Profile matching by realising privacy levels via Secure multi-party computation

P.M.BALAGANESH, M.E., (P.HD) DEAN, CSE Sembodai Rukmani Varatharajan Engineering College, Sembodai.

N.VICTORIA, (ME) Asst prof, Sembodai Rukmani Varatharajan Engineering College, Sembodai.

P.KATHAMBARI, (ME) CSE, Sembodai Rukmani Varatharajan Engineering College, Sembodai.

Abstract

Matching their profiles using their physical proximity via mobile social networking is a critical thing. In certain applications the user's complete profile has not to be made public. However in existing services the user publishes their complete profiles as a key for others to search. We propose FindU, the concept used to limit the privacy levels and also to find the best matching profiles. To realize the user privacy levels here we are using secure multi-party computation (SMC) techniques. We also propose protocols such as PSI, PCSI to prove their security proofs. We evaluate the efficiency of the protocols by adopting the total run time and energy consumption.

Index terms

Shamir secret sharing algorithm, Secure multi-party computation, Private Set Intersection and Private cardinality set intersection protocol, FindU enhancements, set inflation attack, Honest but curious model, Blind and permute model.

Introduction

An important thing is to make new connections by realizing their privacy levels within their proximity to match their profiles. For example, let we take one user using yahoo messenger and the other Skype for their conversation. In certain applications, the user makes a conversation with other by matching their id. The scope of these chances made very effective but also it commit some errors.

The fact is to allow the initiator and the responder to match their profiles by knowing the related attributes whereas others couldn't know anything about their profiles. There exists lagging in the authorization in which the attributes can't be identified by the rest of the users. It also interferes with the system usability.

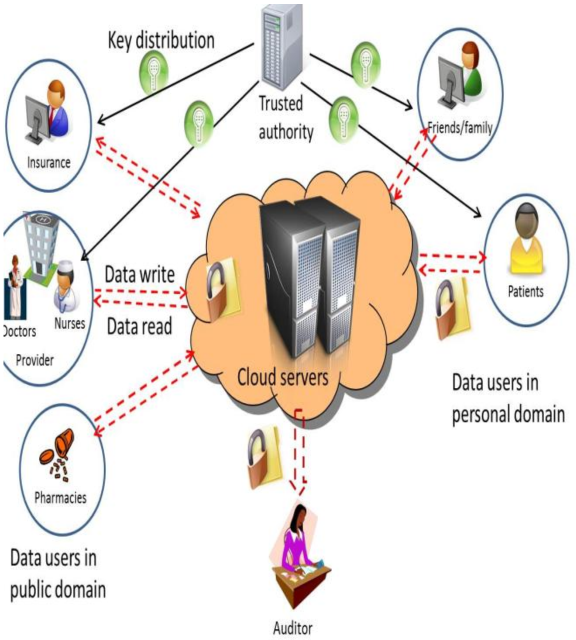

Fig 1: The above figure explains about the architecture. Here the profiling takes place by using the cryptographic concepts. This also explains about user best matches and key enhancements.

The following contributions have to be formulated as,

- Two levels of privacy such as higher and lower which deals with the profile information.
- Two fully distributed privacy preserving protocols.

  (i.e.) Private Set Intersection protocol (PSI)

Private Cardinality Set Intersection protocol (PCSI)

To improve the computation and communication services we are proposing several key enhancements based on secret sharing techniques.

To prevent the malicious attacks, we provide security proofs under Honest-but-Curious (HBC) model.

Data Flow diagram

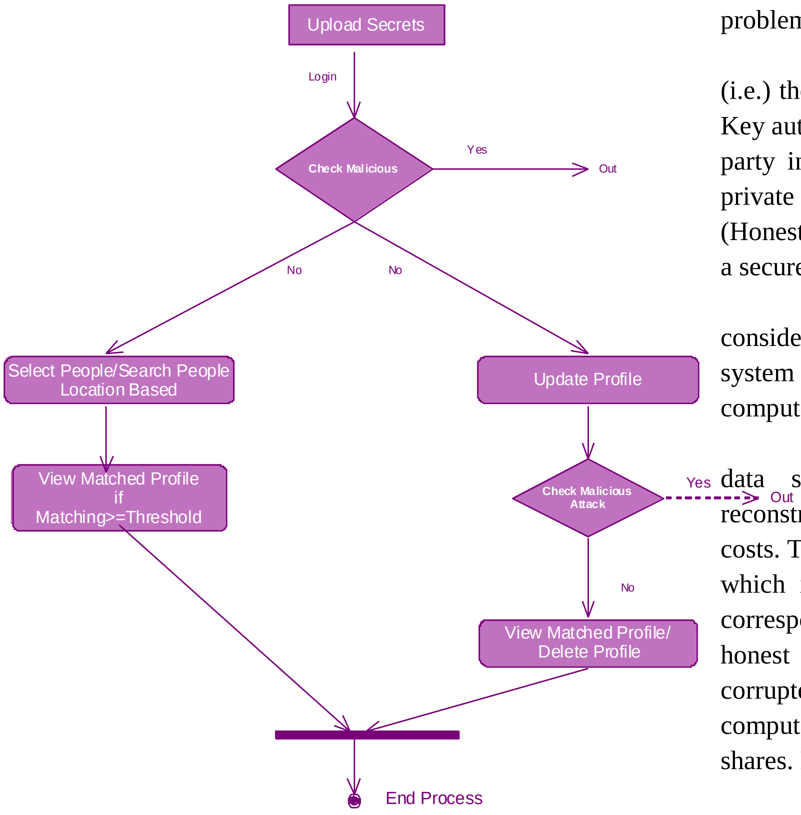
Upload Secrets
Login
Check Malicious
Yes
Out
No
No
Select People/Search People Location Based
Update Profile
View Matched Profile if Matching>=Threshold
Check Malicious Attack
Yes
Out
No
View Matched Profile/ Delete Profile
End Process

Fig: 2 The above figure explains how the profile matching takes place between the users by realizing their privacy levels. If any malicious attacks exist means no matching takes place otherwise their exists matching

Proposed system

We propose a system that consists of a set of initiators and the responders containing several set of attributes whereas our goal is to find the best matching party. There exists matching if they possess the same set of attributes. We also formulate here the intersection between the two sets of attributes which proves their similarity. Based on this similarity the best matches can be made using our protocols.

We also establish a communication channel between the users for their security purpose. In this the user can only participate at the end of the protocol run. We are designing the system as a lightweight and practical one which enables different users to personalize their privacy levels. We have achieved our goals by providing multiple instances of PSI and PCSI respectively. Using SMC techniques we tackle many problems.

We have also prove the concept of user profiling (i.e.) the best matches profile between each pair of users. Key authentication has to be enhanced to prevent the third party interruption. We mainly focused to minimize the private information in one way. By using the HBC (Honest-but-curious) model, the profiling can be done in a secured manner via their protocols.

Our paper is made to be very effective by considering the human needs for their matches. Our system is also easy to handle by comparing the previous computations.

The basic scheme consist of three phases such as data share distribution phase, computation phase, reconstruction phase which increases the communication costs. To generate the shares we are using the simulator in which it provides the local inputs and outputs of the corresponding parties. First the simulator generates the honest parties input to match with the local outputs of corrupted parties. Then the real protocol run of the computation phase can be takes place by using the input shares. By

Using the induction method, we show that the execution takes place in a distributed manner. The partial view output and also the full view can be displayed in the output reconstruction phase.

The schemes uses the Blind and permute (BP) method in which it initiates the encryption techniques between each pair of users and then generates a random number by sharing their items. By using pseudo-random number the receiver permutes the share and then transfers to sender, finally it results in an expensive computation.

We permute one invocation between the parties by using their random number. It results in a very effective computation by using the BP protocol. Our privacy levels should be personalized by conveying the information initially. Practically our FindU concept can be used with mobile devices for short range of communication (ex: - Bluetooth, WiFi). Here we are using the Diffe-Hellman Key Exchange (DHKE) to reduce the complexity. We also used Tamper-evident pairing (TEP) in which it helps to prevent the malicious attacks. The communication cost and the time complexity is O (N). TEP requires the user to alert once and it is also fully distributed.

We are also uses Shamir secret sharing schemes which are multi party protocols related to key establishment. The original motivation for secret sharing was the following. To safeguard cryptographic keys from loss, it is desirable to create backup copies.

The greater the number of copies made, the greater the risk of security exposure, the smaller the number, the greater the risk that are lost. Secret sharing scheme address this issue by allowing enhanced reliability without increased risk.

Our existing system has the following disadvantages

- Opens up the possibility for hackers to commit fraud and launch spam and virus attacks.
- Increases the risk of people falling prey to online scams that seem genuine, resulting in data or identity theft.
- May result in negative comments from employees about the company or potential legal consequences if employees use these sites to view objectionable, illicit or offensive material.
- Potentially results in lost productivity, especially if employees are busy updating profiles

Our proposed system has overcome these disadvantages with low computation cost and also with good communication

Related works

We achieve the good computation and communication by using the SMC techniques via PSI and PCSI protocols. Basically it depends upon the concept of cryptography. We propose a secure friend discovery (i.e.) the computation differed from the previous one.

We also prove here the centralized authority between the coordinates without finding their intersection sets. To prevent the manipulation between the contact lists, we introduce a private contact discovery protocol.

The time consumption is getting higher when the users also provided with poor signals. Without depending on their client-server relationship, we propose a fully distributed privacy preserving profile matching protocols. We also provide several methods to minimize the cost of computation and the energy consumption level.

We are achieving high performance by using the protocols and also by neglecting the homomorphic properties of secret sharing algorithm. Our paper has a power to face the practical problems for ex, a salesman with their report submission for their marketing purpose.

Conclusion

In this paper, we propose two protocols to realize the user’s privacy levels and also for profiling with best matches by preserving their private information. To lower the communication costs and to improve the computation we follow the Shamir secret sharing concepts by exploiting the homomorphic properties. As a result of our study, we prove the concepts to prevent the malicious attack by using the HBC model. Our schemes are to be more effective in MSN’S without any central server while they are possessing a less query attributes.

Acknowledgment

I would like to thank Mr.Balaganesh (Dean) and Ms.Victoria (guide) for encouraging me to present this paper in an effective manner with good schemes and suggestions.

References

1. M. Li, N. Cao, S. Yu and W. Lou, ”Findu: Privacy-preserving personal profile matching in mobile social networks”, in IEEE INFOCOM’11,Apr 2011,pp.1-9.
2. Q. Ye, H. Wang, and J. Piperzyk,” Distributed private matching and set operations,” in ISPEC’08, 2008, pp. 347-360.
3. A. Shamir,” How to share a secret,” Commun. ACM, vol. 22, no. 11, pp. 612-613, 1979.
4. L.Kissener and D.Song, “Privacy-preserving set operations,” in CRYPTO ’05, LNCS. Springer, 2005, pp. 241-257.
5. A.C. Yao,” Protocols for secure computations,” in SFCS ’82, 1982, pp. 160-164.