ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 2, Issue 4, April 2015

Sybil Identity Defender in Social Networks

Akshay Ambekar[1], Pravin Bhoi[2], Shekhar Gaikwad[3], Taksen Parvat[4]

B.E Final year student, Sinhgad Institute of Technology, Lonavala, Maharashtra, India[1,2,3]

Professor, Sinhgad Institute of Technology, Lonavala, Maharashtra, India[4]

Abstract: In today's world use of social networking sites are increased. Thus many users trying to create multiple bogus identities to compromise the running of the system. It is harmful to social network user. There are many methods available to solve bogus identity problem.

Sybil means multiple bogus identities in social network. Sybil attacks are one of the well-known and powerful attack against online social network. Sybil users propagate spam or unfairly increased the influence of target user. Here we propagate Sybil defender mechanism to prevent the Sybil user to enter in the social networking site.to test we design a basic Facebook module and apply this Sybil defender mechanism to check proper working of Sybil defender. Sybil Defender first detects the Sybil user and prevent user from login into system.

Keywords: Sybil, Sybil defender, Sybil attacks

I. INTRODUCTION

Today's special networking communities are open for every mankind, any user can join that system by providing their personal details. For example facebook, twitter, orkut etc. The user can access many other services/websites using facebook authentication. In such identity based systems, each user should have unique identity and user should use this unique identity when interacting with other users in the system. Because of bogus identities it is vulnerable to Sybil attack.

The situation where an attacker attacks on many user identities each called Sybil and join target system for various purpose like revenge, destroy private identities. For example social bots in online social network control hijacked or, adversary owned user accounts in order to infiltrates these network, steal private user data, spread misinformation and distribute malware. The social networking sites are vulnerable to Sybil attacks in which attacker creates multiple identities called Sybil identities and distributes the existing system and pollutes system with fake information. The Sybil identities in a variety of tasks, including the online contents ranking, DHT routing, file sharing, reputation system, and Byzantine failure defences. There are similar kind of attacks in ad-hoc and sensor network. The paper presents the fake identity defender. A fake identity defense mechanism that leverages the network topologies to defends against Sybil attacks in a social networks. Sybil defender can effectively authenticates the user identities and also check their activity which is Sybil or not. Also we provide the OPT for security purpose. For defending we used Stemming algorithm, conflation algorithm and encryption algorithm. Sybil attacks are well known and powerful attacks against online social networks. The users propagate spam or unfairly increases the influence of the target users. The previous works is on detecting Sybil users but in this paper we defended the Sybil users using various techniques.

II. LITERATURE SURVEY

Literature survey is the most important step in software development process. Before developing the tool it is necessary to determine the time factor, economy n company strength. Once these things are satisfied, then next steps are to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites. Before building the system the above consideration are taken into account for developing the proposed system. We are considering all the existing systems and protocols of Sybil Defender and using some the features to develop our system which will became good and secured example of online social networking system.

Table 1: Literature Survey

Reference Paper	Existing System	Mechanism used	Merits	Demerits
[1] SybilGuardDefending Against Sybil Attacks via Social Networks	Sybil Guard	To identify sybil nodes, the schemes make use of random routes and random walks.	Identify Sybil nodes.	Suffers from high false Negatives.
[2] SybilLimit: A Near-Optimal Social Network Defense Against Sybil Attacks YEAR 2010	Sybil Limit	A Near-Optimal Protocol.	Improved version of SybilGuard , SybilLimit limits the attack.	Fail to defend Sybil nodes
[3] SybilDefender: Defend Against Sybil Attacks in Large Social Networks	Sybil Defender	Observes the user activity and defend them if Sybil.	Restricts to create bogus identity.	Failure cases.

III.PRPOSED SYSTEM

Sybil Defender architecture is shown in following diagram. To understand working of the system you have to know what types of users in the system.

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 2, Issue 4, April 2015

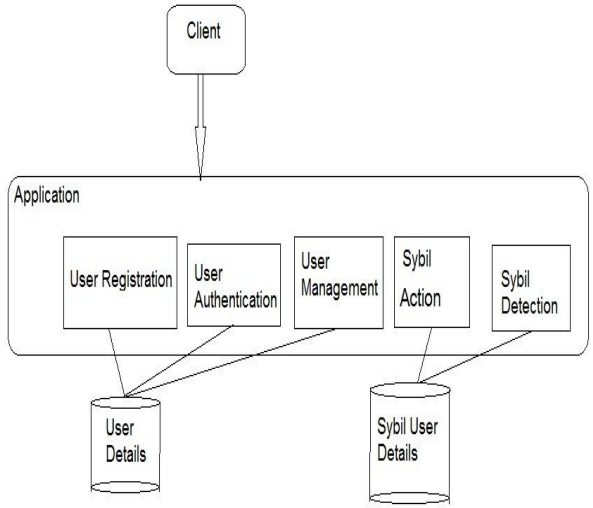

Fig 1: System Architecture

Above diagram shows the architecture of proposed system. We propose Sybil Defender, a centralized Sybil defence mechanism. It consists of different modules and also having different methods to defence from Sybil user. Above architecture shows that user need to register for the use of social network site and User Authentication module authenticate user if multiple identities is not present. Our scheme is based on the observation that a Sybil user's post which may publish in social network. After performing some detection methods on post then it will appear in social network. Hence there is no such activity which may harm to social networking site. User details and Sybil user's details stored in database and also their post details. Proposed system have some advantages like it is helpful to find Sybil users. Also it is used to find fake IDs. Also it is feasible to limit the number of attack edges in online social networks by relationship rating.

IV. IMPLEMENTATION

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

A. *Algorithms*

1) *Sybil Defender:*

This algorithm is used for the detection of the Sybil in the system. The application takes into consideration the user registration time, login time and the activities perform. The module also tracks the rate at which a particular user adds friends in the system along with their activities. If a system after considering all the factors considers that the user is a Sybil.

Sybil Defender consists of two components: a Sybil identification algorithm and Sybil defender. The task of the Sybil identification algorithm presented to determine whether a suspect node is Sybil or not.

2) *Steaming algorithm:*

Steaming algorithm is used to reduce inflected words from users post. According to dataset those word which is harmful are steamed. For that purpose steaming algorithm are used.

3) Encryption algorithm:

Encryption algorithm is used to hide information from Sybil users.

B. *Modules*

1) User registration.
2) Sybil Detection.
3) Admin Module.
4) Sybil Blocking.

1) *User Registration:*

A user created in system by taking in consideration by filling necessary data fields. User can enters in system by providing their personal detail. A user is authenticated by the system by generating an OTP and also comparing validating their provided information.

2) *Sybil Detection:*

This module is used for the detection of the fake identities in the system. The application takes into consideration the user registration time, login time and the activities perform by user. The module also tracks the rate at which a particular user adds friends in the system along with their activities. This module also checks the probability of the Sybil information post by particular user. Then the system automatically recognizes the fake identities and notifies to admin.

3) *Admin Module:*

The admin will have the right of viewing all the individuals and then taking the action of blocking an individual or a group after the system notifies them as the Sybil group. This can be done using the Sybil Blocking module.

4) *Sybil Blocking:*

This module is used by the admin for blocking an individual or a group, which the system considers as the Sybil group. The admin has the right of browsing the user page or the group before marking them as a Sybil group.

V. RELATED WORK

Many researchers investigated the coercion resistance in online Social networking site attacks. The proposed protocol in Sybil guard and Sybil limit also focus on providing security against to Sybil attacks and to find Sybil users. Our scheme is based on the observation that a Sybil user's post which may publish in social network. After performing some detection methods on post then it

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 2, Issue 4, April 2015

will appear in social network. Hence there are different modules to perform each task of detecting, defending. Algorithm that are used for the user's post and to detect each user's activity. Sybil guard and Sybil defender failed to defend Sybil user. Our module can defend Sybil user by observing their activity and post.

VI. CONCLUSION

In this paper we present Sybil defender system which makes the effective use of social network.
Sybil defender mechanism effectively detects the bogus identities and prevent them for accessing social sites. During registration system checks for multiple identities of new user. If detect then prevent them from registration. It also checks harmful post in the sites and take action against them. So Sybil defender mechanism effectively defend against Sybil attack.

VII . ACKNOLEDGEMENT

We are thankful to Prof. Mr. T. J. Parvat and Prof. Miss R. S. Shishupal for encouragement and the support they have extended to us for completing this review paper. For their support to make this paper analysis good as it is.

REFERENCES

[1] Wei Wei∗, Fengyuan Xu∗, Chiu C. Tan†, Qun Li∗, "SybilDefender: Defend Against Sybil Attacks in Large Social Networks", IEEE TRANSACTIONS ON KNOWLEDGE AND DATA MINING YEAR 2013.
[2] J. R. Douceur. The sybil attack. In *IPTPS*, 2002.
[3] H. Yu, P. B. Gibbons, M. Kaminsky, and F. Xiao. Sybillimit: A near-optimal social network defense against sybil attacks. In *IEEE* symposium on *Security and Privacy*, 2008.
[4] H. Yu, M. Kaminsky, P. B. Gibbons, and A. Flaxman. "Sybilguard: defending against sybil attacks via social networks. In *SIGCOMM*, 2006.
[5] A. Mislove, M. Marcon, K. P. Gummadi, P. Druschel, and B. Bhat-tarcharjee. Measurement and analysis of online social networks. In *ACM/USENIX IMC*, 2007.
[6] B. Viswanath, A. Post, K. P. Gummadi, and A. Mislove. An analysis of social based Sybil defenses. In *SIGCOMM*, 2010.
[7] C. Wilson, B. Boe, A. Sala, K. P. N. Puttaswamy, and B. Y. Zhao. User interactions in social networks and their implications. In *EuroSys*, 2009.
[8] K. Xing and X. Cheng. From time domain to space domain: Detecting replica attacks in mobile adhoc networks. In *IEEE INFOCOM*, 2010.
[9] RL. Bilge, T. Strufe, D. Balzarotti, and E. Kirda. All your contacts are belong to us: automated identity theft attacks on social networks. In WWW, 2009.
[10] M. Mitzenmacher and E. Upfal. *Probability and Computing. Cambridge University Press,2005.*

BIOGRAPHIES

Akshay Ambekar is student of BE in computer engineering from Sinhgad Institute of Technology, Lonavala, Pune affiliated to AICTE under Savitribai Phule Pune University and Completed HSC in Science in the year 2011 from D. P. Mehta Jr. college.

Pravin Bhoi is student of BE in computer engineering from Sinhgad Institute of Technology, Lonavala, Pune affiliated to AICTE under Savitribai Phule Pune University and Completed Diploma in computer engineering in the year 2012 from Dattakala polytechnic, bhigvan, in MSBTE.

Shekhar Gaikwad is student of BE in computer engineering from Sinhgad Institute of Technology, Lonavala, Pune affiliated to AICTE under Savitribai Phule Pune University and Completed Diploma in computer engineering in the year 2012 from Cusrow wadia institute of technology, pune in MSBTE.

Taksen J. Parvat, Associate professor, Department of CSE, sit, Lonavala.