Privacy Preserving Profile Searching Problems and its Management in Social Networks - A study

Preetha Mathew K[1] , Dr. Mathew Cherian [2], Shibu V[3]
[1]Associate Professor,
[2]Associate Professor &Principal,
[3]Lecturer
Cochin University College of Engineering KuttanadPulincunnu, Alappuzha Kerala, India

Abstract

The unprecedented growth in the popularity of social network system has to deal the privacy of individual participating in them. People are unwilling to disclose their personal profile to arbitrary persons without deciding to interact with them. Therefore to protect the privacy of the participants seems to be a task that needs to be addressed.This paper deals withthe techniques for privacy preserving profile management in the social networks.The protocols discussed in this paper are provably secure, in which the security is reduced to a known hard problem like discrete logarithm problem or its variants.

1. Introduction

According to Danah M Boyd and Nicole B Ellison[1] social network sites are web based services that allow individuals to

1. Construct a public or semipublic profile within a bounded system

2. Articulate a list of other users to whom they share a connection (friend list)

3. View and traverse their list of connection and made by others within the system (social graphs).

The two basic functions of the social networks are communication and making friends. When people join in the social network the first step is to create their profile and then start interact with others. The content of the profile consists of personal back ground, the place of stay, hobbies etc. To find friends with common interests or experience or to find lost connection people normally use profile matching technique.Disclosing information on the web is a voluntary activity on the part of users. But users are unaware of the fact that who is able to access the data and how the data is used by others without the owner's permission. Hence user's profile is vulnerable to unauthorized intrusion. Data privacy is defined as freedom from unauthorized intrusion[3]. Therefore privacy disclosures often occur in the social networks. Learning the private information of the individual from publicly available data or finding dependencies from the perturbed information is possible in the social networks. Preserving the privacy and searching the profile becomes a problem of the social networks. Privacy preserving profile searching (PPPS) is one of the key problems in social networks. The Privacy Preserving Profile Searching (PPPS) problem can be defined as follows[4]. Suppose there are two persons say P1 and P2, P1want to access the profile of P3, who is a friend in the friend list of P2. Friends in the friend list of P2 are hidden from P1(Hidden Access Control,HAC[5]. If P2 is having the requested friend's P3 profile and P2 is ready to transfer the information, P1 can get only the profile of P3 from P2. In this case the sender P2 should remain oblivious to which profile has been transferred to P1(Oblivious Transfer,OT)[6,10]. Therefore PPPS is closely related to the concept oblivious transfer with hidden access control(OT-HAC)[9]. One can rephrase PPPS problem as searching among encrypted data. Public key searchable encryption isa scheme which allows data owner to delegate a searching trap door to an untrusted server for searching among cipher texts, without delegating the power of encryption. Public Key encryption with keyword search(PEKS) can be built by using identity based encryption with anonymity[27].

2. Related Work

In asymmetric encryption scheme, users have both public key and private key constructed with the help of a certification authority called Public Key Infrastructure(PKI). The user’s public key should be certified by a certification authority. Therefore key management was the problem associated with this.

Identity based encryption(IBE)was coined by Shamir[16].The public key in the identity based encryption system will be a known string, hence key management problem will not be there. But the secret key is generated by a trusted third party called Key Generation Center (KGC). The problem associated with this is if KGC is malicious, secret key of the user can be used illegally. This problem is called key escrow problem. The IBE is implemented by Boneh and Franklin[11].Accountable IBE is proposed by [19,20] when the KGC maliciously generates and distributes or uses a decryption key for an identity, it may be caught using a trace algorithm. Should two keys for one identity be generated by the KGC, this algorithm can identify which key was generated for the individual that requested it, and which was generated for potentially malicious use by the KGC. IBE is said to be recipient anonymous[21,22] if no information about the recipient can be obtained by viewing the cipher text.

Symmetric encryption based privacy profile matching and secure communication channel establishment mechanism in decentralized social networks without any presetting or trusted third part is proposed by Zhang and Li[28].

The profile searching in the Facebook type social network and access are done either using global name search or by social graph traversal[18].

2.1 Global name search

This is the first method of searching the profile.A successful search would produce for the accessing user the search listing of the target user. A user may specify the search policy to allow only a subset of users to be able to reach her search listing through a global name search.

2.2 Social Graph Traversal

Another means to reach a search listing is by traversing the socialgraph. Facebook allows users to articulate their relation with one another through the construction of friend lists. Each user may list a set of other users as friends.This can be viewed as a graph in whichusers are nodes and relationship as edges. A user can traverse this graph by examining the friend lists of other users.Face book allows user to restrict traversal by specifying the traversal policy which specify the set of users who are allowed to examine her friend list.

Once the search listing of a profile owner is reached then accessing the profile starts.Here the user should not allow every user to access his/her profile. Therefore the owner may assign access policy.

2.3 Private Similarity Discovery

Common interests, common friends or common profile are considered as similarities. These similarities are known to both sender and receiver before they run private similarity discovery protocol. The privacy requirement of these protocols guarantees no extra information but the similarities is revealed to the participants. Commonly adopted technique is private set intersection[23]. A PSI scheme is a two party protocol between a client (initiator) with an input set and a server with another input set. At the end of the protocol the initiator learnsthe intersection of both the inputs. Two common friend discovery protocols based on private similarity intersection have been proposed by [25,27].

3. Motivation

Face book like social network offers a set of predefined policies for users so that a certain profile item is accessible only by friends or available to friends of friends. Investigation is made to find the methods that can be used in the scenario mentioned above. The mechanisms found in the literature are searchable encryption, oblivious transfer with hidden access control and anonymous identity based encryption with blind key extraction and so on. This paper enumerates the mechanisms that can be used to access the profile mentioned in the above scenario. The paper also explains how each mechanism can be used for the profile searching preserving the privacy of the users. The protocols are proven to be secure by reducing it to hard problems like discrete logarithm problem or its variants.

4. The solutions for solving PPPS in social networks

The solutions for privacy preserving profile searching can be enlisted as Searchable encryption, Oblivious transfer with hidden access control,and Anonymous blind identity based encryption

4.1 Searchable Encryption

Searchable encryption schemes provide an important mechanism to privately search keywords on encrypted data in a public key setting and decryptthe search results.The two primitives used for this are public key encryption with oblivious keyword search (PEOKS) and committed blind anonymous identity based encryption[7].PEOKS is an extension of public key encryption with key word search in which users canobtain trapdoors from the secret keyholder without revealing the keywords. Committed blind trapdoor extraction, which facilitates the definition of authorization policies to describe which trapdoor aparticular user can request. To have an oblivious search mechanism in a database,hiding the keywords from the security server and hiding the search results from the database. The above two primitives are presented in Camenisch et al.[7]. In the context of committed blind anonymous IBE anonymous meansthat the cipher text does not leak the key(identity) under which it was encrypted and blind means that a user can request the decryption key for a given identity without key generation entity learning identity. A public key encryption with oblivious keyword search is implemented using the committed blind anonymous IBE.Blind key extraction with committed keywords, which facilitates the use of a policy that states for which key words a trapdoor can be extracted while still keeping them hidden from the trapdoor generation entity. While comparing the PPPS problem P2 will be searching profile of P1 which is encrypted, sothat P2 will be learning only one data and P1 doesnot know what data P2 is accessing.

4.2 Oblivious Transfer with Hidden Access Control (OT HAC)

An oblivious transfer protocol(OT) enables receiver to obtain one of many pieces ofinformation from senderand sender cannot know which information the receiver receives. The basic OT considers all items are of same kind, such that the receiver specifies the interested item by a choice(index). The sender does not the choice of the receiver and the receiver should not know the other information other than his choice. OT HAC was proposed by Camenisch et al[9]. The said protocol allowsuser to access the database(server with user profile in social network) such that the database does not learn who queries the record, the database does not learn which record is queried and its access policy, the database does not learn whether the attempt to access the record is successful or not, the user can access only single record per query, the user can access the record only it he/she has right permission, the user does not learn any other information about the structure of the database and the access control policies other thanwhether he was granted access to queried record and if so the content of the record and the credential of the user can be revoked. Therefore OTHAC is run between issuer, database and one or more users. The issuer provides access credentials to users for the data categories that they are entitled to access. The database hosts a list of records and associates to eachrecord an access control policy. Users can request individual record from the database, and their request will succeed provide they have the necessary credentials. The access control policies are never revealed.

The working of OTHAC is as follows. The issuer generates the key pair for issuing the credentials and publishes the public key as system parameter. The database server initializes a database containing record protected by access control policies. It generates encrypted database, which also containsthe encrypted access control policies and makes it available to users. Each user contacts the issuer to obtain a credential that lists all data categories that user is entitled to access. When user wants to access the record, the user proves to database in zero knowledge that her credential contains all the data categoriesrequired by the access control policy associated to the record. The user performs computation on encrypted access control rule associated with the desired record so that with the help of database the record key if and only if the user satisfies the encrypted access control policy. The database never learnswhich record with which access control policy. Also it will not learn whether users attempt is successful. Comparing the working of OTHAC, in Facebook like social networks, where the user can provide access control searching the profile by preserving the privacy is as follows.P2and P1 can act as sender and receiver. The items being transferred is the friend list of P2 and the access control attribute describing the friend list is hidden from P1. P1 who is searching for certain type of profile contacts P2 and check whetherP2 hasprofile P1 searching forprovided both are willing to reveal minimum information(zero knowledge). (A zero knowledge proof is a method in cryptography in which one party (PROVER) can prove to another party(VERIFIER) that a given statement is true, without conveying any additional information apart from the fact that the statement is indeed true. To prove the statement some secret information is required from the part of thePROVER and the VERIFIER will not be able to prove the statement to anyone else.)P2 will be sending theprofile to P1 only if the access control rights are satisfied. Also P2 does not want to reveal any other information from his friend list

4.3 Blind Identity based Encryption

Another way to construct OT is to use blind identity based encryption which was introduced by Green and Hohenberger[15]. It is constructed using an IBE with a blind key extraction(BKE) protocol.BKE of IBE guarantee that a user can obtain decryption keyfor an identity without letting the key issuer learning the identity.It helpsthe receiver to get only one decryption key of the IBE systemwhich fulfills the security of the sender.The receiver'schoice is protected since the identity being requested is not leaked via blinding. OTHAC can be constructed as an extension of Blind identity based encryption by making it anonymous. If anonymity property is not satisfied access control policy of the encrypted item cannot be hidden. Therefore a blind anonymous encryption can be used for the construction of OTHAC.

Let P1 be the initiating party who will send the request of profile to P2 and starts the process.The information that P1contain is a specification of his target profile. The user P2 has a private friend list L[9]. P1's goals to get introduced to those of P2's private friend list who match his requirement at the end of the protocol.

Eachfriend in list L willbeassigned with a random index by P2 at the beginning of the protocol. Each index will be encrypted under an attribute (or set of attributes) using anonymous IBE(hierarchical).The cipher text will be published by P2.

The blind key extraction of the anonymous IBE is having a major role in this protocol. P2 will usehis master key of IBE. After an invocation of the protocol P1 will receive independently generated private key corresponding to the attribute he is interested while P2 gets nothing.

P1 then uses the private keyhe receives to decrypt all the ciphertexts given by P2 and returns the decryption results to P2.Since all the information P1 receives during the decryption are randomindexes (the decryption issuccessful if a matchbetween the specification of private key and the attribute set labeled with the cipher text) or a random element if decryption is not successful.In both the cases P1 will be getting a random result but does not obtain any information from the list. After receiving the decryption result, P2 candecide whether he will introduce P1to the matching private friends.Suppose none of P2's friends meet P1'srequirement then P2 gets only *m* independent decryption results due to unique randomness in eachof P1's m private keys.P1 will get a chance to know the correct person if and onlyif P2 decides.An anonymous blind IBE is proposed by Lin et al. using anonymous IBE proposed by Ducas[13] and use a zero knowledge protocol for blind key extraction. Another anonymous blind IBE proposedby Sangeetha et al.[17] , using the anonymous IBE proposed by

Boneh and Franklin[11] and the blind key extraction is done with the help of BLS signature[12]. The second scheme seems to be efficient as it uses a short signature and the communication overhead of the zero knowledge proof is also not present.

5. Conclusion

In this paper we present various solutions to privacy preserving profile searching problem in the social networks like Facebook using asymmetric encryption schemes.These techniques can be used in anonymously reading the databases without security breach and also able to control the access. The same technique can be applied for security of cloud also. The security of the protocols is based on the provable secure approach.A blind attribute based encryption and OT with fine grained access control is proposed by Alfredo Rial and Bart Praneel which allows the enforcement of large class of access controlSymmetric encryption based privacy profile matching and secure communication channel establishment mechanism in decentralized social networks without any presetting or trusted third part is proposed by Zhang and Li[28].

policies and has an improvement in the communication complexity .

References

[1] Danah M Boyd and Nicole B Ellison ,"Social Network sites: Definition, History, and Scholarship",Journal of computer mediated communication Oct 2008 pages 210-230.

[2] Elena Zheleva and LiseGetoor"Privacy in social networks: A survey", Social network data analytics C CAggrawaled.

[3] Y. Z. J. Vaidya, C.Clifton"Privacy Preserving Data Mining" Springer 2006

[4] Lin, H., Chow, S. S., Xing, D., Fang, Y., & Cao, Z. "Privacy Preserving Friend Search over Online Social Networks". *IACR Cryptology ePrint Archieve2011:445.*

[5] Frikken, K., Atallah, M., & Li, J. "Hidden Access Control Policies With Hidden Credentials". *WPES '04.*

[6] Kilian, J. "Founding Cryptography on Oblivious Transfer"*STOC 88*, (pp. 20-31).

[7] Camenisch, J., Kohlweiss, M., Rial, A., & Sheedy, C. "Blind and Anonymous Identity-Based Encryption and Authorised Private Searches on Public Key Encrypted Data."*Public Key Cryptography'09* (pp. 196-214). Lecture Notes in Computer Science, Springer.

[8] Crepeau, C. "Equivalence Between Two Flavours of Oblivious Transfers". *Advances in Cryptology* (pp. 350-354). Proceedings of Crypto '87, volume 293 of Lecture Notes in Computer Science, Springer-Verlag.

[9] Camenisch, J., Dubovitskaya, M., Neven, G., & Zaverucha, G. M. "Oblivious Transfer with Hidden Access Control Policies". *Public Key Cryptography*, (pp. 192 - 209).

[10] Rabin, M. O. "How To Exchange Secrets with Oblivious Transfer". Cryptology ePrint Archive 2005: 187.

[11] Boneh, D., & Franklin, M. "Identity-Based Encryption from the Weil Pairing". *CRYPTO'01* (pp. 213-229). Lecture Notes in Computer Science, Springer.

[12] Boneh, D., Lynn, B., & Shacham, H. "Short Signatures from the Weil Pairing". *ASIACRYPT* (pp. 514-532). Lecture Notes in Computer Science, Springer.

[13] Ducas, L. "Anonymity from Asymmetry:New Constructions for Anonymous HIBE". *CT-RSA 2010* (pp. 148-164). Lecture Notes in Computer Science, Springer.

[14] Galindo, D. "Boneh-Franklin Identity Based Encryption Revisited". *ICALP* (pp. 791-802). Lecture Notes in Computer Science, Springer.

[15] Green, M., & Hohenberger, S. (Blind Identity-Based Encryption and Simulatable Oblivious Transfer. *ASIACRYPT'07* (pp. 265-282). Lecture Notes in Computer Science, Springer.

[16] Shamir, A. (1984). Identity-Based Cryptosystems and Signature Schemes. *CRYPTO'84* (pp. 47-53). Volume 196 of Lecture Notes in Computer Science.

[17] Sangeetha Jose, Preetha Mathew K., C. PanduRanganA Privacy Preserving Profile Searching Protocol in Cloud Networks, ICCSM 2013

[18] Philip W. L. Fong and Mohd Anwar, Zhen Zhao "A privacy preservation Model for Facebook-Style Social Network Systems"

[19] V. Goyal. "Reducing Trust in the PKG in Identity Based Cryptosystem". LNCS 4622:430-2007

[20] V. Goyal, B Sahai and B. Waters Blackbox accountable authority identity based encryption. 15th ACM conference on computer and communication security page 427-437.2008.

[21] M.Abdalla, M.Bellare, D.Catalano, E. Kiltz T. Kohno, T. Lange, J-Malone-Lee, G.Neven, P. Paillier and H.Shi, "Searchable Encryption revisited: Consistency properties, relation to anonymous ibe and extensions". J Cryptology, 21(3):350-391,2008.

[22] C Gentry-Practical Identity based encryption without random oracles EUROCRYPT 2006 pages 445-464

[23] M.J Freedman and A. Nicolosi.” Efficient private techniques for verifying social proximity. In NSDI, 2006.

[24] E.D. Cristofaro, J. Kim, and G. Tsudik. Linear-complexity private set intersection protocols secure in malicious model. In ASIACRYPT, pages 213-231, 2010.

[25] E.D Cristofaro, M.Manulis and B. Poettering, “Private discovery of common social contacts”. In ACNS, pages 147-165,2011

[26] M.J. Freedman, K. Nissim and B. Pinkas. “Efficient private matching and set intersection”. In EUROCRYPT, pages 1-9, 2004

[27] Boneh D, Di Crescenzo, Ostrovsky R, PrsianoG,” Public Key Encryption with key word search”, Eurocrypt 2004.

[28] Zhang L ,Li X “ Message in a sealed bottle: Privacy Preserving Friending in Social Networks” arXiv 1207.7199 Jul 2012