International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

Security Risk Detection and Prevention in Online Social Networking

Abhiruchi V. Rahatgaonkar[1], Prof. Dr. Vijay S. Gulhane[2], Prof. J. S. Karnewar[3]
[1]PG Scholar, [2]Professor & Head, [3]Assistant Professor, Dept. of Information Technology, Sipna College of Engineering, Amravati.

Abstract: Online Social Networking System plays an important role in both the modern lifestyle and business models, which changes the way we connect with the physical world.
It attracts lots of people and hence users drastically enhance day by day. The end users of the online social network increase ultimately.
So that privacy issues increased in this site which leads to several legal issues. The millions of people are facing security issue, such as cyber-crimes, device hacked and so on.
The intention of this proposed project is to investigate risks in this social system and used to analyze the attack activity pattern in the social network. In this projects attack detection will be done.
And also attack prevention is done by this project. So that end user gets alter regarding his account which is available on social site. After getting alter user can take action regarding his attack. And also this project will help to block the attack. By using this project, the user can trust on social networking system if in case an attack occurs when the system can evaluate it and get alter to the user.
Keywords: cyber-crimes, security, attack.

I. INTRODUCTION

A social networking site is an online platform which people use to create social networks or use to build social relations with other people who share similar personal or career interests, activities, backgrounds or real-life connections. Web-based social networking services make it possible to build a connection with people who share interests and activities across political, economic, and geographic borders.
These social networks provide incredible opportunities and resources for online users, however, there is also a high risk for online security threats or attacks. The social network also makes cyber attackers easier to exploit vulnerabilities and it is being weaponized by the attackers. A cybersecurity attack can result in everything from identity theft, to extortion attempts, to the loss of important data like family photos. Cybersecurity refers to a set of techniques used to shelter the integrity of networks, programs, and data from attack, damage or unauthorized access.
Recently, with the research progress made in big data analysis, a number of research works have done on analysis of forensics in social networks. But then also users are facing security related issue.
This project will help to find the security-related issue which users are facing today. All the attacks like account hacking, malware, etc. Their causes can be detected and the user can get alter regarding his account. It is clear that a good model of user activity can be very helpful for analyzing the risks and security threats for the activity patterns in social networks.

II. EXISTING SYSTEM

In the existing system, there are no methods for detecting a fake user in the system. And also there is no method used for behavior tracking of any user. In case of an attack happened in the system. Then there is no alter generate for the user. For example, any person who is trying to hack the system, then after some attempt if that person behavior is suspicious then the system must have to generate alterations to the authorized user.

III. PROPOSED SYSTEM

The proposed system design Social Networking Site such as if any attacker attack on the Site then it can able to send alteration to the authorized user on his email or register mobile number. In this site, the not only attack can get detect but also it can prevent by the site.

A. System Architecture

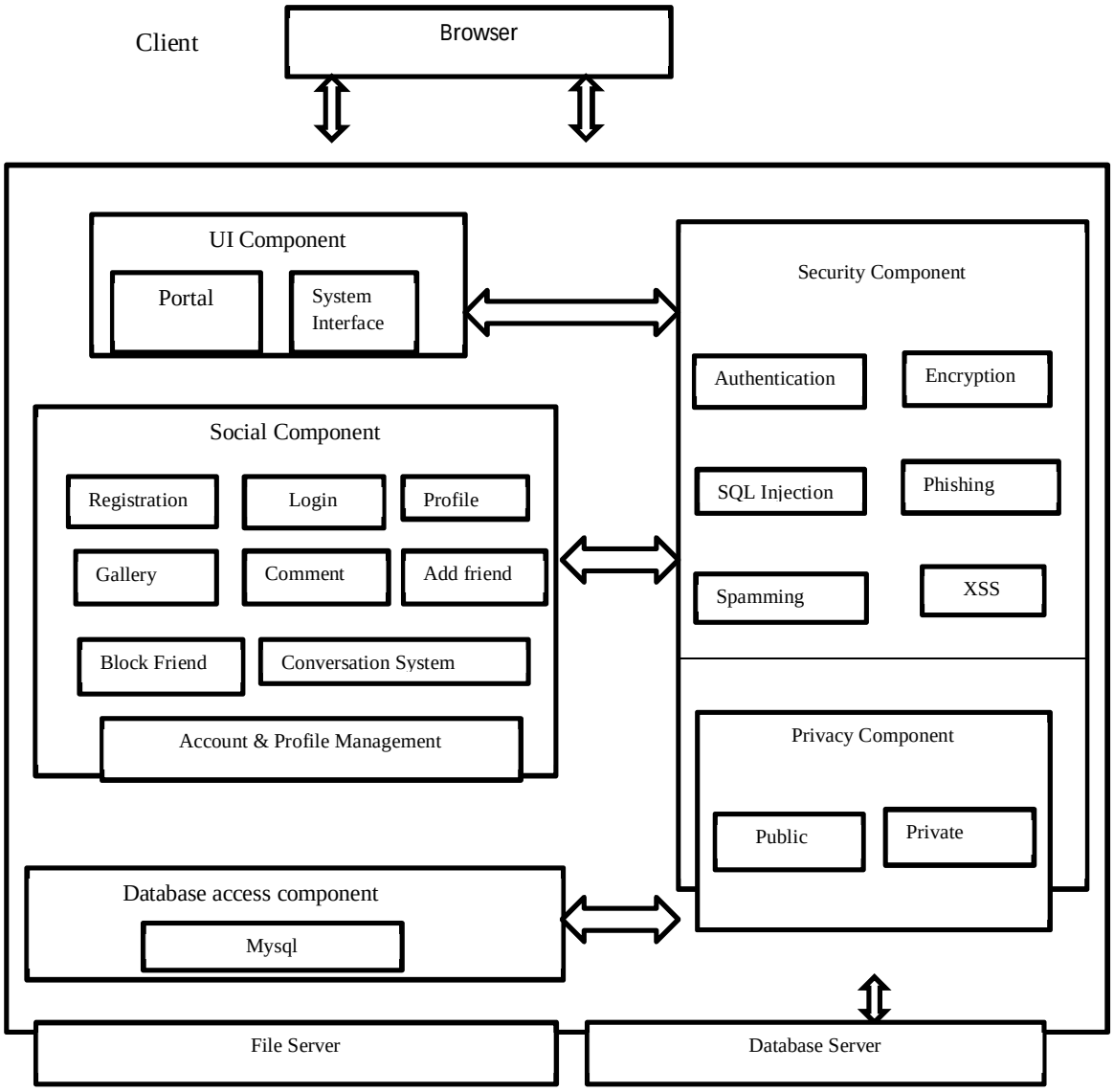

Fig. 3.1 System Architecture

B. Algorithm Used

In Online Social Networking Site three type of Algorithms are used:

1) Pattern Matching Algorithm
2) Artificial Neural Network
3) AES (Advanced Encryption Standards)
4) For document/content encryption and decryption

a) *Pattern Matching Algorithm:* In Online Social Networking site, If any suspicious activity happened then it can be easily tracked by this algorithm. Likewise:

i) Clicked Activities sequences will be checked with existing suspicious activity sequences tracked in the database using a pattern matching algorithm.

ii) If suspicious sequence found, the system will ask an auto-generated question to the user, if the user specified correct answer within 30 sec he will be considered as an authenticated user.

iii) Otherwise, attack detected and the account will be deactivated temporarily

b) Artificial Neural Network

i) In this project will develop Inner activity wise neural network to find out whether the activity is suspicious or not?

ii) For example, if an attacker trying to share a private document with any user, we will check whether the user is an authorized user to share the selected file using ANN.

iii) If there is no possibility that the file can be shared to the selected user, the activity can be considered as suspicious activity.

c) Advanced Encryption Standard: AES is depend on a design principle known as a substitution-permutation network and is efficient in both software and hardware. AES required fixed size block of 128 bits, and a key size of 128, 192, or 256 bits. By contrast, Rijndael per se is specified with block and key sizes that may be any multiple of 32 bits, with a minimum of 128 and a maximum of 256 bits. AES is used for uploading and downloading a document which user want to upload and download. Encryption and Decryption are used for it.

C. Attacks Detection and Prevention in Online Social Networking:

1) Behavior attack Detection Algorithm: In Online Social Networking Site, System will keep a track of following activities after login:

a) Login time span
b) Client machine from which the user made a login attempt
c) Performed social activities
d) The time period spent on every Social activity
e) Close friends detection
f) Content sharing pattern tracking

All the above activity will by track by the system so that if any suspicious activity observed then alteration will be sent to the user.

2) SQL injection Prevention Module

a) SQL injection attack is considered one of the web vulnerabilities threats directed to data-based applications.
b) To protect against SQL injection, the input data must not directly be embedded in SQL statements especially when the data comes from a user.
c) That problem is avoided entirely with prepared statements by making sure that the embedded query doesn't execute at the time of inserting the data and also validating and escaping the user's input data before sending it to the database.

3) Spamming Attack

a) Two types of security techniques are proposed as anti-spam registration security level. a) Email activation strategy for a new user account: this feature helps to prevent spammers from signing up to the system. After a user submits the registration form, an account activation module sends an activation link to that user’s email.
b) After the user successfully activated his account, he will be able to log in.

4) CSRF Prevention Module

a) CSRF attacks are exploitation of a particular web site in which the user sends vicious requests that the vulnerable web site will trust without the user’s knowledge.
b) For OSNs this attack can be used to publish posts, changing user's personal information including a profile picture, uploading pictures or any other activities that result in dishonoring user's reputation without the user's knowledge.
c) This module is responsible for preventing this attack by using a secure random token (e.g. CSRF token). CSRF token is a long random generated value which is difficult to guess. This value will be generated at the beginning of a user session and it will be correlated with this specific user’s session.
d) The token will be embedded in every request associated with sensitive server-side operations as a hidden field or inserted directly in Ajax requests. Then, the server will use that token to verify the validity of the user's request.

5) Brute Force Defense Module: Usually, when a website requires user authentication it will be a target of brute force attack. Hackers use this attack to gain unauthorized access to the user’s profile. So this attack can still be a dangerous threat to the online social network unless proper precautions are taken. Three strategies have been proposed as follows:

a) Enforcement Of A Strong Password Policy

i) This strategy used to defend against a targeted attack based on the fact that an attacker will use an automated tool that tries all possible combinations of letters, numbers and special characters.
ii) The length of the password must be at least 6 characters (the longer password, the more difficult to be broken by brute force). The password must include letters (uppercase and lowercase) and numbers.

b) Delay Strategy

i) The success rate of the brute force attack highly depends on time. The reasonable delay can greatly slow down the attack. The delay strategy was provided by the password hashing process. The applied hashing algorithm is based on a cost factor (delay factor) which is used to make the hashing process slower and it may take even seconds to produce the hash.

c) Enforcement Of A Strong Password Policy

i) This strategy used to defend against a targeted attack based on the fact that an attacker will use an automated tool that tries all possible combinations of letters, numbers and special characters.

ii) The length of the password must be at least 6 characters (the longer password, the more difficult to be broken by brute force). The password must include letters (uppercase and lowercase) and numbers.

IV. RESULT AND CONCLUSION

The result includes all those activities that take place to convert from the old system to the new. The old system consists of some different operations, which is operated in a very different manner from the proposed new system. Proper implementation is essential to provide a reliable system to meet the requirement of the organization.

As a result in online social networking site is an ongoing process and also the requirement of online social networking changes every day. Also, every architecture has been found to have with some of the limitations. It is a very challenging task for the service providers and researchers to fulfill all requirement of the user.

The result of the system will given below:

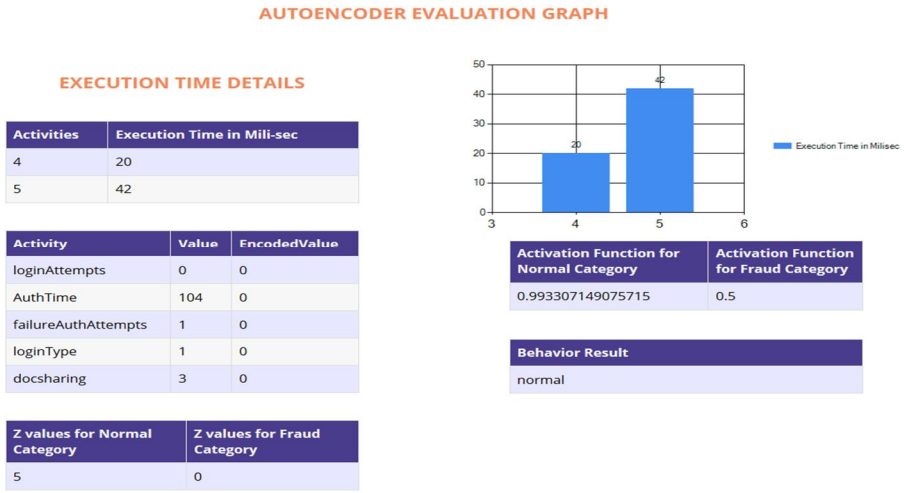

Fig. Screenshot of result.

REFERENCE

[1] P.Andriotis,G. Oikonomou, T. Tryfonas, and S. Li, “Highlighting relationships of a smartphone’s social ecosystem in potentially large investigations,” IEEE Trans. Cybern., vol. 46, no. 9, pp. 1974–1985, Sep. 2016.

[2] "Social networking goes global". Reston, VAR: comscore.com. 2007. Archived from the original on August 19, 2007. Retrieved September 9, 2007.

[3] Bruce Schneier; John Kelsey; Doug Whiting; David Wagner; Chris Hall; Niels Ferguson; Tadayoshi Kohno; et al. (May 2000). "The Twofish Team's Final Comments on AES Selection (http://www.schneier.com/papertwofishfinal.pdf)(PDF). Archived (https://web.archive.org/web/20100102041117/http://schneier.com/paper-twofishfinal. pdf) (PDF) from the original on 2010-01-02

[4] Daemen, Joan: Rijmen Vincent (March 9, 2003). “AES Proposal: Rijndael”) (http://csrc.nist.gov/archive/aes/rijndael/Rijndaelammended.pdf#page=1) (PDF). National Institute of Standards and Technology. p. 1. Archived (http://web.archive.org/web/20130305143117/http://csrc.nist.gov/archive/aes/rijndael/Rijndaelammended.pdf#page=1)(PDF) from the original on 5 March 2013. Retrieved 21 February 2013.