to trust a third party server with their preferences. The matching server has thus full knowledge of the users' preferences, which raises privacy issues, as the server may leak (either intentionally, or accidentally) users' profiles. When signing up for an online matching service, a user creates a "profile" that others can browse.

Disadvantages:

- The efficiency is low
- low performance

III. PROPOSED SYSTEM

We proposed a new solution for the privacy-preserving user profile matching with the homomorphic encryption technique and multiple servers. Our solution allows a user to find out the matching users with the help of multiple servers without revealing the details of query and the user profiles. Security analyses have shown that the new protocol achieves user profile privacy and user query privacy.

Advantages:

- The security parameter.
- The performance is high.

System Architecture:

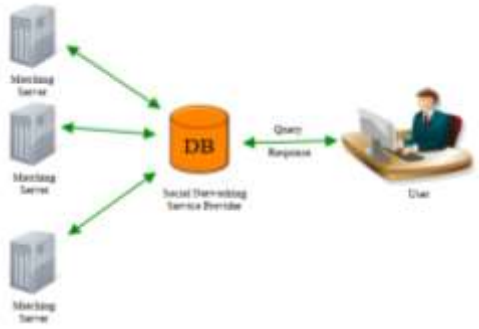


Fig.1: Model for Privacy-Preserving User Profile Matching

Modules:

The modules are as follows:

Admin
User

Admin:

Admin login with valid credentials. Admin can view user's details, and upload (decrypt) users list into our local server.

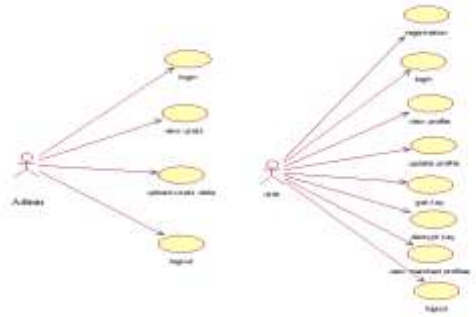
1. Login (Admin login with valid username, and password)
2. View Users (Admin can view the all users list)
3. Upload users list (Here users list could be stored in a text file, the users list file can be view and upload and encrypts the file and store into database)

User:

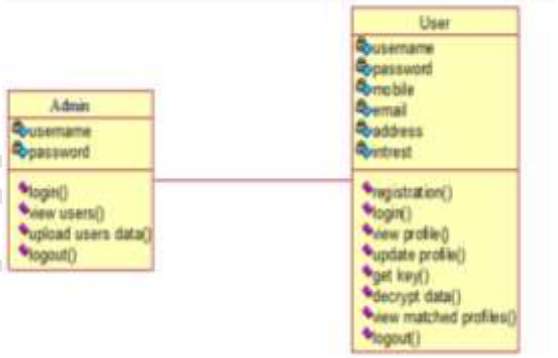
User can initially register with their details. Then login with registered email id and password. User's view their profile details and update profile details. He / She find to view matched profiles.

1. Registration (Users initially register with their details)
2. Login (Login with registered email and password)
3. Profile (user view their registered details in profile module)
4. Update (the user can updates their profile, then the user details could be changed in database and also users list file)
5. Check Profile matchings' (user check matched profile wants to a keyword, then use gets a keyword, and after entering the keyword user can decrypt uploaded user list and the use can view matched profiles list only).

Use case diagram:

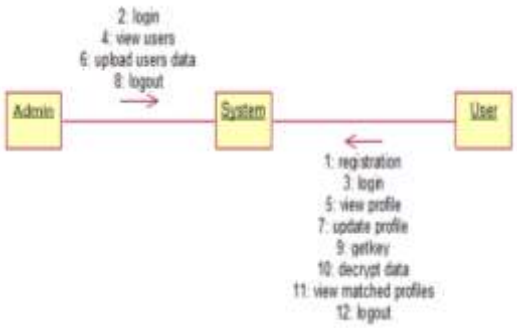


Class diagram:

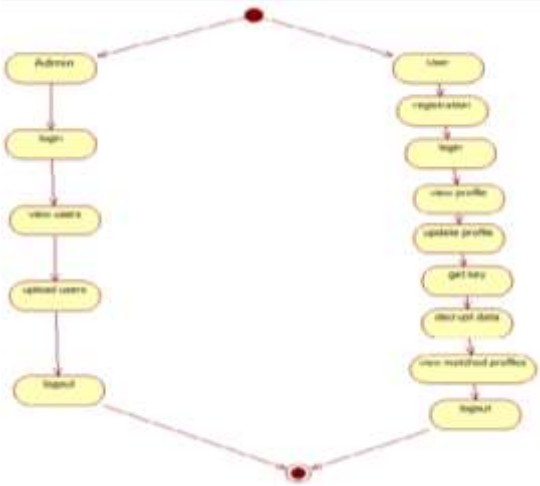


Sequence diagram:

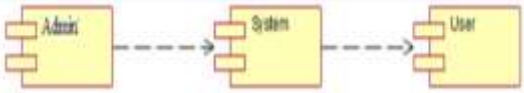
Collaboration diagram:



Activity diagram:



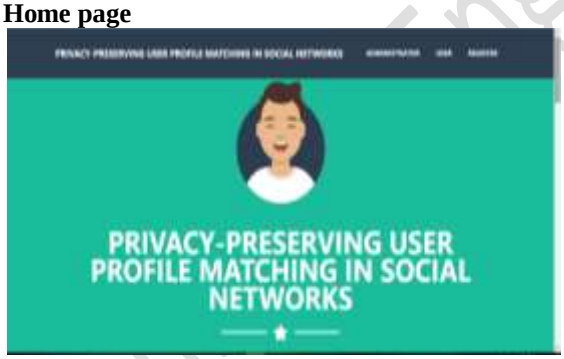
Component diagram:



Deployment diagram:

IV. OUTPUTS

Home page



Admin login page

Admin homepage

Users_list page

Upload file1

Upload file2

Registration page

Users_login page

Users_home page

User Profile Details

Update profile details

Get key page

Decrypt file page

Matched profile details

CONCLUSION

We proposed a new solution for privacy-preserving user profile matching with homomorphic encryption technique and multiple servers. Our solution allows a user to find out the matching users with the help of multiple servers without revealing the query and the user profiles. Security analyses have shown that the new protocol achieves user profile privacy and user query privacy.

REFERENCES

[1] R. Agrawal, A. Evfimievski, and R. Srikant, Information sharing across private databases, in SIGMOD 2003, pp. 86-97.

[2] M. von Arb, M. Bader, M. Kuhn, and R. Wattenhofer, Veneta: Serverless friend-of-friend detection in mobile social networking, in IEEE WIMOB 2008, pp. 184-189.

[3] B. H.Bloom, Space/time trade-offs in hash coding with allowable errors, Communications of the ACM 13 (7): 422-426, 1970.

[4] D. Boneh,E.J.Goh, K. Nissim, Evaluating 2-DNF formulas on ciphertexts, in TCC 2006, pp 325-341.

[5] D.Chaum,Blind signatures for untraceable payments, in Crypto 1982, pp. 199-203.

[6] E.D.Cristofaro and G.Tsudik, Practical private set intersection protocols with the linear complexity, in the Financial

Cryptography and the Data Security 2010.

[7] D.Dachman-Soled, T. Malkin, M. Raykova, and M. Yung, Efficient robust private set intersection, in ACNS 2009, pp. 125-142. T. ElGamal, A public-key cryptosystem and a signature scheme based on discrete logarithms, IEEE Transactions on Information Theory 31 (4): 469-472, 1985

[8] M.Freedman, K.Nissim, and B.Pinkas, Efficient private matching and set intersection, in EUROCRYPT 2004, pp. 1-19.

[9] C. Gentry, Fully homomorphic encryption using ideal lattices, in STOC 2009, pp 169-178.

[10] S. Goldwasser and S. Micali, Probabilistic encryption and how to play mental poker keeping secret all partial information, in Proc. 14th Symposium on Theory of Computing, 1982, pp. 365-377.

[11] D. Harris, D. M. Harris and S. L. Harris, Digital Design and Computer Architecture, Morgan Kaufmann Publishers, 2007.

[12] C. Hazay and Y. Lindell, Efficient protocols for set intersection and pattern matching with security against malicious and covert adversaries, in TCC 2008, pp. 155-175.

[13] C. Hazay, G.L.Mikkelsen, T. Rabin, T. Toft, A.A.Nicolosi,Efficient RSA key generation and threshold paillier in the two-party setting, in CT-RSA 2012, pp. 313-331.

[14] Y. Huang, L.Malka, D. Evans and J. Katz, Efficient privacy-preserving biometric identification, in NDSS 2011.

[15] S.Jarecki and X. Liu, Efficient oblivious pseudorandom function with applications to adaptive OT and secure computation of set intersection, in TCC'09, 2009, pp. 577-594.