Journal of Industrial Information Technology and Application *ISSN(Online): 2586-0852*
Vol.7 No.2

Social media IDS against fake accounts using Vicinity based Languages

Dr.B.Harichandana[1)], Dr.Abdul Subhahan Shaik[2)] and T. Murali Krishna[3,*)]
[1)]Dept. Computer Science Engineering, Srinivasava Ramanujan Institute of Technology, Anantapuramu, B.K. Samudram Mandal, Andhra Pradesh ,India.
[2)]Dept. of Computer Science Engineering, Avanthi Institute of Engineering & Technology, Hyderabad, Andhra Pradesh, India.
[3)]Dept. of Computer Science Engineering, Ashoka Women's Engineering College, Kurnool, Andhra Pradesh, India.

Abstract. The substantial growth of social computing in recent years has created the need for a development of novel theories and methodologies to address the human behavior and social relations. Social Networking Sites are increasingly gaining its importance in various domains such as academics, research and development. Apart these strengths of Social Networking Sites, it has one major disadvantage which is inefficient authentication of user login because single user can have Multiple Identity within the same group. Due to which various types of fake message, personal or national threats, non-social activities, vulgar and harassing figures and videos etc. are posted by some imposters or nonsocial personals. To defeat this attack we propose an authentication scheme using vicinity languages. The implication of fake account's will be prohibited and prevent from fraud and forgery of user's identity. Our analysis is validated through a Simulator. It relies on social graph properties for authentication and authorization in social network sites. Social simulator is computationally efficient and can scale to graphs with hundreds of millions of nodes as users.

General Terms. Social network, Face book, Enhanced authentication scheme, identification

Keywords. Social network sites, fake accounts, unique identity, authentication, authorization

---

[*] Corresponding author: Murali2007tel@gmail.com
Received: Feb 15, 2023; Accepted: Apr 10, 2023; Published: Jun 30, 2023

1. Introduction

Social networks are web-based services that allow individuals to construct a public or semi-public profile within a bounded system, it articulates a list of other users with whom they share a connection and traverse their list of connections and those made by others within the system. The substantial growth of social computing in recent years has created the need for a development of novel theories and methodologies to address the human behavior and social relations [1]. The social computing enables online communication through user content contribution and provides the new data patterns based on the human behaviors and characteristics, such as age, race, relationship and language [2]. A social network is a social structure that is made up of nodes representing individuals or organizations. These nodes may be tied to each other by properties such as friendship, common values, visions, ideas, business relationships and general interests.

The nature and nomenclature of these connections may vary from site to site. While Social Network has implemented a wide variety of technical features, their backbone consists of visible profiles that display an articulated list of Friends who are also users of the system.

The public display of connections is a crucial component of Social Networks. Although the idea of social networks has been around for a long time [3], social networking web sites and services are a relatively new phenomenon on the Internet. Social networking sites such as Face book [4] Myspace have been gaining popularity among Internet users. According to a recent statistical analysis, Face book has more than 1 billion active subscribers worldwide and Google+ has more than 250 million active users [5]. The Friends list contains links to each Friend's profile, enabling viewers to traverse the network graph by clicking through the Friends lists. So in a social network sites authentication and authorization is a major challenge in creating a trusted account.

These Online Social Networks are the network spaces where the individuals are allowed to share their thoughts, ideas and creativity, and also to form social communities. These online networks provide significant advantages both to the individuals and in business sectors. The success of an SNS depends on the number of users it attracts; there is pressure on Social Network Service providers to encourage design and behavior which increase the number of users and their connections. However, the authentication and the authorization mechanisms of Social Network Services are relatively weak by design as the security and privacy are not considered as the first priority in the development of Social Network Services.

2. Contribution

This paper presents a methodology which can protect online social services users from various security and privacy threats. More specifically, this paper offers the following contributions: First, we outline the Social Network service threats that target every user of social networks. Second, we propose an authentication scheme. The Proposed method is to avoid duplicate identity using edge cost value. Third, this is done using Authorization, Authentication. Where Authorization is preceded by Authentication. Authorization checks for valid user by accessing their unique user id and restricts the access when the user tries with another id. Finally, the value reflects on to the edge on each and every mobile nodes as shown in simulated approach which is easy-to-implement the recommendations on how Social Network users can better protect their security and privacy when using social networks.

3. Organization

The organized work of our paper is as follows: In Section 4, we describe the threats in social network services. Next, in Section 5, we discuss about the authentication and authorization of the system. In section 6 the network formation model is described. In Section 7, the simulation results with authenticated nodes and authorization nodes by using social simulator. In Section 8, we offer future research directions. Our conclusions are presented in Section 9.

4. Identity Threats

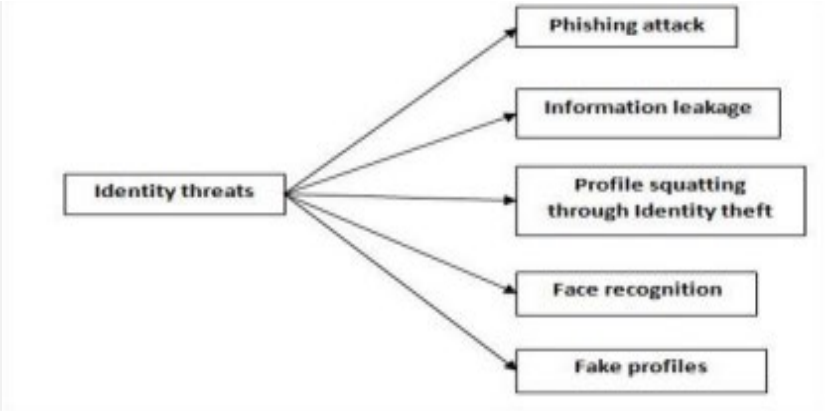

Figure 1. Various identity threats

4.1 Phishing

A phisher can easily and effectively exploit the information available on social network to increase the success rate of a phishing attack. For instance, the email phishing attacks can be achieved 72% hit rate by using the information available in the social network [6]. SNSs are also vulnerable to social engineering techniques which exploit low entry thresholds to trust networks and to scripting attacks which allow the automated injection of phishing links. Phishing can reveal the sensitive information, such as passwords and credit card or bank account numbers and cause financial and reputation damage.

4.2 Information Leakage

The privacy of online social networks is jeopardized since an adversary can easily become a friend of a member of any restricted group by dissembling his identity and then access to the private information that belongs to the members of only that group. Moreover, on many SNSs such as Myspace it is even possible to use scripts to invite friends. Some of the potential risks associated with this threat are: Leakage of Private information, Phishing for information and conducting spamming and marketing campaigns.

4.3 Through Identity theft

A malicious attacker can create a fake profile to impersonate a renowned person or a brand. Such profiles are usually created by the people who know the personal details of a user and create a profile to impersonate him or her and thereby causing all sorts of problems for the victim. Profile squatting can do a significant damage to the reputation of a person or any brand which may in turn lead to the financial and social embarrassment.

4.4 Face Recognition

Many people use Online Social Networks for uploading pictures of themselves and their friends. Millions and millions of photos are uploaded to Face book each day. Moreover, many Face book user profile pictures are publicly available to view and download. For instance, the Faces of Face book website allows Internet users to view the profile images of over 1.2 billion Face book users. These photos can be used to

create a biometric database, which can then be used to identify OSN users without their consent.

4.5 Fake Profiles

Fake profiles (also referred to as Sybil's or social bots) are automatic or semi-automatic profiles that mimic human behaviors in Social Network Services. In many cases, fake profiles can be used to harvest users‟ personal data from social networks. By initiating friend requests to other users in the OSN, who often accept the requests, the fake profiles can gather a user's private data which should be exposed only to the user's friends. Moreover, fake profiles can be used to initiate Sybil attacks [7], publish spam messages, or even manipulate OSN statistics [8].

By analyzing the different kinds of identity threats associated with the Social Network Sites, we have found the following major factors that might be considered as the root of all threats are because of Lack of appropriate authentication and access control mechanisms as well as other security related tools to handle different privacy and security issues of online social network.

5. Discussion

The recommended strategies for circumventing the threats associated with the online social networks are promoting stronger authentication and authorization. The strength of authentication and authorization method varies from one Social Network Services to another Social Network Services.

5.1 Authentication

Authentication is a process of determining whether a particular individual or a device should be allowed to access a system or an application or merely an object running in a device. This is an important process which assures the basic security goals, viz. confidentiality and integrity. Also, adequate authentication is the first line of defense for protecting any resource. Most of the existing authentication schemes require processing both at the client and the server end. Communication with external entities must be authentic, unmodified, and secret in some cases. Authentication is necessary so that the parties involved in a message exchange are mutually assured of the identity of whoever they are communicating with. Integrity is necessary to be assured that messages are not

altered in transit. Preventing anyone from knowing what data is being communicated is the realm of confidentiality. Thus, the acceptability of any authentication scheme greatly depends on its robustness against attacks as well as its resource requirement both at the client and at the server end. The resource requirement has become a major factor due to the proliferation of using social network sites.

5.2 Authorization:

Authorization is the function of specifying access rights to resources related to information security and computer security in general and to access control in particular. More formally, "to authorize" is to define an access policy. Access control also uses authentication to verify the identity of users. When a user tries to access a resource, the access control process checks that the consumer has been authorized to use that resource. Authorization is the responsibility of an authority.

In this paper, we specifically target on face book and propose a new and intelligent authentication scheme using a new simulator. However, our proposal can also be used in other do-mains where confidentiality and integrity are the major security requirements.

6. Network Formation Model

As stated, before the aim of our work is to provide trusted communication to end users when they are connected in social network services i.e. (face book). The model is based on connections between people create value, the value is distributed among the people involved in the connection and relationships have an associated cost which provides an authentication.

We define a simple method for assigning value to nodes, based around the idea that any connection between two nodes (no matter how distant) has a value of 1.

That value is divided evenly amongst all nodes that appear on some shortest path between the two nodes.

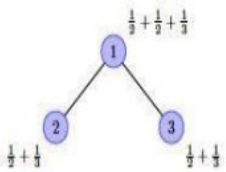

Figure 2. Assigning value to nodes on a very simple network.

From fig 2 there are three connected pairs: (1; 2), (1; 3), and (2; 3). There are unique shortest paths between all of these pairs: (1; 2) and (1; 3) have paths that use two nodes, and (1; 3) has a path that uses three nodes. In our system, value is split amongst all nodes that appear on some shortest path between a pair of nodes. So, each node on the (1; 2) and (1; 3) paths receive +1/2 value, as there are two nodes on each of those paths. Likewise, each node on the (1; 3) path receives +1/3 value. The total values for each node are shown in figure 2.

We analyze the behavior of this network on fixed-cost groups and simple hierarchical social structures to find that our model mostly fulfils the desired goals of authenticated connectivity, and the formation of cliques with sparse connections between them. Our network formation model is defined by a set of nodes, a value function, and a cost function.

A. Set of nodes

Nodes represent people. Pairs of nodes are given turns in sequence to decide whether or not there should be an edge between them. If there is already an edge between them, either node may drop it, but if there is no edge, both nodes must agree for it to be added.

B. Value function

Nodes experience value from their relationships with other nodes: a node gains value whenever it is on some shortest path between two nodes.

C. Cost function

Nodes incur a cost for every edge to which they are incident. We refer to the value that a node gains from its relationships minus the cost of its edges as that node‟s utility. Nodes are partitioned into subsets called clusters. Clusters represent divisions amongst people being modelled; there is always one “global” cluster that includes everyone; this ensures that every node is in at least one cluster with every other node.

$$(i) + \Sigma$$
$$(n) \qquad (1)$$
$$= \Sigma$$
$$(j) + \cdots\cdots. + \Sigma$$

From (1) determines the total number of cluster in the network, (i,j…n) is the cluster i,j,..n which varies from 1 to i+1, 1 to j+1 and 1 to n+1

We define a simple method for assigning value to nodes, based around the idea that any connection between two nodes (no matter how distant) has a value of 1. That value

is divided evenly amongst all nodes that appear on some shortest path between the two nodes.

The function for the utility of any node in terms of a function ,

(i) (2)

= ∑

From (2) „i‟ is the node which varies from 1 to n, number of nodes in the cluster

= ∑ (3)

From (3) is the utility function and is the cost function

= - (4)

From (4) is the value gained from all connections it is involved in, and is the cost it incurs. The value function is made up of the value derived from having a connection to other nodes and the value from being a node on a path between other nodes.

On any path, the intermediate node receives the same value from that path as the nodes actually being connected

In standard value function, for every path between any two nodes the contribution to is the inverse of the number of nodes on all shortest paths between those two nodes.

If, { } disconnect „a‟ and „b‟ (5)

From (5) we conclude to disconnect the nodes if it would be beneficial to either „a‟ or „b‟ If, { connect „a‟ and „b‟ (6)

From (6) we conclude to connect the nodes if it would be beneficial to both „a‟ and „b‟ _____

Algorithm: Running one step

_____

input: a social network N

foreach distinct pair of nodes (a, b) in N do

the utility of a // u(a)

the utility of b // u(b)

if an edge exists between a and b

then // disconnect the nodes if it would be beneficial to

either a and b

the utility that a would have

if the a-b edge were removed

the utility that b would have if

the a-b edge were removed

disconnect a and b if > or >

else // connect the nodes if it would be beneficial to both a

and b

the utility that a would

have if an a-b edge were added

the utility that b would

have if an a-b edge were added

connect a and b if > and >

end

Since nodes have well-defined utility functions, it is possible to allow the nodes of the network to connect each other where they will add and drop edges in order to increase their utility. We are considering each node to act independently as an agent for classic best response dynamics seems to violate the idea that relationships are mutual: how can one person unilaterally create a friendship? Our work around is to model relationships as a sequential relation where, on its turn, each pair of nodes decides whether or not there should be an edge between them. The algorithm for running a step (a unit in which every pair takes its turn once) is given above.

7. Simulation Results

The simulation platform used in our project is Social network simulator. We define and implement that attempts to mimic the formation of realistic social networks. There is always one “global” cluster that includes everyone; this ensures that every node is in at least one cluster with every other node.

Because all connections in our model have value, a node should always gain value by making a connection to someone you were not previously connected to. So, unless the cost of having edges within a cluster is set so high that nobody is able to afford one,

then edges should form in the cluster such that all nodes are somehow connected to all other nodes .

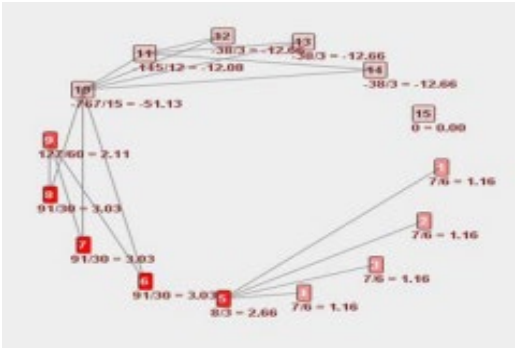

Figure 3. Cluster formation and connections of nodes in each cluster

```
F:\my project ME\code>java -jar socialsim.jar sample2.txt
total no. of nodes = 15
no. of clusters = 3
1       <u=7/6> -> 5
2       <u=7/6> -> 5
3       <u=7/6> -> 5
4       <u=7/6> -> 5
5       <u=8/3> -> 4 3 2 1
6       <u=91/30> -> 9 10
7       <u=91/30> -> 9 10
8       <u=91/30> -> 9 10
9       <u=127/60> -> 6 8 7
10      <u=767/15> -> 14 6 8 7 11 13 12
11      <u=145/12> -> 14 10 13 12
12      <u=38/3> -> 11 10
13      <u=38/3> -> 11 10
14      <u=38/3> -> 11 10
15      <u=0> -> <no edges>
-------------------------------
```

Figure 4. Utility values of the network with cluster formation

From fig: 3 initially we have considered 15 nodes in the network. Node1 to Node5 are considered as cluster1, from Node6 to Node10 as cluster2 and from Node11 to Node15 cluster3. Node10 is connected to Node6, 7, 8 in cluster2 likewise in cluster3 node11 is connected to Nodes12, 13, 14. Considering the network model with fixed edge cost value

1/3. The graph which is considered in the network is undirected graph. From fig:4 the utility value is determined. The utility value from the network depends upon the edge cost value and number of nodes in the network. As the utility value of each node increases the connection of nodes also increases and this result in high edge cost value. The edge cost value in the network and the value in the network decide whether there must be connection between the nodes in the network.

When node 10 is linked with node11 the Node12, 13, 14 which are connected with Node11 is automatically connected to Node10. These mimic that in face book how friends are tagged in their account. Thus node1 to node15 from fig:4 all nodes are

authenticated nodes. The color in the node it determines about the clusters. Thus this graph shows how the authenticated users are connected in a network as a group. The highest the value functions results in the node is authorized node in the cluster. Where from the result authenticated nodes only can create an edge (i.e.) link between them. From a node single link is created multiple links are dropped. So this results in prohibiting fake accounts in social network services.

8. Future Research Direction

The present work is discussed only with validating 15 nodes as users and the algorithm we used only forms 3 clusters in the network. The network formation model we used is the standard model with a fixed edge cost value corresponding to the nodes present in every cluster. As in future we can validate the network by increasing the nodes. As the nodes increases the cluster formation also increases. The edge cost value can also be used dynamic.

9. Conclusion

The authentication scheme proposed in our paper provides a security for users to access social network site (face book) in a trusted manner where the user has an account constraint to access. A single user is provided with only one authenticated identity to log into their account this method is to avoid all identity threats. This was done using Authorization (cluster head node in the network) and Authentication (node). In simulator, the Value reflects on to the edge/link on each and every mobile node as shown in simulated approach. Here only one link is created between multiple nodes likewise in social network site (face book) single user is provided with a single identity, fake identities and other threats are prohibited and the result is proved through social network simulator.

References

[1] Shu, Kai, et al. "Fakenewsnet: A data repository with news content, social context, and spatiotemporal information for studying fake news on social media." Big data 8.3 (2020): 171-188.

[2] Nosouhi, Mohammad Reza, et al. "Blockchain for secure location verification." Journal of Parallel and Distributed Computing 136 (2020): 40-51.

[3] Pourghomi, Pardis, Milan Dordevic, and Fadi Safieddine. "Facebook fake profile identification: technical and ethical considerations." International Journal of Pervasive Computing and Communications (2020). [4] Chouchani, Nadia, and Mourad Abed. "Online social network analysis: detection of communities of interest." Journal of Intelligent Information Systems 54.1 (2020): 5-21.

[5] Li, Na, and Sajal K. Das. "Efficiently discovering users connectivity with local information in online social networks." Online Social Networks and Media 16 (2020): 100062.

[6] Zhang, Zhiyong, et al. "A crowdsourcing method for online social networks security assessment based on human-centric computing." Human-centric Computing and Information Sciences 10.1 (2020): 1-19. [7] Zhang, Zhijie, Rui Hou, and Jin Yang. "Detection of social network spam based on improved extreme learning machine." IEEE Access 8 (2020): 112003-112014.

[8] Sundararaj, Vinu, and M. R. Rejeesh. "A detailed behavioral analysis on consumer and customer changing behavior with respect to social networking sites." Journal of Retailing and Consumer Services 58 (2021): 102190.

[9] Gilles, Robert P. "Building social networks under consent: A survey." Game Theory and Networks. Springer, Singapore, 2021. 203-258.

[10] Jiang, Ge. "Social Coordination and Network Formation in Bipartite Networks." The BE Journal of Theoretical Economics 21.1 (2021): 239-268.

[11] ALSaleem, Bandar Omar, and Abdullah I. Alshoshan. "Multi-Factor Authentication to Systems Login." 2021 National Computing Colleges Conference (NCCC). IEEE, 2021.