International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-3, February 2019

Privacy and Security Model for Online Social Network (OSN) Friend Recommendation

Asif Ali Khan, M. Sridevi

Abstract - Today, online social network (OSN) is one of the widely used online communication platform. The technology innovation made easy access to this communication platform for each and every one. This platform generates an enormous amount of data each and every day. It includes personal information of the user. The one question arises how safe is the user data. The OSN providers stores critical information in decentralized locations where the data is being distributed between several numbers of servers and so the information is in the hands of whoever owns the server. This makes the data vulnerable to hacking or data theft. The user has little control over how their data being used. The OSN primary source of revenue is through the commercialization and monetization of the data. The OSN analysis the data to add or update their services according to the user interest. The OSN is all about socializing through communicating, sharing and making friends virtually. OSN providers are rapidly adopting the recommendation system into their applications to improvise friend recommendation. The paper briefly explains how trust calculation and homomorphic encryption are used to achieve security and privacy of the data in OSN.

Keywords: security, privacy, online social network, friend recommendation

I. INTRODUCTION

With advancement in the world of technology each and every day new things are added to the list. Not everything is perfect and it has one or another way it got some limitations. Here we are talking about the popular online social network which has made our virtually social life successful. New things are added to the online social network (OSN) each and every day. Lots of data is being exchanged among the millions of users every day. Some of the famous OSN's are LinkedIn, Facebook and Twitter. In a way, OSN is merging into our real life. Companies are creating contents by mining the latest trends on Facebook and Twitter. Law enforcement agencies are extracting the evidence to solve the crime cases [1], political parties are using OSN as platform to promote their works and gaining the popularity to win the upcoming elections [2][3], business organizations with the help of digital marketing they are focusing onto promote their products and services by creating social campaigns and the employers are using the popular OSN Facebook ,Twitter to analysis the social activity ,LinkedIn to analysis the professional activity of the candidates [4].

Lots of data is processed each and every day and the data consists of multiple things like posts, images, and videos etc. These data are received each and every day and the users can obtain or see this received data anytime. But because of the huge amount of data, the OSN has faced some issues like information overloading.

In a recent scandal a researcher in the pretext of research, given the popular OSN millions of user data to an analytic company. This analytic company used the data in favor to deploy individualized engagement and targeted ads for political agenda. Today OSN's in the name of free service they are gathering the data of users. The users are somehow aware of this fact but they do not know that how little privacy they have over the internet. And the user does not know the data was being used for this purpose without their knowledge. This leads to the user data privacy at high risk. This event caused the dilemma unrest among the users as it has caused the personal data of the user in the hands of some third party unauthorized organization.

The online social voting is a great feature in the OSN but some of the unknown entities are involved in such kinds of event where there is a greater risk of losing the data and it is out of control of anyone to handle it within the limits.

On the OSN most of the things are visible to the public and in most of the cases, the user is not aware of it. Here the problem is the user is not well aware of the security and privacy issues. And the user not educated about the policies of the service network providers. They simply tick on the terms and conditions documents without even having a look into it. If the user is aware of the security and privacy issues then it might not affect his/her privacy and security of the user.

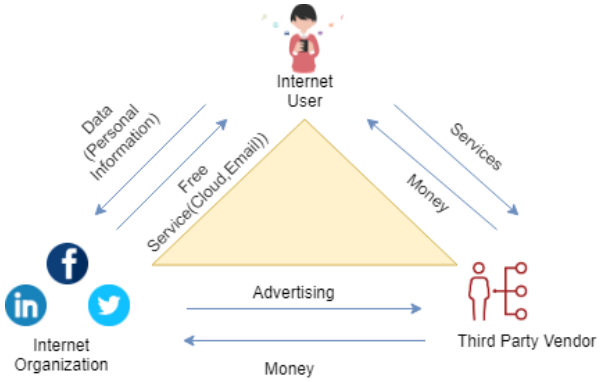

Figure 1. OSN Business Model

Manuscript published on 28 February 2019.
* Correspondence Author (s)
Asif Ali Khan, M.Tech, Dept. Computer Science and Engineering, Anurag Group of Institutions, Hyderabad, Telangana, India
M. Sridevi, Assoc. Prof, Dept. Computer Science and Engineering, Anurag Group of Institutions, Hyderabad, Telangana India

Online social network (OSN's) is all about the people interactivity and the social activities on the online platform. A huge people are attracted to this thing and they join social networks. People are the main entity which adds value to the social community [5].But the OSN contains good and bad entities which tend to have good or malicious intentions. The users are the first line of defence for their profile data. But due to lack of knowledge the user became the weak link in the online social network. Some of the actions of users like accepting the request from unknown contacts. sharing personal information over the profile make them vulnerable inside the weak spot. OSN has some inbuilt setting for the privacy controls but those are limited which are not helpful to maintain the confidentiality of the user because it is dependent on the trust of other users and also the user character.

II. RELATED WORK

In [6] the basic idea of the proposed system is to improve wise the accuracy of the friend recommendation without compromising the privacy of the user interest. The authors in [6] have proposed "privacy-preserving protocol" which enhances the precision and authenticity of friend recommendation.

They had proposed a model where the target user sends a request to the central authority which is a third party trusted provider. The CA takes the request of the user and by using the tag model it matches the tag id with the similar tag id users by using the similarity threshold. The suggestion is carried forward from the CA to the target user accordingly and finally, the user sends the request to the desired suggested friends.

In [7] the authors describe how the existing system data has been decentralized and how the risk revolves around the data of the user over the decentralized system. In the decentralised system the data is being stored in different locations (in some cases outside the country also}and the OSN use the third party providers to store their data. So there is no centralized data storage where the data is kept safe. So due to this decentralisation of the data there is a risk of data stolen which eventually leads to the concern of the privacy of the data.

The authors [7] proposed a system in which they proposed there own encryption and decryption method to maintain the secrecy and privacy of the data. In that system, only a single encryption operation is done on each file. The unique idea of the author is to prevent the changing or updating of the group keys whenever a user or a member has left or joined the group at any time.

In their model, the researchers assign a unique key to each new user of the group. The user is verified to gain access to the encrypted data (document or files) by using the unique key. To decrypt the data the user has to prove their identity. Here the decryption is done by combining the ID key, User ID and the group key. If the user wants to upload the document the same thing is repeated for the encryption.

In [8] the author has proposed a social network where the profile matching of the users takes place with the combination of username and his or her phone number. In this way, the only users who have the details of the particular user like his name or phone number can send message or request or communicate with the target user. The author has used the cryptography method which maintains the privacy of each individual and even the server does not know who the user is communicating.

Few Features of this model are:

1. Users of the social network can find new contact anonymously
2. Users of the social network can add or delete new contact anonymously
3. Users of the social network can communicate with each other anonymously

The paper [9] the author used the various cryptographic methods to improve the privacy control of the existing SNS (Social Network Service) model. The model works like in this pattern Key generation: Encryption: Storage: Request: Evaluation: Response: Decryption. The author analyzed the privacy control setting on the present SNS. The paper also gives the evidence how the modern cryptographic methods can improve the security of the SNS by enhancing the privacy.

In [10] the authors have proposed a system which works on the time-based calendar system. The OSN has different types of accounts like personal, private and public accounts. In the system the user decides what to share and with whom to share according to the schedule. So due to this factory, the information shared among the user is safe within the trusted users. So the personal information of the user is not shared and the information received from the other user can be trusted and this leads to the no loss of privacy.

S.No	Title	Problem Discussed	Method Used	Advantages	Disadvantages
1.	An Efficient Privacy-Preserving Friend Recommendation Scheme for Social Network," in IEEE Access, vol. 6, pp. 56018-56028, 2018	Privacy-preserving protocol which enhances the precision and authenticity of friend recommendation. The proposed model process is are as follows: similarity threshold – tag matching- ca verification- final candidate.	Tag matching based on preserving protocol, similarity degree threshold.	Improvement in the privacy of the user and it is maintained throughout the user profile.	Performance issue, the high computation cost.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

2.	Privacy Preserving and Information Sharing in Decentralized Online Social Network," (ICICCT), Coimbatore, 2018, pp. 152-155.	The data of online social network present in the decentralized location is not secured and chances of losing data which leads compromise security and privacy of data. The proposed model is to minimize the risk of leakage of data by using encryption methods.	Encryption and decryption algorithm.	Secure information sharing between the group users.	Maintaining and safeguarding encryption keys (lose of keys means loss of data associated with it).
3.	Privacy Preserving Profile Matching for Social Networks," 2018 Sixth International Conference on Advanced CBD, Lanzhou, China, 2018, pp. 263-268.doi: 10.1109/CBD.2018.0005	Preserving the privacy of user by using encryption method for profile matching if target user anonymously.	Attribute based encryption.	Maintain anonymity.	Limited to attribute like phone number and name.
4.	A Hybrid Privacy Protection Scheme in Cyber-Physical Social Networks," in IEEE Transactions on Computational Social Systems, vol. 5, no. 3, pp. 773-784, Sept. 2018.	Privacy in existing SNS are not effective and system eliminates the use of the private key to be used on encrypted data.	Homomorphic encryption schemes.	Improved privacy compared to present SNS privacy control methods. , data can be exchanged without a private key.	A lot of computing resource is needed to perform the cryptographic techniques.
5.	Social Networking Without Sacrificing Privacy," 2018 International Conference on System Science and Engineering (ICSSE), New Taipei, 2018, pp. 1-6.doi: 10.1109/ICSSE.2018.8520188	Confidentiality of the data on the social media without violating the privacy of the user. The proposed system works on the authorization approach where the user decides with whom the data is shared.	Social calendar system.	Individual custom authorization approach confidentiality.	Time based system will have to be consistent for different category of users.

III. EXISTING SYSTEM

The present working system has four important entities:

1. User
2. OSN provider
3. Third party vendor
4. Advertisers

The user is the key component. The user is responsible for the creation of the data over the networked application. The user stores his/her data and you can say give their private information to so-called trusted OSN provider. But the user does not have the awareness of how their data is being handled. In the present system, the user opens the account by providing some basic information about themselves. The user can update or delete the information from their profile anytime and for providing their information they are offered or you can say they are eligible to the user the OSN services. They aren't aware of what their private information is used for.

Basically, the user uses a browser to connect to the OSN application over the internet. The user can access his /her profile by using the credentials provided to them for authorization over the secured network. The application is accessed through the graphical user interface by the user and it is responsible for connecting the user to avail the OSN services.

OSN providers are the people who the programmed the web application for the user interactivity socially over a virtual network. In other words, the OSN provider is people who created a piece of a web application to obtain the information of the user and sell them to the advertisers. They are the one who maintains or take responsibility to store the user data securely. They consistently work to improve their services and to add more features to the service.

One of the trending new features in OSN is the recommended systems. By using recommendation system method they are analyzing the large chunk of user data. And according to the requirement of the advertisers, this system is directly targeting the correlated user who has a similar interest of the advertiser and recommends the things accordingly.The OSN providers are just the people who make the code to make a superior application to connect people across the globe. And the other things like running the application on the server which is used by an enormous amount of people where the traffic is more are maintained by third-party vendors. It is not limited to utilizing the server.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

The OSN provider utilizes the storage facility to store an enormous amount of the data from the third party vendor. The third party vendor makes the job of OSN provider much easier by maintaining the storage and running of the application without any interruption. And these vendors store data in different part of location over the globe. They are highly interested in user data and extend the OSN services.

OSN's are highly dependent on the advertisers for the capital to run there OSN networked application. The more the user uses the service, the more advertisers approach the OSN provider. More advertisers mean more money. This is how the business model of OSN works. They directly target the user which has the matching similarity interests which are mentioned in the targeted strategies provided by the advertisers and the OSN provider includes those advertise in there OSN service.

So finally, the user is the only entity who is affected by the whole system. The private confidential data of the user is at risk. The user data is getting sold in the black market like hot cakes. Recommended system, decentralization, involvement of third party providers is directly or indirectly affecting the privacy of the user in one or the other way. The next emerging technologies like artificial intelligence and machine learning which is wholly dependent on a large amount of data by processing the user usage pattern and all.

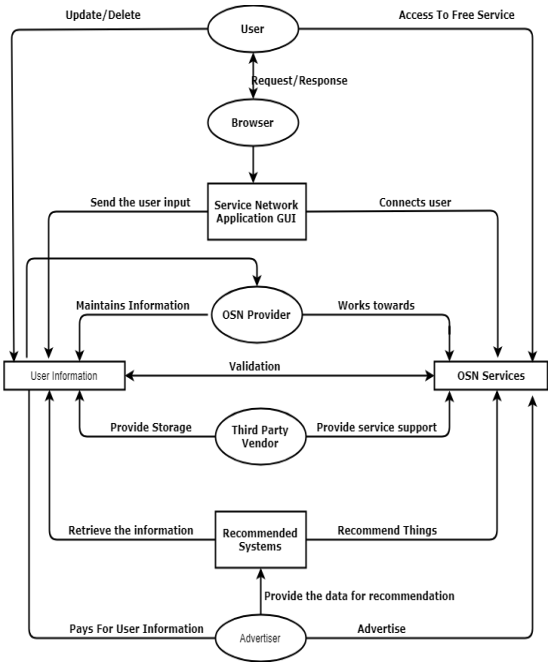

Figure 2. Architecture of Existing System

IV. PROPOSED SYSTEM

In our proposed model we propose an online social network model which uses a collaborative filtering approach with trust calculation and encryption added as an advantage over the model to keep the data of the user safe. By considering some of the concept from previous research [8][11][12] and integrating with some new methodologies, we have proposed a new system model.

In this model after the user is registered successfully each user will get unique user id which is a combination of their first name and email id and the OSN will also provide a unique key to each user respectively. Then the system uses filtering methods and trust based calculation to recommend friends to the user. And the sending of data in between the user and OSN is protected by the homomorphic encryption. The working model is illustrated in fig 3.

The model consists of :

1. Users
   a) New Users: Participants willing to join the OSN.
   b) Existing Users: Users who are already part of the OSN.
2. Modules
   a) User Panel: This module consists of a login and user friend list.
   b) User Management: This will have the following contents:
      i. Registration
      ii. Generate User Id
      iii. Login
      iv. Search topics
      v. Potential friend recommendation
      vi. Send friend request
      vii. Approve friend request
      viii. Remove friends from list
      ix. View friend list
      x. Send Documents
      xi. View documents
      xii. Data access permission
      xiii. Identify and decrypt data (Document/Message)
3. Encryption
4. Decryption
5. Key generator

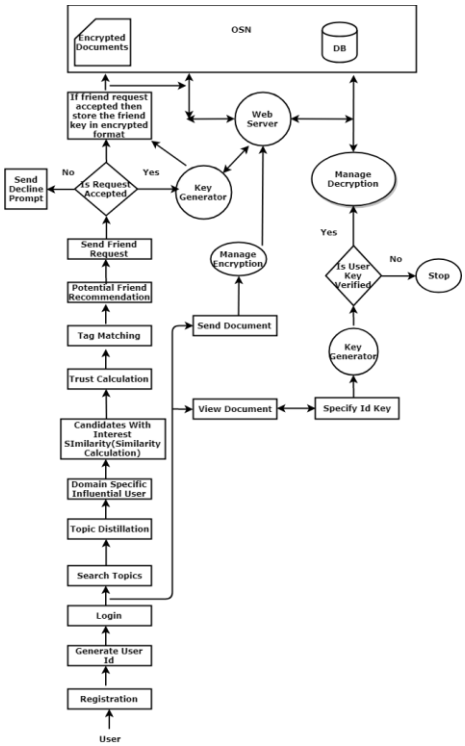

Figure 3. Architecture of Proposed System

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

In fig 3. The architecture of the proposed system is described. In figure 3, the bottom part is the registration block, where the user registers itself to the OSN to avail the services. The OSN is decentralized so the data storage is not localized.

After the registration of the user. A unique user ID is generated. By using the method used in [8], where the user ID is generated using the first name and mail ID of the user.

Next is the login block in fig 3. where the user logs into their account, where they can manage their friend list. If the user is new then they are redirected to page where there is a list of topics. Further, the user can search for topics of their interest such as a collection of music, arts, games etc.

Moving over to the next step the friend recommendation kicks in. In [11] the authors have briefly explained the accurate prediction for friend recommendation. It can be achieved by following these steps:

1. Subject Filtration
2. Domain-specific users
3. Users with an equal interest
4. Friend recommendation

Interest degree and the impact of followers are taken into consideration to perform the mining of top- k influential candidates based on latent topic.

Candidates with similar interest are defined with higher probability values are identified by the dominant interest calculation of the target user.

Finally, the friend recommendation is done by combining the interest similarity and social interaction of the user.

Finally, the trust calculation [12] is done on the basis of the singular value decomposition collaborative filtering approach. The trust between the u1 and u2 are calculated on the basis of specific date 'd' as :

trust(u1 ,u2 ,d) = w1(u1)a1(u1,d)C(u1 ,u2 ,d) + w2 (u1)a2(u1,d)L(u1 ,u2 ,d) + w3 (u1)a3(u1,d)S(u1 ,u2 ,d) + w4(u1)a4(u1,u2)N(u1 ,u2)

Note:

C(u1 ,u2 ,d) : Number of commands by u1 and u2 entries
L(u1 ,u2 ,d) : Number of lines
S(u1 ,u2 ,d) : Number of shares
N(u1 ,u2) : Represents common friends
a1 , a2 ,a3 ,a4 : Auxiliary values
w1 , w2 ,w3 ,w4 :Weight factors

This trust calculation is mostly based on user-based collaborative filtering recommended system. It is based on analysis of user and the targeted user calls, messages, contacts etc. so as to make an effective recommendation.

In figure 3. the send friend request block allows the user to send the friend request from the suggested list. Afterward, if the request is not accepted the user is notified by the decline prompt. If the request is accepted then the key is generated by combing the u1 , u2 and OSN public key and it is stored in the database in encrypted format.

Now, whenever the user logs into his account if they wanted to send the document to other friend/user then before sending the document it is being encrypted. And if the participant wanted to view the received file then the user has to specify their ID.

By using their ID the unique key is generated. And after that, it is being verified from the database DB whether they match or not. If the key is not verified or said to be invalid then the system denies the particular user to access it. If it is verified then the document is decrypted and the user is able to view the document.

The encryption and decryption system works on the homomorphic encryption principles [13][14] is being used in our proposed system. The operation of the homomorphic encryption are as follows:

1. The user u_1 of the social network system generate the private key and public key.
2. The user u_1 encrypts the data with the public key and sent the encrypted data and the public key to the SNS (Social network system) server.
3. The public key and encrypted data are stored in the SNS decentralized database.
4. The user u_1 sends the request to the SNS server to perform the operation.
5. The server takes the request and processes the request and performs the operation which is requested by the user.
6. The server responds to the user u_1 request by sending the encrypted result.
7. Then the user decrypts the data by using its private key.

V. CONCLUSION

As the semiconductors and the network devices are getting affordable day by day in the coming years the OSN will be more adopted by many people and it will be one of the most utilized networks application over the internet. Each and every day large chunks of data is being generated by this applications. In the pretext of free services, the OSN providers take the advantage of this and they sell the user private data to the third parties.The user needs to be aware and get educated how things work over the internet. Countries and the organizations should introduce new policies and enforce security measure which is better than the approaches which are implemented today. In the paper, we have proposed a model which will make user data which is present in the decentralized locations much secure compared to traditional OSN. And the data communication is also secured by means of using encryption and decryption method. We have used collaborative filtering technology as an approach to improve friend recommendation by combing the interest similarity and social interaction of the user which will have a high success rate and less time complexity. Finally, in future, the model can be verified on the large-scale OSN for performance and complexity.

REFERENCES

1. H. Kelly, Police embrace social media as crime-fighting tool, 2012, URL: http: //www.cnn.com/2012/08/30/tech/social-media/fighting-crime-social-media.
2. G. Lotan, E. Graeff, M. Ananny, D. Gaffney, I. Pearce, et al., The arab spring — the revolutions were tweeted: Information flows during the 2011 tunisian and egyptian revolutions, Int. J. Commun. 5 (2011) 31.
3. P. Jha, Facebook users could swing the results in 160 Lok Sabha constituencies, 2013, URL: http://www.thehindu.com/news/national/facebook-users-could-swing-the-results-in-160-lok-sabha-constituencies/ article4607060.ece.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

4. E. Protalinski, 56% of employers check applicants' Facebook, LinkedIn, Twitter, 2012, URL:http://www.zdnet.com/article/56-of-employers-check-applicants-facebook-linkedin-twitter/.
5. Security and Privacy in Online Social Networks Cutillo, Leucio Antonio; Manulis, Mark;Strufe, Thorsten Book chapter in "*Handbook of Social Network, Technologies and Applications*", Part 4, Springer, October 2010, ISBN: 978-1-4419-7141-8
6. H. Cheng, M. Qian, Q. Li, Y. Zhou and T. Chen, "An Efficient Privacy-Preserving Friend Recommendation Scheme for Social Network," *in IEEE Access*, vol. 6, pp. 56018-56028,2018. doi: 10.1109/ACCESS.2018.2872494
7. N. V. Ghodpage and R. V. Mante, "Privacy Preserving and Information Sharing in Decentralized Online Social Network," 2018 *Second International Conference on Inventive Communication and Computational Technologies (ICICCT)*, Coimbatore, 2018, pp. 152-155. doi: 10.1109/ICICCT.2018.8473268
8. T. Guo, K. Dong, L. Wang, M. Yang and J. Luo, "Privacy Preserving Profile Matching for Social Networks," 2018 *Sixth International Conference on Advanced Cloud and Big Data (CBD)*, Lanzhou, China, 2018, pp. 263-268.doi: 10.1109/CBD.2018.0005 URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8530850&isnumber=8530796
9. Y. Qu, S. Yu, L. Gao, W. Zhou and S. Peng, "A Hybrid Privacy Protection Scheme in Cyber-Physical Social Networks," in *IEEE Transactions on Computational Social Systems*, vol. 5, no. 3, pp. 773-784, Sept. 2018. doi:10.1109/TCSS.2018.2861775 URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8444976&isnumber=8464016
10. C. Yu and A. Ginsberg, "Social Networking Without Sacrificing Privacy," *2018 International Conference on System Science and Engineering (ICSSE)*, New Taipei, 2018, pp. 1-6.doi: 10.1109/ICSSE.2018.8520188 URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8520188&isnumber=8519965
11. M. Huang, B. Zhang, G. Zou, S. Cheng, Z. Zhou and F. Chang, "Friend Recommendation in Online Social Networks Combining Interest Similarity and Social Interaction," *2018 International Conference on Audio, Language and Image Processing (ICALIP)*, Shanghai, 2018,pp.303-309. doi: 10.1109/ICALIP.2018.8455483
12. Xiao Shen, Haixia Long, and Cuihua Ma, "Incorporating Trust Relationships in Collaborative Filtering Recommender System", Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), *16th IEEE/ACIS International Conference on. IEEE*, 2015
13. Yi, X., Bertino, E., Rao, F. Y., & Bouguettaya, A. (2016). Practical privacy-preserving user profile matching in social networks. In 2016 *IEEE 32nd International Conference on Data Engineering, ICDE* 2016 (pp. 373–384). http://doi.org/10.1109/ICDE.2016.7498255
14. Makkaoui, K. E. L., & Ezzati, A. (2015). Challenges of Using Homomorphic Encryption to Secure Cloud Computing. In 2015 *International Conference on Cloud Technologies and Applications (CloudTech)*, 2-4 June 2015,Morocco,IEEE. http://doi.org/10.1109/CloudTech.2015.7337011