Cryptography Based Privacy Protection Mechanism for Online Social Networks

Ravindra Zarekar[1], Rahul Patil[2]

[1]Department of Computer Engg., Pimpri Chinchwad College of Engg., Savitribai Phule Pune University, India
ravizarekar007@gmail.com

[2]Asst. Professor, Department of Computer Engg., Pimpri Chinchwad College of Engg., Savitribai Phule Pune University, India
rahul.patil@pccoepune.org

Abstract

The wide use of online social networks (OSNs) such as Facebook, Google+, Twitter, etc., where users interact with each other by sharing their personal information**.** On-line social network applications severely suffer from various security and privacy exposures. One of the important issues in OSNs is that how user privacy is protected because OSN providers have full control over users' data. The OSN providers typically store users' information permanently; the privacy controls mechanism in OSNs offer limited options to users for customizing, managing and defining access policies for their data over the network. An efficient privacy protection mechanism is important for OSNs that can be used to protect the privacy of online social relationships and users' data from third parties. Cryptographic privacy protection mechanism shifts the control over data sharing back to the users by providing them with flexible and dynamic access policies. Also the proposed Validation Check Module focuses on handling the human attacks by providing an additional level of security, including auto-locking features to protect the user's account in online social network. This mechanism provides enhanced security features from both automated program attacks and the human attacks.

Keywords: OSN, Privacy, Data, Social relationships.

1. Introduction

Online Social Networks (OSNs) such as Facebook, Google+, Twitter, MySpace, Orkut, etc are becoming one of the most popular ways for users to interact online. Over the last few years, Online Social Networks (OSNs) have played an important role in changing society, offering people the ability to post their ideas, activities and build relationships, communities around shared interests. A number of social network sites are becoming a popular and useful approach in people's daily life. The popularity Online Social Networks (OSNs) such as Facebook [2] and Google+ [3], where more than 800 million and 170 million active users share their activities, information and communicate online with each other. The amount of shared digital data like messages, web links, status, photo albums is increasing and is seen to be over 2 billion posted items each day over Facebook.

The increasing importance and use of social networking in the connected world raising issues related to privacy within the online world. In Online Social Networks (OSNs) Users' data which includes personal data, friendship information are merged and stored permanently in the OSN storage space having the full control of the OSN provider. The common terms and conditions of service, which users must accept and allow the ownership of all their shared content to the OSN provider. The ownership agreement gives all the legal rights to the OSN provider to use and distribute users' data. This user's personal private data can be used for commercial purposes, promoting unnecessary resources and products. This data can also accessible to other entities by the OSN provider.

Online social relationships can change day by day so only the friends who are currently assisted access to shared data that only able to see it. So it is important to provide users the flexible facility for defining new relationships and access policies to their personal data. The customizable and flexible privacy protecting mechanism should be provided to meet users' privacy needs. In other words, shifting the control from provider-centric to user-centric is important to better protect the privacy of users. Because of this OSN providers are given limited trust and users are given full flexible control over their personal information.

Securing users' privacy in OSNs requires the following properties:

- There is a need to hide the user's private information from anyone also including the OSN provider and other than those authorized by the user.
- There is a need to allow users to flexibly define their relationships that provides variation of users' relationships in a dynamic fashion.

Cryptographic privacy protection mechanism i.e. CP2 that provides a scalable flexible solution to the privacy issues of OSNs, in this private data of user are stored in encrypted form in the OSN storage space. Also, users have full control over their data without the typical condition put by OSN providers. CP2 user can sort their friends into privacy groups and to share encrypted private data with any subset of friends. Further users have chance to dynamically allot access permissions to their friends or to restrict them at any time. Nobody except the user is aware of their defined relationships.

2. LITERATURE SURVEY

Online social Networks have been an important component of our daily life, but currently that more number of peoples are connected to the Internet.

2.1 Privacy preservation in OSN

There have been different mechanisms that provide the ability for users to protect their privacy in OSN, including FlyByNight [4], NOYB [5] and EASiER [6].

In the following, we discuss above approach based on the required privacy capabilities which are:

- OSN providers and unauthorized friends are not able to access the user's data.
- Nobody except the user is not able to know user's online social relationships in his OSN environment i.e. relational confidentiality.
- The user is able to define and control own access permissions over her friends in OSN environment. i.e. Fine-grained access control.

- The user is able to define new access policies using the combinations of friends and relationship i.e. Flexible access control
- The user is able to add a new friend or remove a friend from a relation i.e. Dynamic access control.

In FlyByNight [4], the user having collaboration with OSN provider can securely communicate with each friend or a group of them. FlyByNight uses public key cryptography for one-to-one communication and proxy cryptography for one to-many communication. The users' private data are never posted without encryption over OSN. FlyByNight has some drawbacks that are as the following: 1) FlyByNight depends on trustworthy of both FlyByNight servers and OSN. 2) The user is able to communicate with only one group at time.

NOYB [5] in OSN provide privacy using an encryption and encoding technique. Facebook is one of the popular OSN. In which user's a profile having almost 40 fields of personal and private information. Then this data is portioned into atoms that are small enough to not leak much information, and yet large enough to be internally consistent. For example name and sex of a person are contained in a single atom. NOYB uses dictionaries which store on users' computers or trusted third party. Then each private atom is pseudo randomly substituted with fake atoms from dictionaries.

When encrypting the field, for above instance, the input dictionary is that indexed by the real name and sex of the user, while the output dictionary is that indexed by the ciphered name and sex. NOYB has some limitations as the following. 1) There is no option for flexible classification of user's friends. 2) Key revocation is handled by issuing a new key.

EASiER [6], an architecture that supports fine-grained access control policies and dynamic group membership by using attribute-based encryption. EASiER does not provide flexibility for defining access permissions. In this mechanism user unable to create a new relation if he wants and also the numbers of friend's revocations are limited to a maximum number which are specified in the set up. In this mechanism the user is not able to define flexibly access policies over the combination of friends and relations.

2.2Confidentiality and access control

Considering privacy requirements in above section, OSN users with the capable to create privacy relations in such a way that:

- The confidentiality of the user's shared data and social relationships is protected from OSN providers and non-friends.
- The user is able to assign an authorized friend to access the shared data and also past or new members of the relations are not able to access future or previous shared data of the relation.

3. MODIFIED BROADCAST ENCRYPTION (BE) SCHEME

The BE scheme of [8] is used for many-to-many communication. Employing this BE scheme in such a way that each user is the admin of an instance of her BE domain. Therefore simplifying the BE scheme to provide user only one-to-many secure communication.

3.1 Setup

The administrator uses the setup algorithm [8] to create the proper bilinear maps and parameters for key sharing/accessing. It takes the number of users in the system as input and outputs the master public key (MPubK) and master private key (MPrvK). The master public key is shared between all users. The corresponding master private key belongs only to the administrator.

3.2 KeyGen

The key generation algorithm takes input as a random value and an unused index, which represents the identity of the given user. And gives private key (PrvK) as output for the corresponding user. The admin creates n private keys for each user to give the ability of producing broadcast messages to all users.

3.3 Encrypt

In encryption it takes the message and the subset of users as inputs who will access the message. Using the master public key, it outputs a header (Header) and a message encryption key (MEK). The header contains data which help the intended users to find the message encryption key used to encrypt the broadcast message.

3.4 Decrypt

In decryption it takes as user's index and its corresponding private key as input, the header for the given set and the master public key of the system. If the user's index is included in the set of intended users, the decryption algorithm can output the correct message encryption key.

4. CRYPTOGRAPHIC PRIVACY PROTECTION (CP2) MECHANISM FOR ONLINE SOCIAL NETWORKS

In OSN privacy protection framework that addresses privacy requirements are based on the following three steps:

1. The *privacy settings customization* step OSN users are able to access and have full control over their privacy settings and flexible enough to customize them. Modified Broadcast Encryption scheme presented in point 3 in such a way that each user is the administrator of her own BE domain in the system.
   This ability does not depend on OSN providers for trust.
2. The *data sharing* step allows user to sharing of private data between OSN users and their friends. In this user sets up the cryptographic key and able to shares encrypted data with intended friends.
3. The *data accessing* step allows user to assign access the user's private shared data.

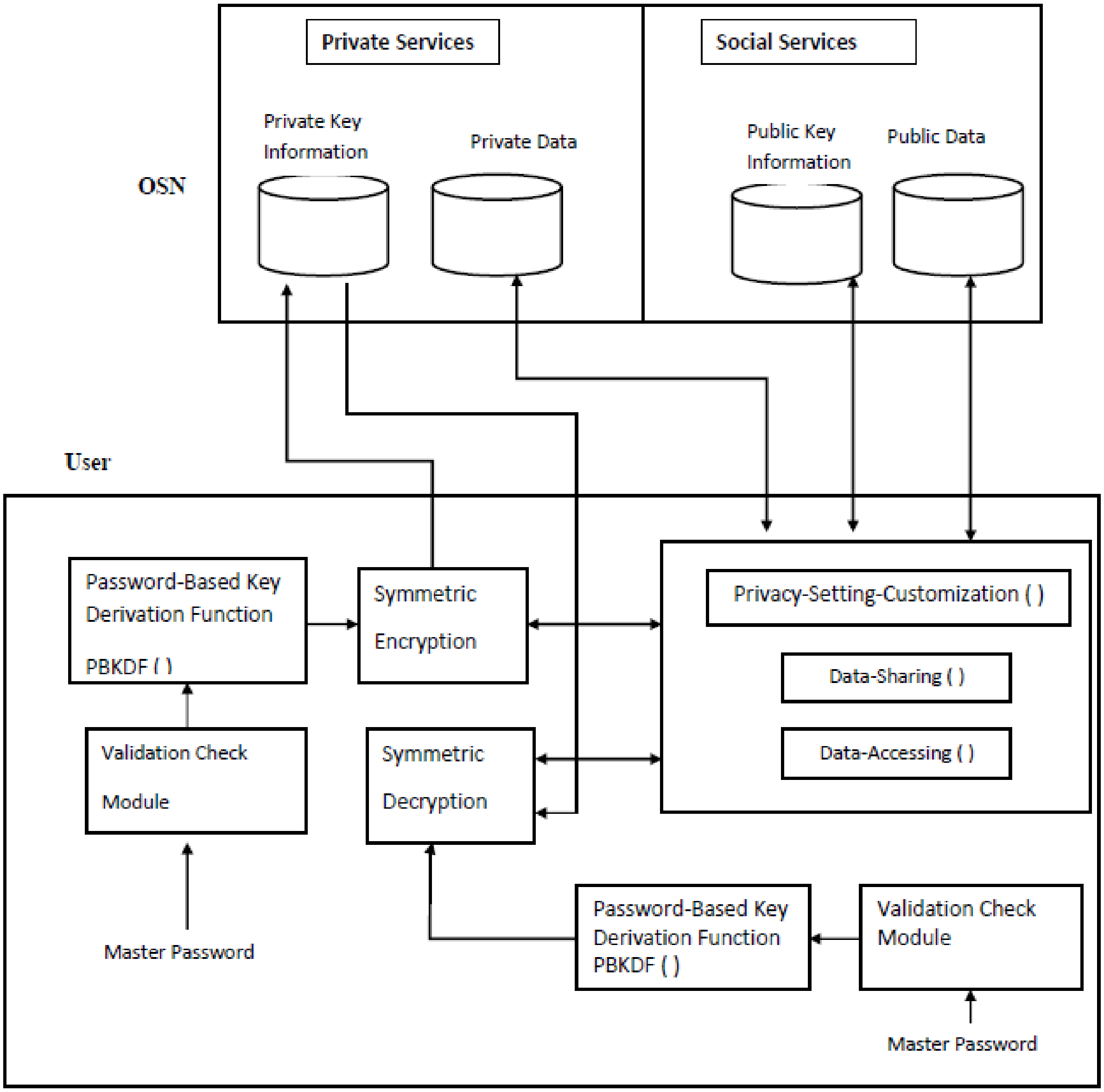

Figure 1 CP2 Framework

In above CP2 Framework interaction of user in the OSN. As with typical centralized OSNs like Facebook, CP2 framework consists of two main components i.e. the OSN provider and the Users OSN provider. The OSN provider offers services for both central online storage space and social communication for all users' information. However, contrary to the setups in the typical centralized OSNs in which all users' data are disclosed to the OSN provider, in this architecture the OSN provider utilizes only non-private information of user for social services. OSN provider also provides privacy services for storing/retrieving the users' private data to/from the OSN storage space.

In CP2 architecture the users' private data and their key information are transferred to the OSN storage space only in encrypted forms. OSN provider with a few malicious users in the network trying to access other users' private data. However, each CP2 user is her own BE authority and the user's private data is encrypted before being stored over the OSN storage space. As a result, only the authorized friends, having proper credentials, are able to get access to the corresponding plaintext of the encrypted data. The CP2 framework enables OSN provider to offer privacy services and to act as an online storage provider. However, with the emergence of cloud computing, online storage spaces are much affordable, and users can instead use the cloud services to store their private data.

The CP2 cryptographic operations are performed at the user's side. The user only has to remember a single password, imitating the same user experience in current OSNs, such as Facebook and all other web applications. The user employs her password to blind the private key information and then stores the results on the OSN storage space. Whenever the user wants private key information, the user employs her password to un-blind it. OSN provider can use an authentication method in order to send the encrypted content to the user. If an unauthorized user gets this encrypted content, he unable to access the plaintext of the encrypted data.

Validation Check Module

The sub-component i.e. Validation Check Module focuses on handling the human attacks by providing an additional level of authentication, including auto-locking and extra security features to protect the user's account as shown in Figure 2. The process of signing up is made by entering a unique username then a master password.

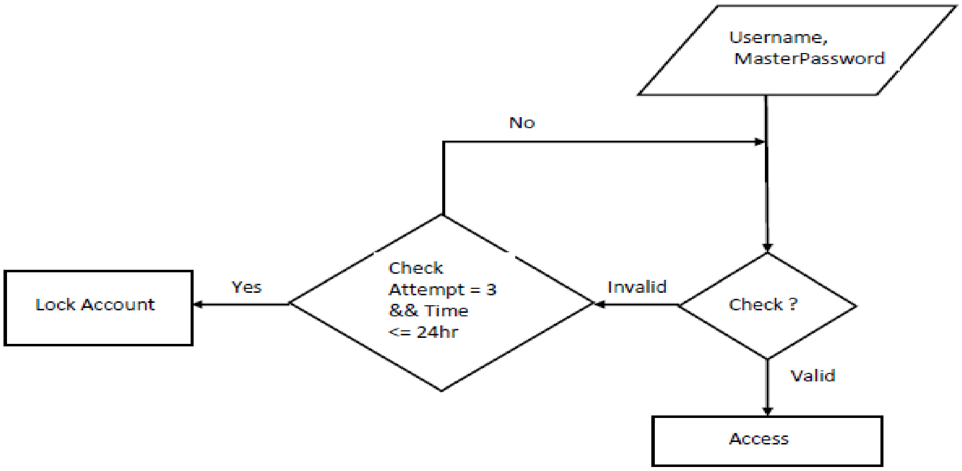

Figure 2 Validation Check Module

When an existing user wants to access her account, the user has only three chances within 24 hours to enter the correct password. If he fails put correct password, the account is automatically locked. This auto-locking feature within a short period of time provides a higher level of protection for the accounts from human attacks. This auto-locking feature provides additional higher level of security. Once the account is locked, a notification message or e-mail is send to the owner of the account informing that the account has been locked because of security reasons. Only the owners of the account can un-lock the account. Furthermore security feature is invoked for the next 24 hours to provide additional security to recently un-locked accounts, this protect from attackers trying to re-attack. This above additional security features provide enhanced security from both automated program attacks and the human attacks.

5. ANALYTICAL STUDY

In this section, we comparing some privacy preserving mechanisms based on the OSN privacy requirements. Assuming full satisfaction of the requirement by Y, partial satisfaction of the requirement by P, and failed to satisfy the requirement by -.

Table 1: comparison of some privacy preserving mechanisms.

Methods	**Protection against breach of confidentiality by OSN providers**	**Protection against breach of confidentiality by non-friends**	**Relational confidentiality**	**Access control**		
				Fine grained	**Flexible**	**Dynamic**
FlyByNight	Y	Y	-	Y	-	-
NOYB	Y	Y	-	-	-	-
EASiER	Y	Y	-	Y	P	P
CP2	Y	Y	-	Y	Y	Y

The Cryptographic privacy protection mechanism satisfies the privacy requirements because of the following reasons:

- Data confidentiality: The confidentiality of the shared data over ONS is provided with encryption, without requiring full trust the OSN provider.
- Fine-grained access control: Protecting the privacy of users, shifting control from provider-centric to user-centric therefore the CP2 mechanism is user centric, giving the user ability to manage and control access to her encrypted private data.
- Flexible access control: CP2 allows flexibility in defining access control. The user is able to flexibly define new access control policies. The users share their private data with friends and relations.
- Dynamic Access Control: the user get the ability for adding a new friend to a relation or removing/revoking a friend from a relation i.e. relationship modification.

6. Conclusions

The wide use of social networks raises privacy issues encountered by OSN users. The privacy protecting mechanism is fully customizable to satisfy users' privacy needs. In which each user was the administrator to personalize privacy settings and to define access rights. Therefore for better protecting the privacy of users, shifting control from provider-centric to user-centric is essential. Finally, providing user the ability to flexibly define new relationships and access policies to their data, in these mechanism OSN providers are getting limited trust and users are given full control over their personal information.

References

[1] Fatemeh Raji, Ali Miri, Mohammad Davarpanah Jazi, "CP2: Cryptographic privacy protection framework for online social networks", Computers and Electrical Engineering – Volume 39, issue 7, October 2013.

[2] Facebook statistics. < http://en.wikipedia.org/wiki/Google > [accessed 10.14].

[3] Google+ < http://en.wikipedia.org/wiki/Google%2B > [accessed 10.14].

[4] Lucas MM, Borisov N. FlyByNight: mitigating the privacy risks of social networking. In: 7th ACM workshop on privacy in the electronic society (WPES'08); 2008.

[5] Guha S, Tang K, Francis P. NOYB: privacy in online social networks. In: First workshop on online social networks (WOSP'08); 2008.

[6] Jahid S, Mittal P, Borisov N. EASiER: encryption-based access control in social networks with efficient revocation. In: 6th ACM symposium on information computer and communications security (ASIACCS); 2011.

[7] Raji F, Miri A, Jazi M Davarpanah, Malek B. Online social network with flexible and dynamic privacy policies. In: 15th CSI international symposium on computer science and software engineering (CSSE2011); 2011.

[8] Mohammad H. Al Shayeji, Ghufran A. Al Shiridah, and M. D. Samrajesh , "A Secure Framework for Multimedia Protection in Social Media Networks", IJIMT , Dec 2012.

[9] Malek B, Miri A. Adaptively secure broadcast encryption with short ciphertexts. Int J Netw Secur 2012.

Author Biography

Ravindra Zarekar - RAVINDRA ZAREKAR has completed his B.E. degree in Computer Engineering from Savitribai Phule Pune University in 2012 and is pursuing his M.E. degree in Computer Engineering at Pimpri Chinchwad College of Engg., Savitribai Phule Pune University, India. His research interests include Web Security, Social Network Security and Ad-hoc Network.

Prof. Rahul Patil- Prof**. Rahul Patil** is currently working as Asst. Professor in the Department of Computer Engineering in Pimpri Chinchwad College of Engg., Savitribai Phule Pune University, India. His research interests include Network Security, Data Mining.