POSN: PRIVATE INFORMATION PROTECTION IN ONLINE SOCIAL NETWORKS

Muhanad A. Al-Khalisy¹, Dr. Haider K. Hoomod²

¹Institute for Post Graduate Studies, Iraqi Commission for Computer & Informatics, Baghdad, Iraq
²Computer Science Department, University of Mustansiriyah, Baghdad, Iraq

ABSTRACT

Social relationships and networking are key components of human life. Online social networking sites (OSNs) offers a new, easy and inexpensive way to maintain already existing relationships and present oneself to others by offer people new and varied ways to communicate via the internet. The increasing number of actions in online services gives a rise to privacy concerns and risks. There are some serious privacy problems that need to be resolved in existing OSN. There has to be methods to protect user-provided data. A fully flexible privacy and security management should exist to protect private data against attackers and unauthorized users. In this work a Protected Online Social Network (POSN) developed as web 2.0 technology, privacy and security management techniques used to protect user data. The system protects user private data with three cryptographic mechanisms, RC4 and AES cipher for data encryption and public key RSA cryptographic for key encryption. The work shows how POSN provide the functionality of OSN with additional privacy benefits and acceptable performance even with cryptographic techniques used.

Keywords: POSN, OSN, Social Networks, RC4, AES, RSA, Privacy, Web 2.0.

1. INTRODUCTION

The issues of social networks have played an important role in social life and people connect online in many ways. Social networking sites, e-mail, instant messaging, video- and photo-sharing sites, and comment posting are all tools that help people communicate and socialize with each other. Each connection is a piece of the larger arena of online social networking [1].
Online social networks (OSNs) have become a de facto portal for Internet access for millions of users. These networks help users share information with their friends. In recent years, a dramatic increase of online social networks have seen such as Facebook and MySpace just to name a few; where one can set up a profile about oneself, invite friends to join the site and link these people together with the purpose of sharing information and resources [2].

It is believed that social networks have challenges for mankind as well as its opportunities has a special dynamic attribute to human social development. To provide more evidence for this point, online social networks have both positive and negative sides, definitely, it is cheaper to use online social networking for both personal and business use because most of the services are free, and at the same time, users can easily develop their social life. However, for the negative side, sometimes users have to be extra-careful in using online social networks. This is because; there are many reporting cases of hacking of one’s identity. Besides, this negative consequence, social networking sites (SNS) are online environments in which people create self-descriptive profiles and then make links with other people they know on the site [1].

While most of the leading social platforms have primitives for providing privacy in the platform and the applications they are insufficient. There are some serious privacy problems that need to be resolved in existing OSN [3].

2. SOCIAL NETWORK PRIVACY AND SECURITY

Through OSNs the users share personal identifying information about themselves as the basic purpose of online interaction and communication. But they are unaware of who will get access to their private information and in which limit.

Information is vulnerable to be revealed to a group of people unpredictably as the digital information can be easily copied and stored indefinitely. It will be a threat to the users information is revealed through different ways, and gets in the hand of the untargeted people [4].

2.1 Social Network Privacy

Privacy is the right or opportunity to decide who has access to user personal information and how that information should be used. Information privacy is “an individual’s claim to control the terms under which personal information identifiable to the individual is acquired, disclosed or used.

The actual privacy risks are believed to occur when users disclose identifiable information about themselves online to people who they do not know or normally (that is, offline) would not trust [4].

2.2 Threats of Online Social Networking

The casual posting of personal information on a digital medium might create a permanent record of the users’ indiscretions and failures of judgments that can be exploited by the third-party commentary to produce a number of threats to the users. The potential threats that the users might face can be broadly categorized in four groups: Privacy related threats, OSN variants of traditional network and information security threats, Identity related threats and Social threats [5].
In short two main classes of privacy threats distinguished: those that involve disclosure to other users (registered or not) that this paper will focus on it, and those that originate from the OSN service provider’s side.

3. TECHNOLOGIES OF THE PROPOSED POSN SYSTEM ARCHITECTURE

The development of the proposed Protected Online Social Network system composed of two parts, online social network site development and privacy management development.

Online social network site developed as Web 2.0 technology application using PHP, MySQL, Ajax and JQuery techniques. Privacy setting management developed based users privacy levels and with using of symmetric, asymmetric encryption with key management techniques.

3.1 Privacy Techniques

The proposed POSN system used many techniques to achieve more privacy for system users.

3.1.1 Privacy User Levels

The proposed system has two major privacy management settings that allow users to control and manage privacy, these are:

A. Profile Privacy Management Setting

Profile management has four levels for manage the user profile private information these are:

- **Public Level**: this level makes the information for the user’s profile public to all other user.
- **OnlyMe Level**: this level makes the information for the user’s profile hidden (private) to all other user.
- **Friends level**: this level make the information for the user’s profile hidden (private) to all other user except to the friends.
- **Customs level**: this level make the information for the user’s profile hidden (private) to all other user except to some friends of the user.

B. Share Privacy Management Setting

Share management has three levels for manage the user share information these are:

- **Public level**: this level makes the share information (comments, posts, upload) for the user public to all other user.
- **Friends level**: this level make the share information (comments, posts, upload) for the user hidden (private) to all other user except to the friends.
- **Customs level**: this level make the share information for the user hidden (private) to all other user except to some friends of the user.

To make sure that the user make manage to the privacy setting selection for all his friends, the proposed system enforce the user to select the privacy setting every time when he decide to add new friend to his list to ensure every friend have suitable privacy. Figure 2 shows POSN privacy levels.
The proposed POSN system is automatically managing the data access (data view) depend on rules based privacy settings. These rules are:

1- IF Friend Profile Privacy = “Public” SET View Profile = “True”;
2- IF Friend Share Privacy = “Public” SET View Share = “True”;
3- IF Friend Profile Privacy = “Only Me” SET View Profile = “False”;
4- IF Friend Profile Privacy = “Friend” AND Is_Friend = “True” SET View Profile = “True”; 
5- IF Friend Share Privacy = “Friend” AND Is_Friend = “True” SET View Share = “True”; 
6- IF Friend Profile Privacy = “Custom” GET Related Friend Privacy: ( 
    IF Related Friend Profile Privacy = “Only Me” SET View Profile = “False”;
    IF Related Friend Profile Privacy = “Visible” SET View Profile = “True”;
    IF Related Friend Share Privacy = “Only Me” SET View Profile = “False”;
    IF Related Friend Share Privacy = “Visible” SET View Profile = “True”;
    )

3.2 Cryptography Techniques
One of the major problems that the proposed POSN system focuses on it is the members profile sensitive data, how this data become more secure in the database, additional to the privacy setting management that control who have access to this data and who are not. The proposed system use cryptographic techniques to encrypt these data in the database to become more secure and use these technique again to encrypt the key (secret word) used to encrypt these data to ensure that the process of keys distribution to the members become safely. This section will explain cryptography techniques that proposed POSN system used.
3.2.1 Combination Encryption

Every encryption algorithm have strong and weakness points, some of them related to the performance metrics were encryption throughput, CPU work load, energy cost and key size variation, for example the RC4 is fast and energy efficient for encrypting large packets. However, AES was more efficient than RC4 for a smaller packet size [6]. A new hybrid cipher can develop by combining the characteristics of two ciphers namely AES and RC4 [7]. The characteristics of both ciphers are studied and a new cipher combining the characteristics of both ciphers is generated which is more secure than the original ciphers [7]. For this reasons, the proposed POSN system will use the above hybrid cipher (RC4AES) to encrypt the sensitive data with random key generated by the proposed system. Figure 4 shows proposed POSN hybrid cipher block diagram.

3.2.2 OpenSSL EVP Public Key Interface

EVP is an OpenSSL API (A Programming Interface) that provides a high-level interface to cryptographic functions. EVP is a high-level interface to message digests, symmetric ciphers, and public key algorithms [8].

The EVP interface also provides an interface for enveloping data using RSA keys. Data enveloping is the process of encrypting a chunk of data with RSA, typically for securely sending it to a recipient [9].

One of the features offered by the EVP interface for data encryption is the ability to encrypt the same data using several public keys. Figure 5 shows EVP interface data sealing / unsealing (opening) block diagram.
4. DESIGN AND IMPLEMENTATION OF THE POSN SYSTEM

The proposed POSN design consists of hardware and software components that both form the whole web site design. Hardware design encompasses the hardware components used in proposed web site, while software design explains the application design for the web site. Figure 6 shows the block diagram that explains the main architecture of the proposed POSN.
4.1 The Proposed POSN System Overview

The constitution of the proposed POSN system’s design to be contains the integration of the technologies described in section two; Figure 8 depicts the components of this design where the system in addition to main modules it contains two Substantial modules (privacy management module and cryptographic module).

![Figure 8 The Components of The Proposed POSN System.](image)

4.2 Application Design

The application design perform the whole structure of the proposed Protected Online Social Network (POSN) site, including all site web pages design, web forms used for gathering information and selection menus used by users.

The proposed POSN application design divided into two parts: Front-End Area (User Area design and Encryptions system (cryptography) design).

4.2.1 Front-End Area Design

Front-End area design consists of the following parts
A-User authentication and user registration
B-Adding new post.
C-Adding comments to post.
D-Share media.
E-Change Privacy setting.
F-Add and Delete Friends.
G-Send /receive Private Messages.
H-Edit Profile.
I-Edit Account Setting.
J-Search for a member (Friend).
The proposed POSN site is accessed at the page index.php (the home page) where any user can access this page. Any user tries to access another page directly from URL he will be restricted to access the home page. In this page, visitor can view post titles, and do search for members. Only public post or comments appear on the home page in addition to the name of the post’s author and the date of creation. Figure 9 shows the proposed POSN home page.

![Figure 9 the Proposed POSN Home Page (Index.php)](image)

### 4.3 Encryptions Process Design

The proposed POSN system encrypted the private data (sensitive data) using symmetric RC4 encryption with a randomly generated secret key (session key), which is then encrypted using RSA Asymmetric key encryption with multiple 1024 bit public keys. The encrypted data is known as sealed data, and the encrypted secret key is known as an envelope key that will be distribute to the proposed POSN members or friends for use in decryption process. The proposed system re-encrypt the sealed data using AES encryption with new 128 bit randomly key generated called AES key to generate the encrypted data that called (Encrypted Private Data). To decrypt the data, the recipient must have the related envelope key, the AES key and the related private key. The function conveniently allows for multiple recipients by accepting an array of public keys. Figure 11 shows the proposed POSN private data encryption block diagram while figure 12 shows the proposed POSN private data decryption block diagram.
The proposed system will generate two pair keys (private key and public key) for every user, these keys will use for RSA 1024 bit asymmetrically encryption to encrypt the random key (which is relatively small) that will be use to encrypt private data as mention before.

For add more security to the sensitive data, when any member try to add new friend to his friend list the proposed system will decrypt and encrypt data again and generate new envelop keys for all member’s friends and redistribute these envelop keys again.

When some member try to access profile information for his friend and this member have access right privacy (as mention in section 3 privacy user levels), the proposed system will check for related envelop key for this member in friend envelop key table. If it matches, the envelop key will be used with the member’s private key to decrypt the data. But if the proposed system did not find any envelop key related matches, the system will display encrypted data message to the member.
5. EVALUATION OF THE PROPOSED SYSTEM

This section proceeds with results evaluation of the proposed POSN implementation. Then, it presents the performance evaluation.

5.1 Privacy Evaluation

After the implementation of the proposed POSN system, privacy evaluation tests measure. The proposed POSN installed (published) in the real environment ISP (Internet service provider). Many user accounts were created (registered), each user has different privacy setting, some of them are friends, group of friends and the other was not (public user).

Many activities from the users happened during evaluation time. Friend request, add as friend, remove friend, change privacy, text post, media post and post comments are common activates between those users. Those users try to feed back their opinions about the privacy control for the proposed POSN by post their comments on it.

Many users show their acceptance about how the proposed privacy setting control their profile sensitive data access especially when they used the proposed POSN customs privacy setting facilities. They mention how the proposed system enforce them to select a perpetrate selection for their privacy setting in the first try to login to the proposed system after registrations, by this the proposed system erase the problem of user unawareness of what his default privacy setting was.

Some user also mention how the proposed system direct them to set the privacy setting for every user they try to add as friend, by this the proposed system prevent the user from the problem of queuing many friends in his list without setting or knowing his privacy setting for them. Figure 13 shows the result page of how the user “evaluation user 1” sees his profile information.

![Figure 13 How Evaluation User 1 See His Profile Page](image-url)
Figure 14 shows the result page of how non friends or public users see the same profile from inside or outside the proposed POSN with restricted information. In this case the user selected “only me” profile privacy setting.

Figure 15 show how “evaluation user 1” profile page look like to public or non register user when they ask for it, in this case the user previously selected “public view” setting for his profile privacy. Also the figure show how some profile sensitive information still invisible or encrypted in spite of the user selected public view setting for his profile. By this the proposed system protects private sensitive user data from any intruders or malicious user in case of the member unawareness or mistakenly set “public view” settings to his profile.
In case of friend’s relation with general “friends” privacy setting set, (evaluation user 2 a friend with evaluation user 1). Figure 16 show how “evaluation user 2” sees the “evaluation user 1’s” profile information, the Proposed POSN display all information to all “evaluation user 1’s” friend.

In case of friend relation with “custom” privacy setting set. Figure 17 show how “evaluation user 2” sees the “evaluation user 1’s” profile information, the proposed POSN prevent “evaluation user 2” from see “evaluation user 1’s” profile information but it let him to see share information only (user post) in spite of the two user was a friend. By this the proposed POSN solve the problem of how the user can classify or categorize his friends. This done by let the user to set special privacy for every friend in his list separately, so everyone in his list have its own privacy setting set.

Figure 16 How Evaluation User 2 See Evaluation User 1’s Profile Page In Case of General “Friend View” Privacy Setting Set

Figure 17 How Evaluation User 2 See Evaluation User 1’s Profile Page In Case of “Custom View” Privacy Setting Set
Table 4 shows the privacy setting result of proposed POSN related to user state.

Table 4 Privacy Setting Result of Proposed POSN Related to User Relation state

<table>
<thead>
<tr>
<th>User 1 to User 2 Relation</th>
<th>User 2 Profile Privacy</th>
<th>User 2 Share Privacy</th>
<th>Visible Profile Data</th>
<th>Visible Share Data</th>
<th>Sensitive Data Visible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non friend</td>
<td>Public</td>
<td>Public</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Non friend</td>
<td>Only me</td>
<td>Public</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Non friend</td>
<td>Friend</td>
<td>Public</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Non friend</td>
<td>Public</td>
<td>Friend</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Non friend</td>
<td>Only me</td>
<td>Friend</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Non friend</td>
<td>Friend</td>
<td>Friend</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Friend</td>
<td>Public</td>
<td>Public</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Friend</td>
<td>Only me</td>
<td>Public</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Friend</td>
<td>Friend</td>
<td>Public</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Custom friend</td>
<td>Only me</td>
<td>Only me</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Custom friend</td>
<td>Only me</td>
<td>Visible</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Custom friend</td>
<td>Visible</td>
<td>Only me</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Custom friend</td>
<td>Visible</td>
<td>Visible</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

5.2 Performance Evaluation

The processing and storage requirements of Proposed POSN with measure the time to render POSN encrypted web pages was quantified.

The evaluated of POSN implementation done on a desktop computer using a core i3 2.10 GHz processor and 4 GB of RAM. The desktop, storage service, and application server are connected through a router which introduces an artificial delay that represents a case where the storage service is far away from the user.

In order to analyze the performance of the implementation, it should focus on the cryptographic algorithms that represent the most expensive operations and the response of the tiny link server, which include the network latency and server process.

A profile for “Ali” was built, who was given 25 friends. Additionally, there were 70 strangers user. The database maintained tables for user data, friend lists, friends privacy and encryption keys, all of which were filled with pieces of fake data. User sensitive data are encrypted using RC4AES with key encryption using RSA through the PHP Openssl cryptographic library functions extension. On the test machine, it takes 0.7 milliseconds on average to encrypt a 16 Bytes user sensitive data block, which supports over 1400 sensitive data block encryptions per second. Table 5 show the overhead of the encrypted data regarding the original data.

The performance is determined on the basis of the time taken to encrypt and decrypt the data. Table 6 show Performance of ciphers base time vs. data size.
There is a substantial increase in the size of the stored data, and this will affect both the storage capacity of the storage services and the network resources required to transfer data. The storage services are inherently distributed, so they should be able to scale to support the needs of the system.

Also the original data are texts dealing with social networks typical profile information like “email, website, gender, employ etc...” Because it is text-based data, the overhead imposed can be easily mitigated if the storage server utilizes some text compression technique before the storage is made.

### Table 5 Overhead of the Encrypted Data Regarding the Original Data

<table>
<thead>
<tr>
<th>Original Message (bytes)</th>
<th>Encrypted Time (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>0.7</td>
</tr>
<tr>
<td>32</td>
<td>0.11</td>
</tr>
<tr>
<td>64</td>
<td>0.13</td>
</tr>
<tr>
<td>128</td>
<td>0.16</td>
</tr>
<tr>
<td>255</td>
<td>0.17</td>
</tr>
</tbody>
</table>

The page load time of proposed POSN was measure. Where load time for profile page with decryption for 16 byte data item (sensitive data) was average about 0.050 second. Table 7 shows profile page load time vs. data size.

Page load times increase linearly with the size of data item or the number of elements in the profile need to encrypt. The median page load time is 0.060 seconds and the maximum is 0.100 seconds. Most pages consist of a few, small entries, so most are loaded quickly. So that the time indicating that retrieving keys and decryption process is not too expensive.

### Table 6 Performance of Ciphers Base Time vs. Data Size

<table>
<thead>
<tr>
<th>Original Message (bytes)</th>
<th>Encrypted Message (bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>44</td>
</tr>
<tr>
<td>32</td>
<td>64</td>
</tr>
<tr>
<td>64</td>
<td>108</td>
</tr>
<tr>
<td>128</td>
<td>192</td>
</tr>
<tr>
<td>255</td>
<td>364</td>
</tr>
</tbody>
</table>

The page load time of proposed POSN was measure. Where load time for profile page with decryption for 16 byte data item (sensitive data) was average about 0.050 second. Table 7 shows profile page load time vs. data size.
The evaluations show that it can achieve privacy in online social networks with acceptable performance even with cryptographic techniques used.

6. CONCLUSIONS

A proposed protected online social network (POSN) site that was developed as web 2.0 technologies application with privacy management and cryptography techniques showed that it can successfully protect private information in online social network from user-related privacy threats.

The proposed POSN will solve the problem of how the user can classify or categorize his friends by using custom setting.

The proposed system used the RSA in order to achieve the same ends by encrypting a symmetric key which is used to perform actual data encryption and decryption.

The proposed POSN re-encrypts the private data every time that the user try to add new friend to his list, this will add more security power to the system by regenerating new key for the user.

The median page load times for profile page in the proposed POSN is 0.5 seconds and the median size of the encrypted profile sensitive data is 108 byte. This time indicates that retrieving keys and decryption process is not too expensive. It shows that one can achieve privacy in OSNs with an acceptable performance even when cryptographic technique used and therefore the proposed approach shows that it is possible to be implemented in a real environment.

7. REFERENCES


Table 7 Profile Page Load Time vs. Sensitive Data Size

<table>
<thead>
<tr>
<th>Sensitive Data (bytes)</th>
<th>Page Load Time (s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>0.050</td>
</tr>
<tr>
<td>32</td>
<td>0.060</td>
</tr>
<tr>
<td>64</td>
<td>0.080</td>
</tr>
<tr>
<td>128</td>
<td>0.090</td>
</tr>
<tr>
<td>255</td>
<td>0.100</td>
</tr>
</tbody>
</table>


