IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016.

Two Way Security Mechanism for Sybil Attack in Social Network

Rucha Patil[1], Tejashree Wani[2], Gunjan Bonde[3], Chetana Chopde[4]

UG Students, Department of Computer Engineering, SSBT's College Of Engineering and Technology,

North Maharashtra University, Jalgaon, Maharashtra, India[1,2,3,4]

Abstract: From many years, people were concerned about the security of social area network. In this social area network people create multiple bogus identities. To overcome this drawback, Sybil Defender mechanism is used along with the two way security technique is use. The proposed system involve sybil identification technique along with the concept of the two way security mechanism .This two way security mechanism divide the password in two server and according to fake clustering , ip differentiation ,ip log technique is use to identify where the user is sybil or genuine user. Due to this we can easily identify the sybil user. Thus we conclude that the proposed system provide better security than the traditional one.

Keywords: sybil attack, Sybil Defender, ip log.

I. INTRODUCTION

Today's era, most of the system are vulnerable to sybil attack and there is increase in sybil attack in social network. There are various technique and concept to prevent this. Among the various algorithm and concept, the sybil identification algorithm plays a vital role. The scheme consist of:

1. Sybil node is identified by the sybil identification algorithm. This scheme is based on observation that whether the sybil node go through a small cut in the social graph to reach the honest region. People have failed to notice that, the sybil user can also attack using the user password. This will cause an efficiency in the existing system. Therefore to overcome this drawback, the concept of two way security mechanism is use in which the password is divided on two server .With the presence of one server ,the user is not able to login . Because of this, only the authenticated user can login into the system not the sybil user.

Motivation
The existing Sybil identification Scheme is prone to the sybil Attack, due to which the security of user not ensured.

The two way security can be ensured by dividing the a password on two server, Hence only the genuine user can login into the system.

Due to this, even if an sybil user tries to recover the password he will not be able to retrieve the password which is stored on two server. proposed system involves the sybil identification algorithm along with the two way security mechanism.

This two way security mechanism will enhances the security in large social network.

II. LITERATURE SURVEY

Literature survey plays vital role in the software development process. Different time factor, economic factor are taken into consideration.

The content of the paper focuses on the research and contributions of various sources. These include:

1) The paper describes the basic scheme and the attack to which it is prone. The different sybil attack are discuss .This paper propose the concept of sybil identification mechanism in which sybil user is identified .Due to this the attack is not able to prevent as it is not having mechanism to prevent the sybil user.
2) The paper discusses the describes the mechanism to identify the sybil node using the random walk technique. The advantage of this paper is that it will identify the sybil node but ,it suffers from high sybil attackers.
3) The paper discusses the describes the mechanism to observe the sybil user and identify the sybil user if present this will help to identify the malicious activity and bogus identities. Due to this bogus identity this mechanism also fails to prevent the sybil attack.

III. PROPOSED SYSTEM

The Sybil identification mechanism is solution to the sybil attack . The sybil attack can be prevented by introducing the concept of the two way security mechanism. Due to this , two way security mechanism the password is divided on two server .With the presence of one server ,the user is not able to login.

Because of this, only the authenticated user can login into the system not the sybil user.

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016.

Problem Definition
Secure social network is a necessity in today's era. Among the various mechanism, sybil identification algorithm is use. But using this also the sybil user can attack the node this create adverse affect on system . Therefore, to overcome this drawback, the concept the concept of two way security mechanism is use in which the password is divided on two server .With the presence of one server ,the user is not able to login. Because of this, only the authenticated user can login into the system.

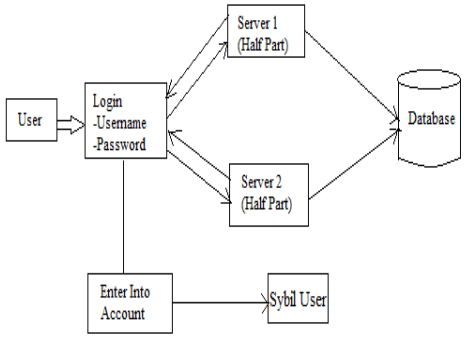

fig.1: Proposed System Architecture

In the past few years, online social networks grows increasingly. Previous techniques are applicable to small area network. O(log n) sybil nodes per attack edge, is identified by the sybil Guard mechanism. To overcome the weaknesses of previous work, the sybil identification mechanism along with two way security is evolved.

The proposed architecture include the mechanism as shown in fig.1.The user is login on the social network using username and password. The password is divided on two server half part is store on one server and another half part is on another server. When the user is login, the password from both servers is compared if they match then only user can login on the system otherwise not. The sybil user is identifies by using fake clustering, ip differentiation, ip log technique in sybil identification algorithm.

IV. IMPLEMENTATION

Implementation plays a vital role in the project development. At this stage ,the project is converted in to actual working system. Careful planning ,study of existing system also plays an important role in implementation phase.

Implementation of the proposed system involves the environment in which the system is implemented and the overall system development. The overall development of the proposed system requires suitable environment and proper resources for its successful completion. The proposed system is developed to prevent the sybil attack.

A. Algorithm:
1. Sybil identification :To identify the sybil user, sybil identification algorithm is use and also determine whether the suspected node is sybil or not.
2. Encryption algorithm: This encryption algorithm will encrypt the password and divide the password on two server to provide more security to user.

B. Modules:
1. User Registration: In user registration module, user is login in the system by filling the personal information. At this time the password is divided on two server to provide security.
2. Sybil Identification: This module is use to identify the sybil user and also checks the probability of the malicious activity. By observing this , the sybil user is identified and it notified admin that the user is sybil or genuine.
3. Admin module: Admin will have an authority to check an individuals user whether he is sybil or genuine user.

Propose system consist of following test cases. By considering this test cases we come to know whether the user is sybil(s) or Genuine(G) and where the test is Pass(P) or Fail(F) .

Table1: Test cases for Propose system

Test Case ID	Test Case Name	Test Case Description	Step	Test Data	Expected Result	Actual Result	Test Result (S/G) (P/F)
1	Enter Password	Divide Password into two server	Divide Password into two server	Password in Number Eg.123456	Successfully store on two server and encrypted	Divide Successfully	P
2			Divide Password into two server	Password in string of character Eg. abcdef	Divide string into two server and encrypted	Divide and encrypted successfully	P
3	Successfully login	Successfully login without any error	Successfully match encrypted password	Encrypted string containing password	Successfully login by client	Successfully login by client	P
4	IP differentiation	Check whether input belongs to same network	Match IP configuration	Eg. 192.168.--.--	successfully match	successfully match	G
5	Culture Fake request	Check request	Request either accepted or deny	Request should be accepted	Maximum request should be accepted	Maximum request may be deny	S

V. RESULTS

Sybil Attackers Result:
Millions of node is involve in this system, However sybil user have power to launch the sybil attack. The number of malicious node is created by sybil user to prevent this we improve the probability that user node will accept more honest node not sybil node. As the user is login on the system the password in the form of number, string, special character or a combination of these is encrypted and divided on two server.

Table2: Result of encrypted password on one server.

username	password
user10@gmail.com	JWA9aYa7dc=
user11@gmail.com	JWA9aYa7dc=
user12@gmail.com	c7zmlyXT7pY=
user15@gmail.com	JWA9aYa7dc=
user13@gmail.com	JWA9aYa7dc=
user14@gmail.com	JWA9aYa7dc=
user16@gmail.com	JWA9aYa7dc=

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016.

The cluster for fake friend is determine by the formula total friend request send is divided by total confirm request using this we can determine whether the user is sybil or genuine. The proposed system provides better reliability, integrity and security as compared to the existing system.

VI. CONCLUSION

Security plays an important role in large social area network .In Existing system social area network people create multiple bogus identities. To overcome this drawback, Sybil Defender mechanism is used along with the two way security mechanism is use. The proposed system consist of sybil identification technique along with the concept of the two way security mechanism .This two way security mechanism divide the password in two server and according to fake clustering ,ip differentiation ,ip log technique is use to identify where the user is sybil or genuine user. The system can be further extended for the secure One more layer of password authentication to Secured a Communication in the cloud computing.

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]. W.Wei, F. Xu, C. C. Tan, and Q. Li, "Sybildefender: Defend against sybil attacks in large social networks," in IEEE INFOCOM, 2012.
[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]. L. Xu, S. Chainan, H. Takizawa, and H. Kobayashi, "Resisting sybil attack by social network and network clustering," in SAINT, 2010.
[6]. G. Danezis and P. Mit, "Sybilinfer: Detecting sybil nodes using social networks," in NDSS, 2009.
[7]. W.Wei, F. Xu, C. C. Tan, and Q. Li, "Sybildefender: Defend against sybil attacks in large social networks," in IEEE INFOCOM, 2012.