International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.8, Issue.4, Apr 2020 E-ISSN: 2347-2693

Asymmetric Social Proximity Based Community Structured Online Social Network

P. Gowrishetty[1*], A. Gopi[2]

[1,2] Department of Computer Science and Engineering, Mahatma Gandhi Institute of Technology, Hyderabad, India.

[*]*Corresponding Author: praharshgowrishetty@gmail.com, Tel.: +91-9550024024*

DOI: https://doi.org/10.26438/ijcse/v8i4.115 | Available online at: www.ijcseonline.org

Received: 2/Apr/2020 Accepted: 23/Apr/2020, Published: 30/Apr/2020

***Abstract*—** The extensive growth of Online Social Networks (OSNs) over the last decade has changed the way people interact with their friends, family and especially making new friends. These social networks have been an important integral part of our life. Since the count of the users of social networks is increasing drastically, so is the security threat and also private information threat. For making new friends, some OSNs work on the principle of similar profile attributes to let people become friends. However, this principle involves a privacy threat of exposing private and personal profile information to strangers over the internet. The existing solutions to secure users' privacy are by finding the intersection of the private set of profile attributes of both the users. These schemes have few flaws and cannot hide users' privacy. Also, in today's online social networks any random stranger can send a friend request, check your information and misuse it too. In this paper, the community structures are used to represent the online social networks and asymmetric social proximity measure is used as people consider friendships differently. Because of social closeness measure, friend suggestions and requests originate only from relevant communities. Then, based on the asymmetric social proximity measure, a privacy algorithm is used, which provides a high level of privacy and can protect users' privacy better than the existing works. This concept is designed using Advanced Encryption Standard Algorithm with the exchange of keys. When there is an exchange of Public and Private keys then only information can be accessed. In this paper, a secured online social network system is designed and developed as a Web application to protect the sensitive data and private information of the users and increase the security and privacy issue for OSNs. This OSN is effective and has high-level privacy protection.

***Keywords*—**Asymmetric Social Proximity, Community Structure, Online Social Network

I. INTRODUCTION

Over the past decade, there has been a tremendous growth of Online Social Networks and Mobile Social Networks. In modern society, there has been a fascination of 'connectedness' among the people by these OSNs and MSNs. Many OSNs have been developed over the years where users a significant amount of their time using these OSNs. OSNs have changed the style of interactions with the existing friends and has paved a new way to create new friends. People make new friends by exploring their interests, mutual friends, education history, career and professional interests, etc. Some of the widely used OSNs worldwide are Facebook, WhatsApp, WeChat, Instagram, Tumblr, Twitter, etc.

Generally, OSN stores all the user's data in its server and then find friends with similar profile and suggests them[1],[3],[4],[5]. The server knows the entire information and if the server gets compromised or if there is any data breach then all the users' privacy is at a stake. There have also been several incidents of a data breach in the past and these incidents create a big flaw for the OSNs. Moreover, the users may not access the servers every time. Therefore, there have been growing interests towards secured distributed solutions to find friends[3]. So many distributed ideas related to social proximity between the users have been proposed[1]. The common way of profile matching is finding out similarities between two people like if their common friends, interests, location, educational history, careers, social coordinates etc.

Even after employing various cryptographic tools to ensure privacy security, there have been issues because of malicious users where such a user gets to know the entire information[6]. Two people can indeed become friends if they have similar profile attributes, but it is not the only way to make friends[2]. For example, a lawyer's best friend may not necessarily be a lawyer but also a doctor who may share very less similar profile attributes. On the contrary, two people may be good friends even with having any common profile attributes. Therefore, it can be inferred that two people can become friends not only based on their common attributes but also if their friends have something in common. It is as simple as a friend's friend can be a friend too.

In this paper, community structures or group structures are used to represent the social network model[1]. And

asymmetric social closeness measure is used as friendship is weighed differently by different people Here, it is considered that each user at least belongs to a single community and these communities can tell a lot about the user[2]. There can be many communities like class, school, department, university, sports, movies, music, certain professions, etc. and a user can be affiliated to any number of such communities. Also, friendships in real life are valued differently. The friendship bond is considered to be asymmetric because a person may be your friend but you may not that person's friend[1]. Hence, asymmetric social proximity is proposed between the users according to the user's perceptions. The world these days has shifted to asymmetric friendship relations. For example, Facebook follows symmetric friend relation and several flaws were observed and to avoid such flaws the today's social networks like Instagram, Snapchat follow the asymmetric friend relations.

The OSN is defined based on this asymmetric social proximity measure between the users considering the perceptions of both the users on the common communities. This can better capture the property of making friends in an OSN. Then, based on the asymmetric social proximity measure, a privacy protocol is used, which provides high-level security. Previously, a malicious user A can become a friend with another user B, A can access the information of B and misuse. In this paper, the malicious user A cannot access and know any personal information of user B apart from his community unless he is a friend of user B. Only when B accepts the friend request of A, then only A can view B's profile information. This concept is designed using Advanced Encryption Standard Algorithm with the exchange of keys. When there is an exchange of Public and Private keys then only information can be accessed. This OSN is effective and has high-level privacy protection[6],[7].

The remainder of this paper is organized as follows. In Section II, the problem statement is discussed. In Section III, the existing and proposed system is mentioned. The Literature Survey is depicted in Section IV. The System Architecture is mentioned in Section V and Flowchart showing the workflow is shown in Section VI. In Section VII, the results are shown. The paper is concluded in Section VIII and future scope is mentioned in Section IX of the paper.

II. PROBLEM STATEMENT

In today's world of social networks, the profile matching involves an innate privacy risk of exposing private profile information to strangers over the internet. This personal information can be misused in many ways. There are few existing solutions to protect user's privacy but they have some limitations. Also, in the existing online social networks, any random stranger can send a request, check your profile information and misuse it too. So, this paper aims to protect the user's privacy and also to restrict friend suggestions and friend requests based on similar communities by asymmetric social proximity measure[1].

III. EXISTING SYSTEM AND PROPOSED SYSTEM

In the OSNs, the symmetric concept of friendship is frequently used i.e the OSN considers friendship as an equally weighed relationship. The most common way of determining friendship between two people is by measuring the similarities between two people. When two people have many common interests, such people are suggested as friends in the OSNs[2]. Also, there is no protection of information and all the private information can be misused by any malicious users[5]. Once when the username is entered, the entire information about a user is displayed in today's OSNs.

In this paper, community structures are used to represent a social network[1]. The community structures are redefined as a society comprising of different groups University, entertainment, art, music, sports, class, etc. In this paper, the concept asymmetric social proximity is used as in the real-world scenarios, friendship is weighed differently by different people. A person may consider another person as his friend but that another person might not feel the same. So, here this concept of asymmetric social proximity is used to measure the similarity between two people and suggest friends to them. In this Social Network, high emphasis is laid on privacy and security. This paper uses the AES Algorithm for encryption and decryption of data. A user will initially not be able to see any of the personal information of another user until he or she accepts his friend request[5]. This process of friend request is done by sharing of Public and Private keys and hence this makes the system more secured and prevents misuse of data by malicious users[6].

IV. LITERATURE SURVEY

Table 1: Literature Survey of the Asymmetric Social Proximity Based Community Structured Online Social Network

S.No.	Year	Name of Author	Title of Paper	Technique	Advantages	Disadvantages
[1]	2013	H.Zhu, S.Du, M.Li, and Z.Gao	Fairness-aware and privacy-preserving friend matching protocol in mobile social networks	Privacy preserving friend discovery in mobile social networks.	Secured friend discovery process as a generalized privacy preserving interest and profile matching problem.	The proposed protocol is less efficient.
[2]	2012	X.Liang, M.Barua, R.Lu, X.Lin, and X.Shen	Health Share: Achieving Secure and Privacy-preserving Health Information Sharing through Health Social Networks	Attribute oriented authentication and transmission schemes.	Attribute oriented authentication makes it secured.	Flaws in profile suggestions and profile matching.
[3]	2011	W.Dong, V.Dave, L.Qiu, and Y.Zhang	Secure Friend Discovery in Mobile Social Networks	Co-ordinated based proximity estimation.	Secured proximity estimation, provides both privacy and verifiability.	Security threat in multi-party computations.
[4]	2009	J.Camenisch, M.Kohlweiss, A.Rial, and C.Sheedy	Blind and anonymous identity-based encryption and authorized private Searches on public-key encrypted data	PEOKS scheme to build a public key encrypted database	Blind identity-based encryption, public key encryption with a keyword search.	The database having public keys can be accessed by unauthorized personnel.
[5]	2008	C.Hazay and Y.Lindell	Efficient Protocols for Set Intersection and Pattern Matching with Security against Malicious and Covert Adversaries	Secure set intersection, Secure Pattern Matching, Relaxed notions of security	Use of secured pseudo random function evaluation to achieve secure pattern matching	A malicious adversary can cheat.

V. SYSTEM ARCHITECTURE

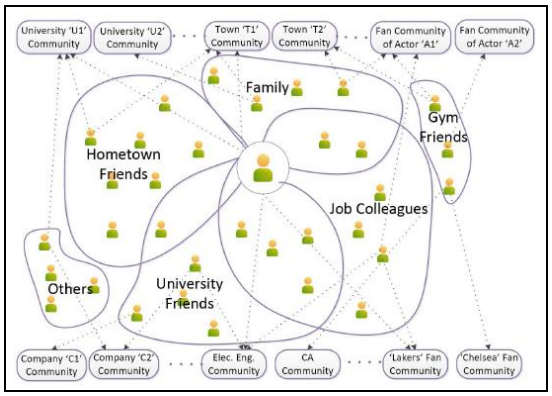

Figure 1: Architecture of the System

The background idea behind the paper is a community structure which is represented as a social network as shown in the above figure 1. The community structures are redefined to appear as a social network and people within the same community's form friends. The social proximity measure is the number of common profile attributes, mutual friends and common interests of people. The proximity measure increases as the overlap between two users' profile attributes or common friend spaces grow. So, as the proximity measure increases the better the friend suggestions work. Here, in this paper, society is divided into communities. There can be various communities like Hometown friends, Job colleagues, university friends, gym friends, family, etc. Based on intracommunity users, we get friend suggestions. The more communities a user exists, the proximity measure of user increases.

VI. FLOWCHART DESCRIBING THE WORKFLOW

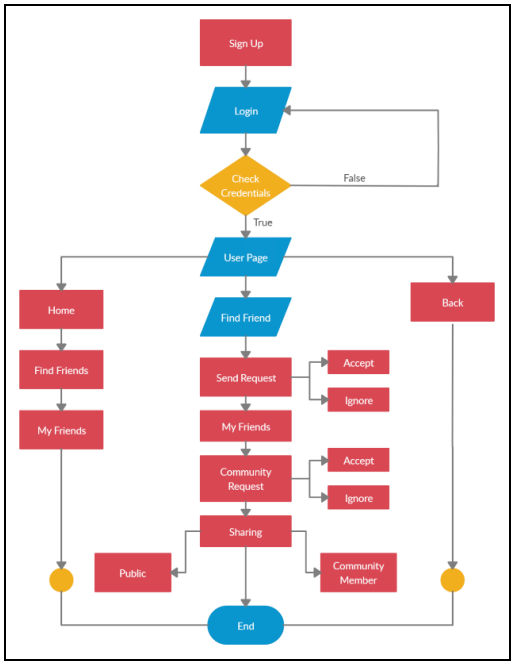

Figure 2: Flowchart depicting the working

In the above figure 2, initially, a new user has to sign up for using the social network. Once when he creates an account with his credentials, the user can log in to the OSN. An existing user can log in with his existing credentials. Then, the credentials are checked and if an account exists, then the OSN page opens. In the OSN there will mainly be three tabs namely Home, Find friends and Community.

A user can make new friends by sending them friend requests. The person can accept or reject the friend request. Similarly, a user can join any of the communities. A user has to send a request to the community groups to join a community and then the existing people of community users can accept or ignore the join request. A user can also share his views by posting messages. While posting a status, a person can choose various privacy measures like post accessibility to all members, accessibility to only specific community members, etc. Once when the user is done with the work, he can log out of the OSN.

VII. RESULTS

Figure 3: Home Page

In the above figure 3, when the web application is launched, the home page appears where there is information about the OSN. The above page is a home page which acts as an index for the entire application. It has linked pages such as User Login and New User Registration pages. The picture adjacent to the information is the architecture diagram which is the backbone of the entire paper.

The below figure 4, shows the registration page for new users. In order to join the online social network, he has to sign up. A new user can register here in the application. The details of the user such as user's name, user id or the username, password, email id, date of birth, community and gender have to be filled here and submitted in order to create an online social network account.

Figure 4: Registration Page for new user

In the below figure 5, shows the login page for existing users. An existing user can log in into this application with his credentials i.e user id and password. If the credentials of the user are correct when matched with the ones in the database then the web page navigates to the User's Home Page. If the user's credentials are found to be wrong or if there's any mismatch then an error alert is displayed.

Figure 5: User Login Page

The below figure 6, shows the user's home page which is navigated when the credentials of the user are matched. This page has several features such as the user can add friends, view requests, view friends, view his profile, create a new community, join into exiting communities, share thoughts and see the posts by his friends and community members.

The user can create a new community by entering the name of the community. He/ she can join into an existing community or communities by viewing them in the drop-down box and then clicking the join button. The user can share his thoughts with other users of the OSN. The user can type his thoughts in the text area and then choose privacy settings for the post. There are several privacy options for every single post. The user can select the post privacy option as public which means the post can be viewed by all the users of the OSN. Or else the user can restrict the post to be viewed within a single community by selecting the respective community in the drop-down box.

Also, in this page, a user can view the Community and public timeline i.e he/she can read the posts put by their friends and community members. Every post or status is indicated by the name of the person who posted it, the timestamp of the status and also the private life of the status i.e the visibility of the post among the OSN users.

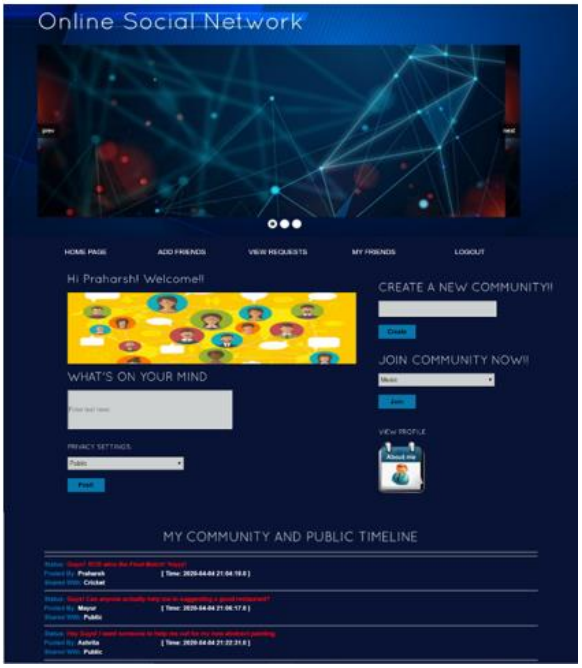

Figure 6: User's Home Page

In the below figure 7, shows the User's Profile Information. When the user clicks on About me in the home page, this web app is navigated to this page. This page contains all the private information about the user such as mail id, age, gender, community list, friend list, etc.

Figure 7: Profile Information of User

In the below figure 8, the detailed list of the requests sent is shown. This page appears when the user clicks on the View Requests tab. All the friend requests sent to the user and also all the community requests sent are shown on this web page. The user can accept or ignore the friend and community requests.

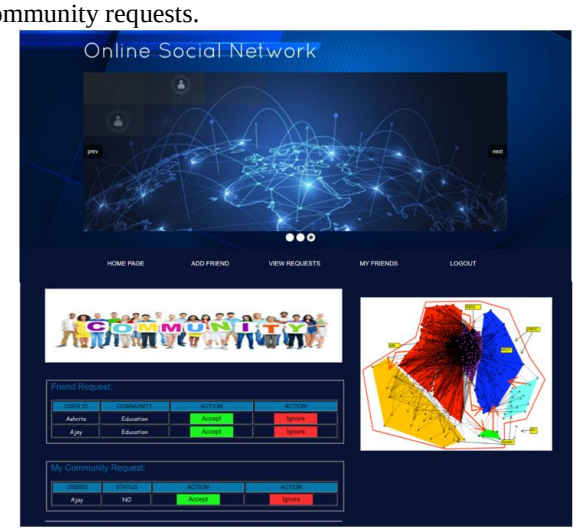

Figure 8: View Friend and Community Requests

In the below figure 9, the lists of the user's friends and also community members are displayed. Since the paper works on the concept of asymmetric social proximity, consider the above example where Ashrita is a friend of Praharsh but not vice versa. So, the friendship ties are viewed as a one-way link.

Figure 9: List of friends and Community Members

The below figure 10, shows the list of available friends whom you can become friends. These friend suggestions are based on the concept of similar communities. So, the friends of a similar community are suggested here as friends. The more the number of similar communities, the better will the friend suggestion work.

Figure 10: Add Friends

The below figure 11, shows the profile information of another user in OSN. When the user clicks on the username of another user and since they both are not friends the personal information of the user is encrypted. AES algorithm is used in this paper to encrypt and decrypt all the details of a user to ensure high privacy making the system secured.

Figure 11: Profile Information of a User in the OSN

In the below figure 12, the page pops out when the user sends a friend request to another person. When the user sends the friend request, he shares his key to another user to prove his authenticity. This message goes to another user who received a friend request.

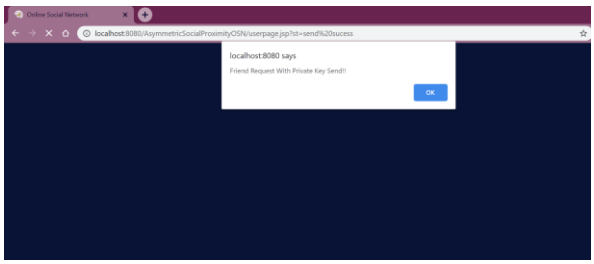

Figure 12: Friend Request Sent

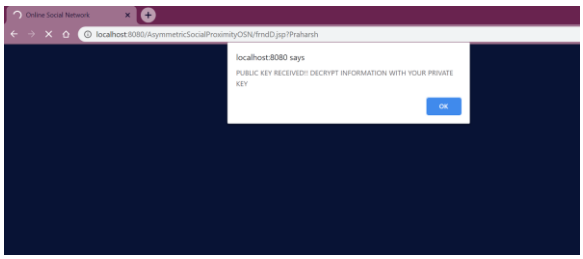

Figure 13: Friend Requested Accepted

In the above figure 13, the page pops out once after another user accepts the friend request. So, once when another user accepts the request, he can view the profile by clicking ok and then the user's profile is displayed.

Figure 14: Profile Information of Friend

In the above figure 14, the web page is displayed when the user accepts the friend request. The entire information is decrypted and the profile information of the user is decrypted. All his information which was previously encrypted can be seen now. The user's name, user id, mail id, date of birth, gender, date of joining and community and friend list can be seen.

VIII. CONCLUSION

The OSNs have paved a new way to interact with the currently existing friends and also to make new friends anywhere all over the world. The existing OSNs have led to privacy breaches and had many security flaws. Making friends and preserving privacy is an important aspect and a challenging problem. In this paper, the community structures are used to find asymmetric social proximity measure and also a cryptographic protocol has been used to ensure privacy between two users by protecting the private information. Also, the friendship relations have been valued as an asymmetric relation in this OSN.

Hence, this OSN is very effective and has high-level privacy protection and would be very efficient for users to use.

IX. FUTURE SCOPE

This paper can be further improvised by working on the security furthermore. Based on the asymmetric social proximity measure, an improvised private matching protocol can be designed in such a way that there can be accurate friend suggestions. Also, despite AES being a powerful cryptographic algorithm, it has few drawbacks which can be overcome by developing a higher secured protocol to increase the security. One breakthrough in this paper can be encryption of data in the database. The user's data present in the servers can be made encrypted and which can be accessed only by the user with the help of a private key. This encryption of data can prevent data breaches and minimise data misuse. Moreover, this can be made into a real-time OSN by using real social network data and be tested.

REFERENCES

[1] Arun Thapa, Ming Li, Sergio Salinas and Pan Li, "*Asymmetric Social Proximity Based Private Matching Protocols for Online Social Networks*", IEEE Transactions on Parallel and Distributed Systems.

[2] David Easley and Jon Kleinberg, "*Networks, Crowds, and Markets: Reasoning About a Highly Connected World"*.

[3] H. Zhu, S. Du, M. Li, and Z. Gao, "*Fairness-aware and privacy-preserving friend matching protocol in mobile social networks*", IEEE Transactions on emerging topics in Computing.

[4] X. Liang, M. Barua, R. Lu, X. Lin, and X. Shen, "*Health Share: Achieving Secure and Privacy-preserving Health Information Sharing through Health Social Networks*", Computer Communications, Elsevier.

[5] W. Dong, V. Dave, L. Qiu, and Y. Zhang, "*Secure Friend Discovery in Mobile Social Networks*", IEEE International Conference on Computer Communications.

[6] J. Camenisch, M. Kohlweiss, A. Rial, and C. Sheedy, "*Blind and anonymous identity-based encryption and authorised private Searches on public-key encrypted data*", International Workshop on Public Key Cryptography.

[7] C. Hazay and Y. Lindell, "*Efficient Protocols for Set Intersection and Pattern Matching with Security against Malicious and Covert Adversaries*", International Association for Cryptographic Research.

Authors Profile

Mr Praharsh Gowrishetty is pursuing his Bachelor of Technology in Computer Science and Engineering from Mahatma Gandhi Institute of Technology, Hyderabad. He has worked as an intern for several companies and has developed projects in the fields of Web Technologies, IoT, Java, Cloud Computing, etc. His areas of interests in research include Business Analytics, Data Mining, Data Analytics and Web Technologies.

Mr Arepalli Gopi is an Assistant Professor in the Department of Computer Science and Engineering at Mahatma Gandhi Institute of Technology, Hyderabad. He has work experience of over 3 years. He was involved in many projects and has published several national and international journals.

