ISSN 2395-1621

Protecting Online Social Network From Data Leakage Consequences

[#1]Reshma Totare, [#2]Akash Khalse, [#3]Pradip Shilkande, [#4]Ganesha Musmuse, [#5]Harshada Rathod

[1]reshma.gaykar@gmail.com
[2]khalseaakash18@gmail.com

[#12]AISSMS IOIT , Department of Information Technology,Kennedy Road Pune- 411001 India,Shri. Savitribai Phule Pune University

ABSTRACT

Social networking becomes increasingly important due to the recent surge in online interaction. Many people find Social networks very interesting, because they offer wide range of online services for socializing between friends and people that have similar interests. However sharing these interests online and using them without considering the security factor can lead a user to become victim of a hacker. There are many different types of threats exists that might put the online social network's users at cyber security risk. One of the major problem is that users often share some contents like photos, text, videos etc. Hackers or other illegal people may download and user these contents for illegal usage. So to prevent this the proposed system aims at developing a module where in each and every content be it a text, a photo, a video it will contain its own unique ID. This unique id will be stored in the database along with the metadata of the content. If the user reports of illegal data leakage and illegal use of his shared and uploaded data then the data will be deleted online from the online social networking site.

ARTICLE INFO

Article History

Received :26th April 2016

Received in revised form :

28th April 2016

Accepted : 30th April 2016

Published online :

3rd May 2016

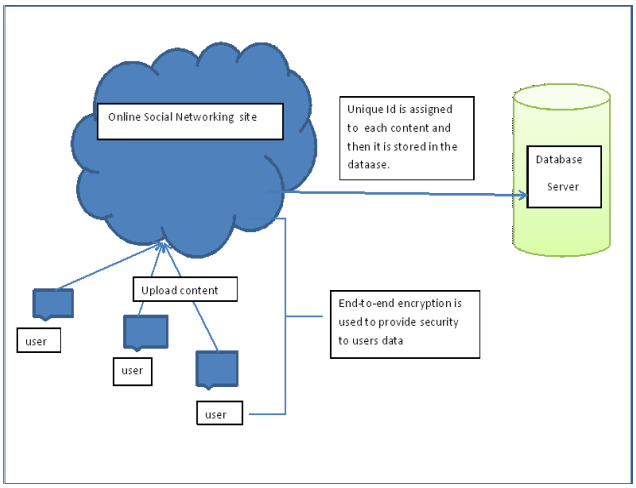
Keywords— **OTP, Data Id Assignment, End-to-end Encryption.**

I. INTRODUCTION

Online Social Networking has become a part of our everyday life. Even the teenagers and the youngsters use social networking sites to communicate and to keep in touch with their friends. [1]Due to lack of knowledge of the harmful possibilities of attacks by hackers and other cyber criminals some people fall prey to these attacks. The information that is shared in social networks can be used against the user to launch cyber-attacks. As soon as any information is posted on a social network, it is not private anymore. Increase in the amount of shared information also increases the amount of chance of exposure of information leakage risks. Hackers are always one step ahead of security specialists. They always misuse human vulnerabilities to launch social engineering attacks. The hackers can also use sensitive information like the texts, photos, and videos shared by the users on the online social networking site. Thus to avoid the illegal usage of this sensitive information the proposed system is developed. The paper gives a brief description of the same. The end-to-end encryption technique can also be used to secure text messages. The end-to-end encryption is a mechanism wherein only the two persons communicating with each other can have the key through which they can decrypt the messages they have sent and received to each other. No internet provider or telecom companies can act as a intruder and can tamper their communication.

II. SYSTEM ARCHITECTURE

The following is the system architecture of the proposed system. It includes the online social networking site, the central database, users and the mechanisms used to provide security to the user's data.



III. WORKING OF THE SYSTEM

The system basically aims at providing safe path for communication and data sharing over the social network sites. The communication through texts messages is made secure with the use of end-to-end encryption. The end-to-end encryption allows users to have their own private key though which they can decrypt their messages. The end-to-end encryption technique is secure because it hardly involves any interruption of the internet service providers, telecom companies or the application service providers. Thus they are away from the decryption key and they cannot easily decrypt the encrypt the messages. This ensures privacy and security of the user using the social networking site and communicating through text messages. The second very import module is the Data Id Assignment module in the system. When the user shares any content on the social networking site the DIA attaches a unique Id to it and then only the content is stored in the site's database. After the content is stored in the database then it is available for manipulation through some smart coding. The programmers of the sites can program a smart coding through which they can manipulate the content be it on any device. Suppose a report is received by a user against a content being leaked and misused. Then the site surveillance team will look into it immediately and find out its ID. Using this ID the engineers will program a smart code through which the content which is leaked will be manipulated. The content can thus receive a command through the smart code which will activate some behaviour of the content. When the device is connected to the internet the content will automatically receive the broadcasted code and thus the smart code command. The content then will change its behaviour on its own. Thus the content can be deleted, can be changed, can be tampered etc according to the wish of the owner of the content who posted and shared it. Thus in this way the negative consequences of the data leakage can be avoided. Thus providing security to the user and user's data.

IV. MODULES IN THE SYSTEM

1. **Online Social Networking Site :**
   This is the online social networking site the user is going to use. For ex say facebook, google+, etc. The user will login to the site with his credentials and access his profile.

2. **Database Server :**
   The user when posts some content to the site it will get uploaded to the database.

3. **Unique ID :**
   Before the data is saved into the database each and every content is assigned a unique Id through which it will be processed when needed.

4. **End-to-end encryption :**
   End-to-end encryption[2] is provided to the users profile while communicating with other users of the social networking site. This will ensure no data and the communication secrets is leaked easily.

V. SYSTEM FUNCTIONALITIES

1. **End-to-end Encryption :**
   End-to-end encryption is a system of communication where only people who can read the messages are the people communicating. No eavesdropper can access the cryptographic keys needed to decrypt the conversation – not even a company that runs the messaging service. Surveillance and tampering are impossible because no third-parties can decipher the data being communicated or stored. The [3]E2EE systems can encrypt data using a pre-arranged string of symbols, called a pre-shared secret (PGP), or a one-time secret derived from such a pre-shared secret (DUKPT). They can also negotiate a secret key on the spot using Diffie-Hellman key exchange.

2. **DIA Algorithm :**
   DIA stands for Data Id Assignment algorithm. In this algorithm the data let it be a text, a photo, a video it is assigned a unique id depending upon its nature. This id is assigned to the data before it is stored in the database. This id once assigned to the data is used to manipulate the data online in the future. The id will be in such form that any manipulation commands can be given to the data and the command will ask the data to manipulate itself. Thus the command can make a data delete itself , alter itself and more. The social network can broadcast a code targeting a specific if to follow certain command. So when that device comes online with that data, the data receives the broadcast code online and the functioning of the command assigned to the data with that id starts to execute the command. Thus the data can be kept safe from illegal usage and the user can be feel secure even if his significant and sensitive information is leaked on to the internet.

VI. CONCLUSION

The theoretical conclusion is that the end-to-end encryption provides a secure channel to communicate. Thus providing privacy to the user's communication. Secondly the Data ID Assignment provides facility to manipulate the content which is leaked. We can delete or alter the content through a smart code. Thus ensuring security to user's content which is leaked. Thus providing more security and privacy to the user.

VII. FUTURE SCOPE

The future scope of the system may involve advancement in the discussed modules and working of the system. It may also involve advanced Data Leak Prevention and Recovery Mechanisms.

ACKNOWLEDGEMENT

We take great pleasure in presenting our Paper on "Securing Online Social Network From Contemporary Threats". It is often the result of invaluable contribution of number of individuals in direct or indirect manner. The motivation factor for this paper was inspiration given to us by our faculty members Prof. Pritesh Patil and our guide Mrs. Reshma Y. Totare.

We are grateful to our faculty for their constant help and encouragement with their valuable advices and suggestions.

REFRENCES

.

[1] Securing online social network from contemporary threats. IERJ journal Volume I Issue 11 Page No: 1653-1656.

[2] https://en.wikipedia.org/wiki/end-to-end_encrption

[3] B. Krishnamurthy and C.E Wills. "On the Leakage of personally identifiable information via online social networks".

[4] S. Livingstone and L. Haddon, Child Safety Online: Global Challenges and strategies, 2011.

[5] Security Threats in Online Social Networks.
Published in : Informatics and Creative Multimedia (ICICM), 2013 International Conference on 4-6th September 2013.

