Two Tales of Privacy in Online Social Networking

Rajendra Mane College of Engineering and Technology.

Punam P. Sawant, Ankita T. Bobhate, Sneha M. Jadhav, Mangesh K. Gosavi

Abstract— Privacy being the main issue in social networking site. We all are users of such social networking sites. Facebook, Twitter, LinkedIn, E-mail, and Blogging such site's popularity is increasing day by day. Though, to protect the personal data of each user, these sites have their own privacy policies now it is necessity to have user level privacy policy. In this paper, we are trying to specify the problem regarding privacy and how privacy can also be achieved at user level.

Index Terms— SNS, Surveillance privacy, Social privacy, Institutional privacy, RSA, Diffie Hellman, Data Sharing Center

1 INTRODUCTION

The whole world is now become single community due to evolution of network and its different communicating fragments. Social Networking Sites (SNS) are like interface for such communicators. Social Networking Sites playing the role of virtual community that communicates world spreaded, like minded, friends, groups, business people. Due to its changing, improving, latest features like multimedia messages, gaming, and quizzes people are always connected and prefers to use these sites. It is an enormous network that made world more closely. Twitter, LinkedIn are used by professional users and followers like us are following them. Facebook, e-mail are more popular as they used casually.

Ultimately, along with its benefits it also has problem regarding privacy. People are giving their personal details like photos, birthdate, comments, job, group membership, friends list, etc. If anyone is not aware about the privacy, then any unknown person can access your different personal information. Though, the site that you are using to communicate provides the privacy policies, sometimes it is also not sufficient to fully protect your account from stranger and your confidentiality may lost.

It is a little option that we are specifying here to secure your account on being SNS, and maintaining confidentiality. In this paper, we are first giving existing privacy types, their details, how privacy issued while communicating and eventually how we can resolve it.

2 Related Work:

As we are discussing there are three types of privacy problems: **Surveillance, Social, and Institutional.**

Surveillance:

This privacy problem arises when personal information and the social interaction of user is leveraged by government or the service providers.

Social:

This is regarding renegotiation or changing scope of boundaries as it social interaction gets mediated due to service providers.

Institutional:

This privacy problem is caused when user itself loses control over his/ her account.

These privacy problems are under the control of server or server is responsible for whatever activities done through it. Server is not a human but sometimes we cannot ignore possibilities of information leakage by machine itself because it programmed by human. Hackers can create such program that may leak user's personal data. And finally user may face these above problems.

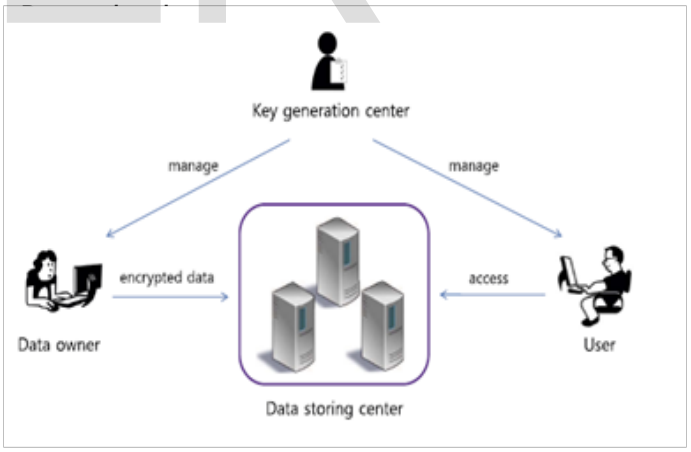

Fig. Architecture of Data Sharing Center

Architecture of Data Sharing Center:

In Distributed data sharing system such as Cloud Computing, Online Social Networking security has been more challenging issue. The above figure shows the different elements in these systems and how actually flows of communication done.

It consists of,

1. Data Storing Center
2. Data Owner
3. User
4. Key Generation Center

1. Data storing Center
It provides data storing services along with generates keys. It also controls the access form outside users by storing their data and providing respective services based on their requests. It is actually controller that controls it other communicating elements.

2. Data Owner
It is client who is responsible for defining his own attributes and communicating to those who, he wishing to share. Data owner has its choices or categories like friends, Family, Colleagues and data owner can categorize the data based on these choices.

3. User
User is one who wants to access the owner's data. User can access the data shared by data owner only when he satisfies the attributes specified by data owner.

4. Key Generation Center
This entity in 'Data Sharing Architecture' generates public and private keys parameters. It issues, updates keys for users.

To make the user account more secure, here we are trying to overcome the problems occurs in existing SNS. So, to make your account more protective it is need to build privacy policies at user level. 'Two Tales of Privacy' means privacy policies hold between two communicating parties without being dependent on server of that specific site. These policies are only specified by account holder. Thus, it results into each user can specify whom to give access of any post. For that user can specify own attributes regarding who can get access of the post specified by him/her. The attributes are like the specific group of people or the special characteristic of people and user can only give access to them by restricting others. Attribute based data sharing provides the new way establishing
Secure communication. People can shares their views, ideas, confidential data of their choices to those who satisfises the attributes specified by data owner.

To understand this, let us consider below example.

Example:

When any two users are communicating with each other, Let, user1 sends any message to the user2 then at a same time it defines the attributes to deliver message only to the respective user. The encrypted message along with specified attributes both are pass through the server, but server doesn't access it. When that particular message is sends to the user2 and if it satisfies the attributes specified by user1, then only the message which is in encrypted form is accessible to user2. Since, message is in encrypted form then it should get decrypted to understand by the user. Each user has its own private key and public key. But, to decrypt message it requires special secret key and that key is provided by sender user1. Now to access the content of message user2 will send key request to the user1. User1 will respond by sending decryption key to user2 if and only if user1 wants to give access of that message to the user2. And by using that secret key user2 will decrypt the message.

3.1 Proposed Algorithms:

3.1.1 RSA

To create key for message encryption, that can be encrypt and decrypt using RSA encryption algorithm. RSA is asymmetric key cryptography algorithm which is invented by three scientists **Rivest, Shamir, Adleman** in 1977.

RSA consists of following steps:

1. Key Generation
2. Message Encryption
3. Message Decryption

1. **Key Generation**

RSA involves a public key and a private key. The public key can be known by everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key. The keys for the RSA algorithm are generated the following way:

1. Select any two prime numbers 'p' and 'q'.

These prime numbers can be any random numbers. This is for more security purpose.

2. Calculate value of n= p * q.
   - 'n' is modulus for both keys that is public keys and private keys. The length of 'n' is expressed in bits called as key length.

3. Calculate φ(n)=φ(p) * φ(q)=(p-1) * (q-1)=(p+q-1)
   Where, 'φ' is Euler's Quotient Function.
4. Select an integer 'e' such that, 1 < e < φ (n)
   And gcd (e, φ (n)) = 1.
   Where, 'e' and 'φ (n)' are coprime.
   - Now, 'e' is prime key. 'e' has short length and also has small hamming value. So, it helps in better encryption.
5. Calculate'd', where d = e ^ -1 mod (φ (n)). And'd' is multiplicative inverse of e (mod φ (n)).
   - It can be gives as, d.e = 1 (mod φ (n)).
   - This is computed using extended Euclidian Algorithm.
   - Finally, 'd ' is considered as private key.

Now, the public key has modulus 'n' and 'e' as public key. Similarly, private key consists of modulus 'n' and private

key'd' , which has to be kept secret. Along with this p, q, and φ (n) must be secret.

2. **Encryption**

Message can be encrypted with,
c = m ^ e mod (n).
Where, 'c' is cipher text.

3. **Decryption**

Message can be decrypted with,
M= c ^ d mod (n).
Where, 'M' is message.

So, by using RSA encryption algorithm we can encrypt the message. Initially, we are giving encryption to text only but in future it can be possible to multimedia files also. [https://www.cs.utexas.edu/~mitra/honors/soln.html]

3.1.2 Diffie-Hellman Algorithm

Now, the keys generated by RSA encryption algorithm are separate for each message. It is need to use those keys to get access of actual message. So, here we are proposed to use Diffie-Hellman key exchange algorithm to exchange the keys. Diffie-Hellman is an Assymmetric key cryptography key exchange algorithm.

Steps in Diffie-Hellman Algorithm:

1) Take two public prime numbers 'n' and 'g'.
2) Both users will generate private numbers 'x' and 'y'.
3) Let, User 'A' will calculate A= g^x mod (n).
   User 'B' will calculate B= g^y mod (n).
4) At this step both users exchange calculated values of A and B.
5) User 'A' by using value of B will calculate,
   K1=B^x mod (n).
   And 'B' will calculate,
   K2=A^y mod (n).
6) Finally, K1 and K2 are the decryption keys used by both users 'A' and 'B' respectively.[http://searchsecurity.techtarget.com/definition/Diffie-Hellman-key-exchange]

Conclusion

'Two tales of privacy' enhances the ability of users to assign their own privacy policies instead of depending on the server of that site. User can categorize people based on attributes and maintains privacy of his own account. Along with categories users are able to communicate by encrypting data to make the communication more secure**.** Category based sharing is nothing but attribute based sharing where user can control whom to give access for which type of data. This is new era of data communication that fulfills some security issues.

ACKNOWLEDGMENT

We wish to thank Prof. Gosavi sir and Prof. More sir for their valuable guidence.

REFERENCES

[1] Two Tales of Privacy in Online Social Networks. IEEE Security and Privacy Vol: PP No: 99 Year 2013.
[2] Analyzing Friendliness of Exchanges in an Online Software Developer Community.6th International Workshop on Cooperative and Human Aspects of Software Engineering.
[3] Improving Security and Efficiency in Attribute-Based Data Sharing. Volume 3 Issue 1, January 2014.
[4] J. Anderson, C. Diaz, J. Bonneau, and F. Stajano. Privacy- Enabling Social Networking over Untrusted Networks. In ACM Workshop on Online Social Networks (WOSN), pages 1-6. ACM, 2009.
[5] A Study of Encryption Algorithms AES, DES and RSA for Security. Global Journal of Computer Science and Technology Network, Web & Security Volume 13 Issue 15 Version 1.0 Year 2013.
[6] Personal Information Privacy Settings of Online Social Networks and their Suitability for Mobile Internet Devices. International Journal of Security, Privacy and Trust Management (IJSPTM) vol 2, No 2, April 2013.
[7] Review Paper on Security in Diffie-Hellman Algorithm. International Journal of Advanced Research in Computer Science and Software Engineering. Volume 4, Issue 3, March 2014.