IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 3, March 2020

Prevention of Multiple Collusion Attacks and Spammer Prevention in OSN's

Surya.S[1], Tamil Arasan.S[2], Venkatash.K[3], Balaji.A.S[4]

Student, B.E. Computer Science and Engineering, Anand Institute of Higher Technology, Chennai, India[1, 2, 3]

Assistant Professor - CSE, Anand Institute of Higher Technology, Chennai, India[4]

Abstract: Online Social Networks (OSNs) have become very popular in recent years, such as Facebook and Twitter, which have been part of many people's daily life. The project starts as simple study on small social clique model, aiming to deeply understand users' friendship types and reveal the fundamental reasons why collusion attacks can be done successfully. Based on observations made from this model, we further propose to classify social network users into non-popular users and popular users; develop different attacks strategies against them and illustrate the attack effectiveness in a general social network through different scenarios. Experiment results show that our proposed prevention of collusion attack strategy has achieved high success rate by using limited number of malicious requestors. However, the rise of social network services is also leading to the increase of unwanted, disruptive information from spammers. Negative effects of social spammers do not only annoy users, but also lead to financial loss and privacy issues. Spammers are prevented using an administrator to approve or disapprove contents.

Keywords: Collusion attacks, Online Social Networks (OSN's), Spam.

I. INTRODUCTION

As millions of users use OSNs every day to conduct social activities, search new friends and connect to them, the development of privacy preserving friend search engines has attracted wide attention. To increase their sociability and attract more users, OSNs tend to release users' friends as many as possible, as it is believed that the larger number of common friends are displayed, the more likely the requestor and the queried user would connect later. However, this search engine may expose more friendship information than what a queried user is willing to share, which is considered as a privacy breach. The authors in [3] have presented a list of threats against OSN users' relationship privacy and the corresponding requirements that privacy mechanisms should fulfil. In [4], a trust chain-based friend recommendation algorithm is proposed with the purpose of preserving users' privacy. A few recent studies also work on protecting users' location information so that their sensitive friendship will not be exposed because of frequent co-locations [2]. Also, they concluded that without appropriate defences, one could discover all users' friendships in the OSN without using many queries. If such a privacy breach is not well dealt with, the OSN users may feel panic and hesitate to continue using the OSNs. However, collusion attacks, where multiple malicious requestors share their knowledge and co-ordinately launch queries, may make the defence scheme ineffective. In-depth analysis has been provided on querying a small-scale complete graph as well as a general network in various scenarios, which well explains the fundamental reasons of why and how the proposed attack is designed. In the advanced collusion attack, in which multiple malicious requestors closely coordinate with one another to launch their queries on different but related users in well-designed orders will be prevented by limiting the number of login attempts and thus banning the particular IP Address if the requestor attempts more than the limit. Users also need to provide an OTP while logging in with correct credentials thus providing more security.

II. EXISTING SYSTEM

In the existing system previous work has proposed a privacy preservation solution that can effectively boost OSNs' sociability while protecting users' friendship privacy against attacks launched by individual malicious requestor. A post needs to be reported multiple times to be banned in current OSN's. In current system, there is no efficient algorithm to stop multiple collusion attacks. It is the complexity task for maintaining the privacy and security for the users from various kinds of malicious attacks.

III. SYSTEM ARCHITECTURE

PROPOSED SYSTEM:

The proposed advanced collusion attack in [1], where a victim user's friendship privacy can be compromised through a series of carefully designed queries coordinately launched by multiple malicious requestors can be prevented using limited attempts per requestor. multiple attackers with very limited initial knowledge (i.e. only the victim node) can

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 3, March 2020

successfully penetrate the defense and violate victim node's privacy settings on friend search engine. When a requestor exceeds his number of attempts to login, then the IP address of the requestor will be banned, and he cannot try another attempt after getting blocked. For this technique, we use Fisher's Algorithm for acquiring requestor's IP address (Fishing). If the authorized user tries to login with correct credentials, then he needs to provide an OTP (sent to user's registered email-id) for further security. Spams are then detected by an admin who check if the posts are malicious, unwanted, or it has to do something with privacy. To classify posts, we use Naïve Bayes Algorithm and Linear regression for predicting. The admin will report the post as spam and the post will be removed and the admin sends a warning to the user.

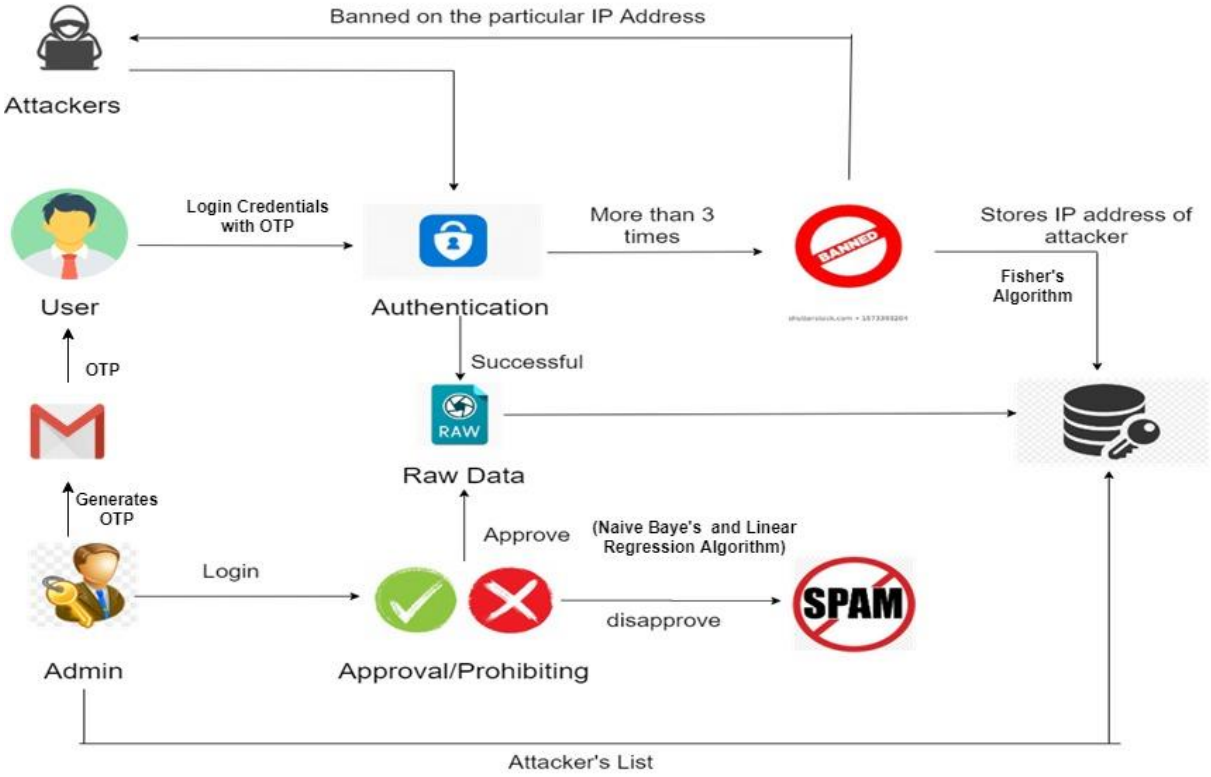

Fig .1 Architecture Diagram

IV. MODULES

1. User authentication module
2. Landing page module
a) Image upload module
b) Status upload module
3. Admin page module
4. Content approval/Decline activity module
5. Attacker records module

1. User Authentication Module:

Every user gets authenticated by providing their credentials in the login form. Users' needs to register with relevant details that is needed to provide an account. User is authenticated based on their credentials and no user can provide false credentials more than 3 times because the IP address will be banned. Optimization algorithm i.e. Fisher's Fishing Algorithm will be running in the background to check whether the IP address is already banned or not. It is a novel optimization algorithm, it checks for fishers.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 3, March 2020

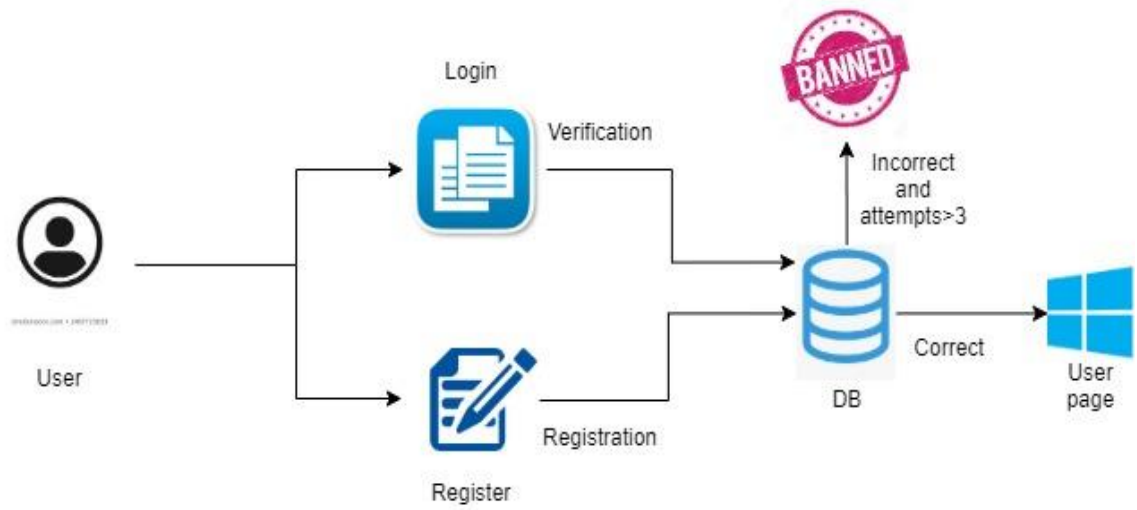

Fig.2 User Authentication Module

2. Landing Page Module:

If user gets authenticated, he will land on his home page, else if the user doesn't get authenticated (i.e. in case of attack) he'll be redirected to page which displays an alert "you are banned".

2i) Image upload module: User can add a post image through this page, which further will be checked by admin for prevention of spam.

2ii) Status upload module: User can add a status post through this page, which further will be checked by admin for prevention of spam.

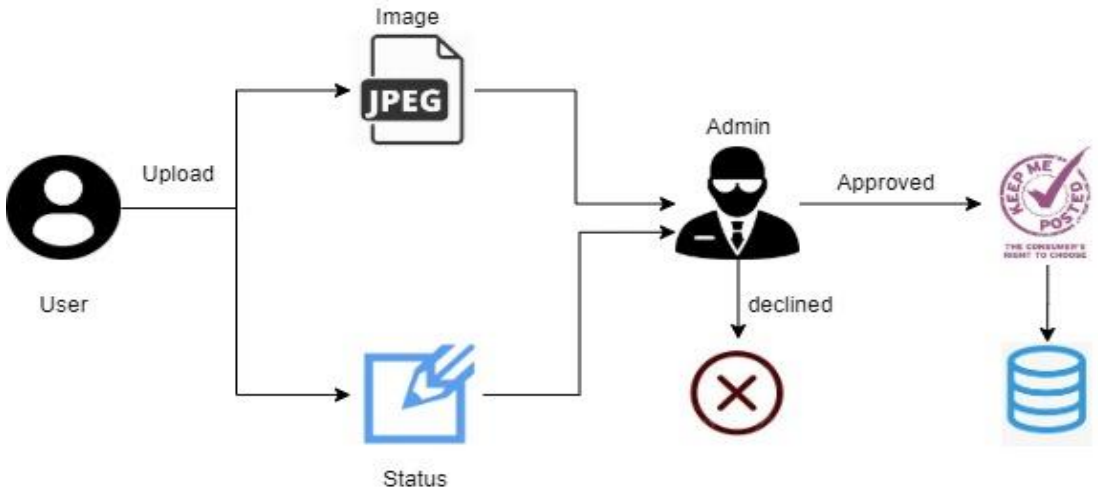

Fig.3 Landing Page Module

3. Admin Page Module:

Admin's need to provide their credentials which will land them in admin home page. Collusion attack in here is also possible, so only 3 attempts will be allowed for admin also. Admin has access to attacker's record, post approval and also he checks for accounts that has been attacked and bans those accounts and sends an OTP (randomly generated) to the user's registered email id which the user needs to provide during next time he logins.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 3, March 2020

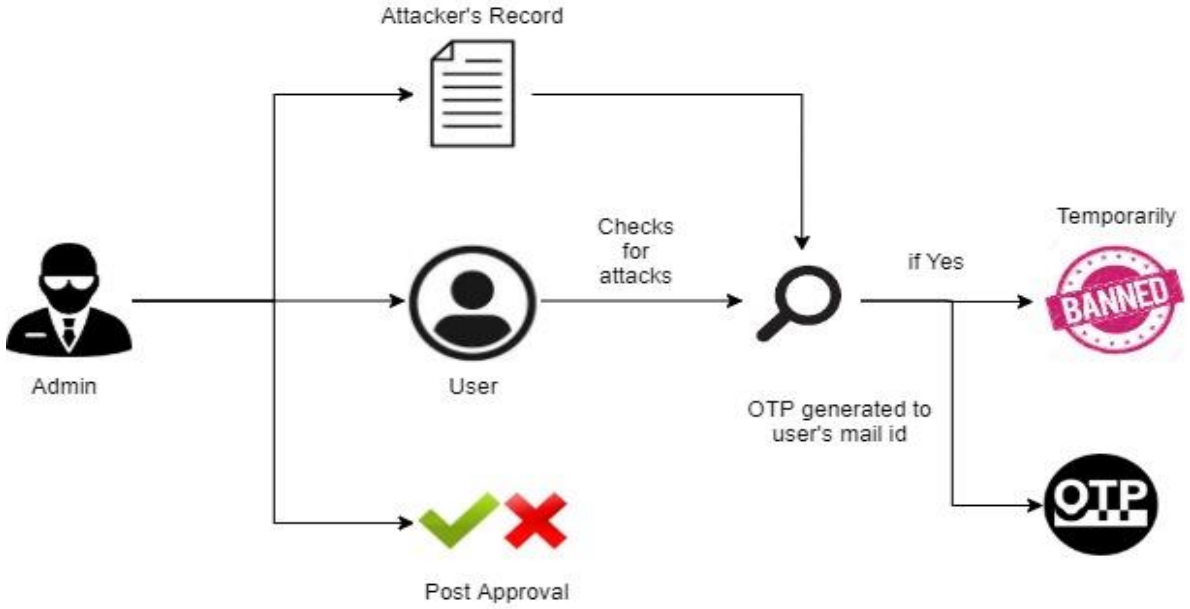

Fig.4 Admin Page's Module

4. Content Approval/Decline activity Module:

This module is only accessible to Admin, he can approve or decline the posts that have been posted by the users based on the content. The major aim of this module is to prevent spam. The admin bans users who posts more than 5 spam post for lifetime.

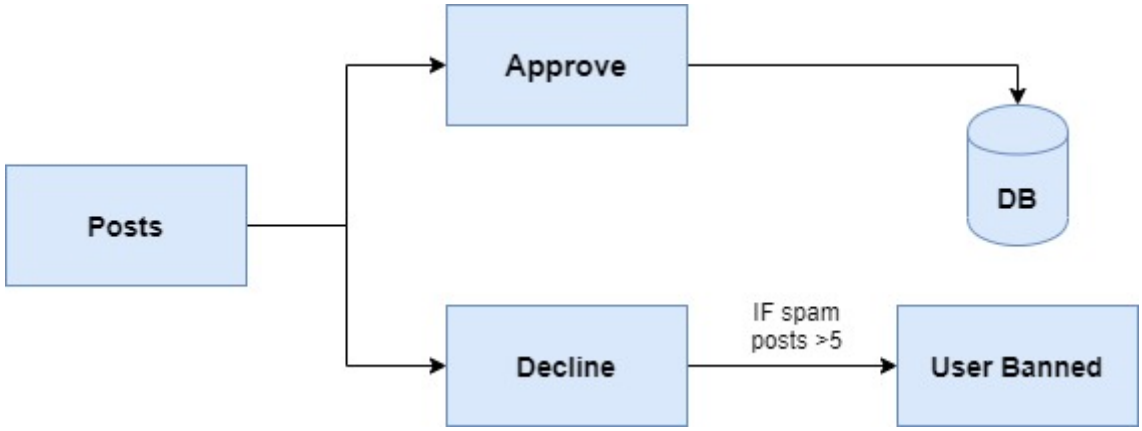

Fig.5 Content Approval/Decline activity Module

5. Attacker Records Module:

The record consists of the Attacker's IP address in the database. Using Fischer's Algorithm attacker's IP can be tracked and stored in database. The account that has been attacked will be banned temporarily. User will be notified with a random 6-digit OTP in his/her registered email if which is used for Re-Activation of a Temporarily banned account.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 3, March 2020

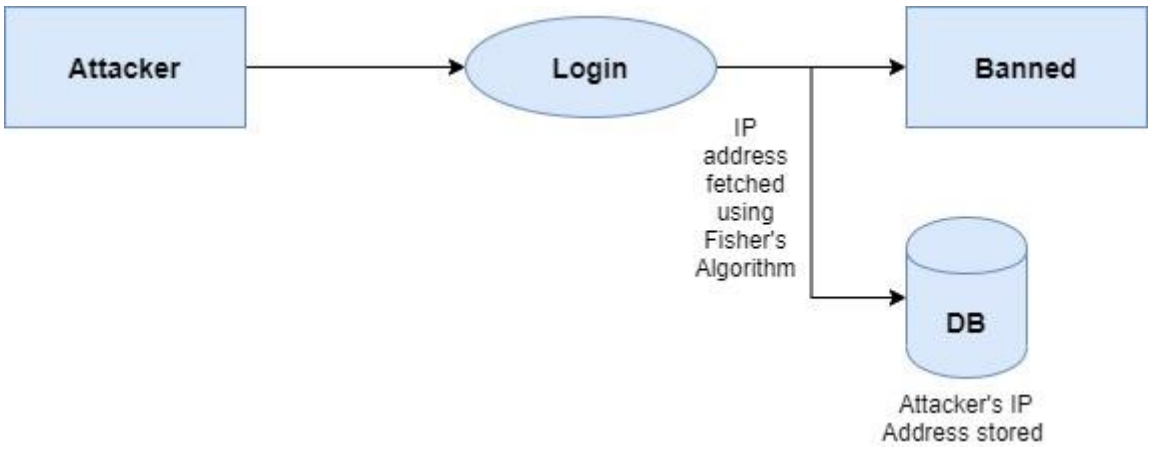

Fig.6 Attacker Records Module

V. APPLICATIONS

This attack is used in the fields of

1.Hospitals

2. Industries and companies

3. Banks

4. Educational universities

5. Military Service

VI. CONCLUSION

In this paper, the advanced collusion attack strategy where multiple attackers with very limited initial knowledge (i.e. only the victim node) can successfully penetrate the defence and violate victim node's privacy settings can be denied by limiting the number of attempts to login and banning requestors in particular IP address. Spammer detection is done by an admin who checks for malicious or spam contents.

VII. FUTURE ENHANCEMENTS

In future the admin can be replaced, where he does the spammer detection by checking each and every post that has been posted, so he can be replaced by techniques like image processing which reduces man work.

REFERENCES

[1]. J. Bonneau, J. Anderson, F. Stajano, and R. Anderson, "Eight friends are enough: social graph approximation via public listings," in Proceedings of ACM SNS'09, 2009, pp. 13–18.
[2]. Z. H. Zhou, M. Li, "Tri-training: exploiting unlabeled data using three classifiers", *IEEE Transactions on Knowledge & Data Engineering*, vol. 17, no. 11, pp. 1529-1541, 2005.
[3]. R. Fogues, J. M. Such, A. Espinosa, and A. Garcia-Fornes, "Open challenges in relationship-based privacy mechanisms for social network services," International Journal of Human-Computer Interaction.
[4]. L. Guo, C. Zhang, and Y. Fang, "A trust-based privacy-preserving friend recommendation scheme for online social networks," IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 4, pp. 413–427, 2015.
[5]. Z. Feng, H. Tan, and H. Shen, "Relationship privacy protection for mobile social network," in Advanced Cloud and Big Data (CBD), 2016 International Conference on. IEEE, 2016, pp. 215–220.