International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 4, June 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Retrieving Hidden Friends a Collusion Privacy Attack against Online Friend Search Engine

R. Brintha, H. Parveen Bagum (MCA)

Prist University, Thanjavur, Tamil Nadu, India

ABSTRACT

Online Social Networks (OSNs) are providing a diversity of application for human users to network through families, friends and even strangers. One of such application, friend search engine, allows the universal public to inquiry individual client friend lists and has been gaining popularity recently. Proper design, this application may incorrectly disclose client private relationship information. Existing work has a privacy perpetuation clarification that can effectively boost OSNs' sociability while protecting users' friendship privacy against attacks launched by individual malicious requestors. In this project proposed an advanced collusion attack, where a victim user's friendship privacy can be compromise from side to side a series of cautiously designed queries coordinately launched by multiple malicious requestors. The result of the proposed collusion attack is validate through synthetic and real-world social network data sets. The project on the advanced collusion attacks will help us design a more vigorous and securer friend search engine on OSNs in the near future.

KEYWORDS: *Social Network Services (SNS), Privacy Preservation, Friend Search, Social Network, OSN*

How to cite this paper: R. Brintha | H. Parveen Bagum "Retrieving Hidden Friends a Collusion Privacy Attack against Online Friend Search Engine" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-4, June 2020, pp.1720-1724, URL: www.ijtsrd.com/papers/ijtsrd31687.pdf

IJTSRD31687

1. INTRODUCTION

Social Network Services (SNS) are currently drastically revolutionizing the way people interact, thus becoming defect a predominant service on the web The impact of this paradigm change on socioeconomic and technical aspects of collaboration and interaction is comparable to that caused by the deployment of World Wide Web in the 1990's.. Catering for a broad range of users of all ages, and a vast difference in social, educational, and national background, SNS allow even users with limited technical skills to publish Personally Identifiable Information (PII) and to communicate with an extreme ease, sharing interests and activities.

An Online Social Network (OSN) offering, usually centralized, online accessible SNS contain digital representations of a subset of the relations that their users, both registered persons and institutions, entertain in the physical world. Spanning all participants through their relationships, they model the social network as a graph. Every OSN user can typically create his or her own OSN profile and use the available OSN applications to easily share information with other, possibly selected, users for either professional, or personal purposes. OSN with a more professional and business-oriented background are typically used as a facility geared towards career management or business contacts; such networks typically provide SNS with a more serious image. In contrast, OSN with a more private and leisure-oriented background are typically used for sharing and exchanging more personal information, like, e.g., contact data, photographs, and videos; OSN provided by such networks have usually a more youthful inter-face. The core OSN application is the creation and maintenance of contact lists.

2. LITERATURE SURVEY

In this paper [1] C. Chen et.al has proposed Statistical structures built constant identification of drifted Twitter spam-Twitter spam has become a major topic now a days. Late workscentred on relating AI methods for Twitter spam location, which utilize the measurable features of tweets. we see that the factual belongings of spam tweets vary by certain period, and in this way, the presentation of prevailing AI built classifiers reduces. This difficulty is alluded to as Twitter Spam Drift. In order to switch this dispute first does a deep study on the quantifiable skin tone for more than one million spam and non-spam tweets.

In this paper [2] projected plan is changing spam tweets since unlabelled tweets and consolidates them into classifier's preparation procedure. Many tests are made to measure the projected plan. The results show the present Lfun plan can altogether improve the spam discovery exactness in genuine world scenarios

In this paper [3] has proposed Automatically recognizing phony news in prevalent Twitter strings Information quality in online life is an undeniably significant issue, however web-scale information impedes specialists' capacity to evaluate and address a significant part of the incorrect substance, or "phony news," current stages in this paper builds up a technique for computerizing counterfeit news location on Twitter by figuring out how to foresee precision evaluations in two validity cantered Twitter datasets: CREDBANK, which supports the exactness for instance in Twitter a publicly supported dataset of exactness appraisals for occasions in Twitter, and PHEME, which contains a set of rumours and non-rumours, We use this to Twitter set content taken from Buzz Feed's fake news dataset and models arranged against freely reinforced experts beat models reliant on journalists' assessment and models arranged on a pooled dataset of both openly upheld workers and authors.

In this paper[4] has proposed A model-based methodology for recognizing spammers in interpersonal organizations In this the errand of distinguishing spammers in informal communities from a blend displaying viewpoint, in view of which we devise a principled unaided way to deal with identify spammers. In method initially speak to every client of the informal community with an element vector that mirrors its conduct and connections with different member. The projected methodology can naturally segregate among spammers and genuine clients, while existing solo approaches require human intercession so as to set casual edge parameters to distinguish spammers. In addition, our methodology is general as in it very well may be applied to various online social destinations. To show the suitability of the proposed technique, we led probes genuine information extricated from Instagram and Twitter.

In this paper [5] Spam identification of Twitter traffic: A system dependent on irregular backwoods and non-uniform element inspecting Law Enforcement Agencies spread an essential job in the examination of open information and need powerful strategies to channel problematic data. Clients' characterization and spammers' ID is a helpful method for mitigate Twitter traffic by unhelpful substance. Analysis are done on a famous datasets of Twitter clients. The known Twitter dataset is comprised of user marked as genuine clients or spammers, portrayed by 54 features. Exploratory results exhibit the viability of improved highlight testing technique.

3. METHODOLOGY

3.1. EXISTING SYSTEM

Social network platform are based on centralized architecture that intrinsically threat user time alone due to potential monitoring and interception of private user information, the goal is to design social network platforms based on a distributed architecture in order to assure user privacy. New method are investigate in order to solve some classical security and trust management problem similar to distributed systems by taking advantage of the information stored in the social network platforms. Such problems range from trust establishment in self-organizing systems to key management without infrastructure to co-Operation enforcement in peer-to-peer systems

DISADVANTAGES

- ➢ Will not manage the whole Social Network system
- ➢ Need more efficient for the security purpose

3.2. PROPOSED ALGORITHMS

Fast community building, rapid exchange of information at the professional and private level, social network platforms raise several issues concerning the privacy and security of their users. The goal of this thesis is to identify privacy and security problems raised by the social networks and to come up with the design of radically new architectures for the social network platform.

ADVANTAGES

- ➢ Our proposed system is based on the online reservation for the user, who are in need of a social network.
- ➢ Our proposed system helps to overcome the difficulties in getting an user profile.

3.3. METHODOLOGY

Fuzzy Clustering Algorithm

Fuzzy clustering (also referred to as **soft clustering** or **soft *k*-means**) is a form of clustering in which each data point can belong to more than one cluster. Clustering or cluster analysis involves assigning data points to clusters such that items in the same cluster are as similar as possible, while items belonging to different clusters are as dissimilar as possible. Clusters are identified via similarity measures. These similarity measures include distance, connectivity, and intensity. Different similarity measures may be chosen based on the data or the application

The FCM algorithm attempts to partition a finite collection of n elements $X = \{\mathbf{x}_1, \ldots, \mathbf{x}_n\}$ into a collection of c fuzzy clusters with respect to some given criterion.

Given a finite set of data, the algorithm returns a list of c cluster centres $C = \{\mathbf{c}_1, \ldots, \mathbf{c}_c\}$ and a partition matrix $W = w_{i,j} \in [0,1],\ i = 1, \ldots, n,\ j = 1, \ldots, c,$ where each element, w_{ij} , tells the degree to which element, X_i , belongs to cluster C_j.

The FCM aims to minimize an objective function:

$$\underset{C}{\arg\min} \sum_{i=1}^{n} \sum_{j=1}^{c} w_{ij}^{m} \left\| \mathbf{x}_i - \mathbf{c}_j \right\|^2,$$

Where:

$$w_{ij} = \frac{1}{\sum_{k=1}^{c} \left(\frac{\left\| \mathbf{x}_i - \mathbf{c}_j \right\|}{\left\| \mathbf{x}_i - \mathbf{c}_k \right\|} \right)^{\frac{2}{m-1}}}.$$

4. EXPERIMENT AND RESULTS

The proposed method has been implemented using .NET Technology. Attack against online friend n this module the admin can view the friends message. The Mutual friends download your image suddenly provides the alert message in your phone. The alert message is date, time, person name also mentioned. In this module the user can post the attack on any friend in the online for the potential security threads. This will bring the privacy protection on user side. Such rules are not defined by the SNM, therefore they are not meant as general high level directives to be applied to the\ whole community. Rather, we decide to let the users themselves, i.e., the wall's owners to specify BL rules regulating who has to be banned from their walls and for how long. Therefore, client strength be banned from a wall, by, at the same time, being able to post in other walls.

4.1. USE CASE DIAGRAM

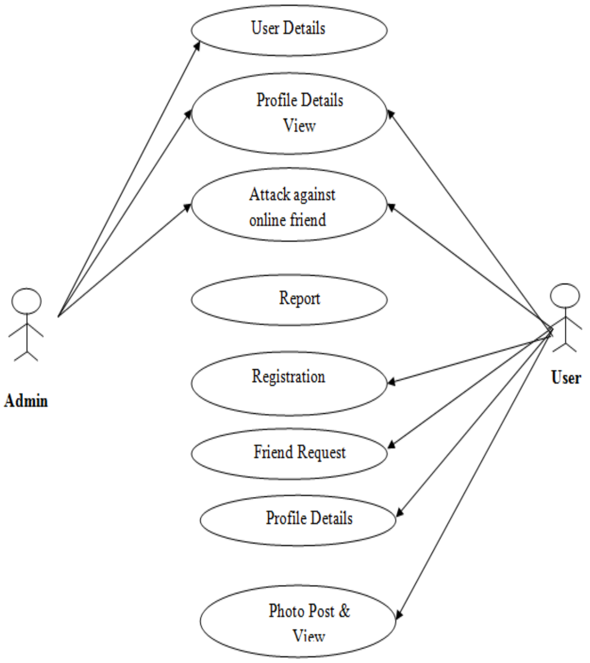
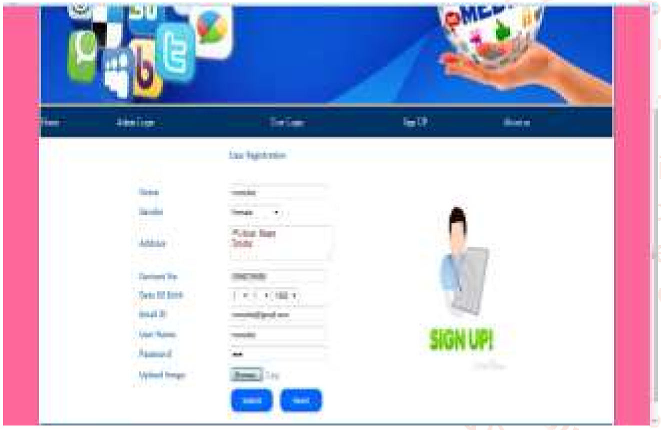


Figure 4.1 Use Case Diagram

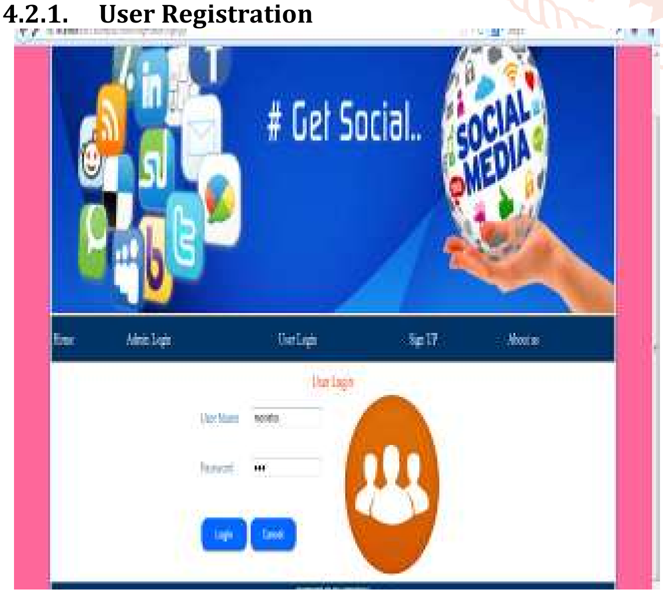
4.2. RESULT



User Registration

Name	monika
Gender	Female
Address	[illegible]
Contact No	[illegible]
Date Of Birth	[illegible]
Email ID	[illegible]
User Name	monika
Password	•••
Upload Image	Browse...

4.2.1. User Registration

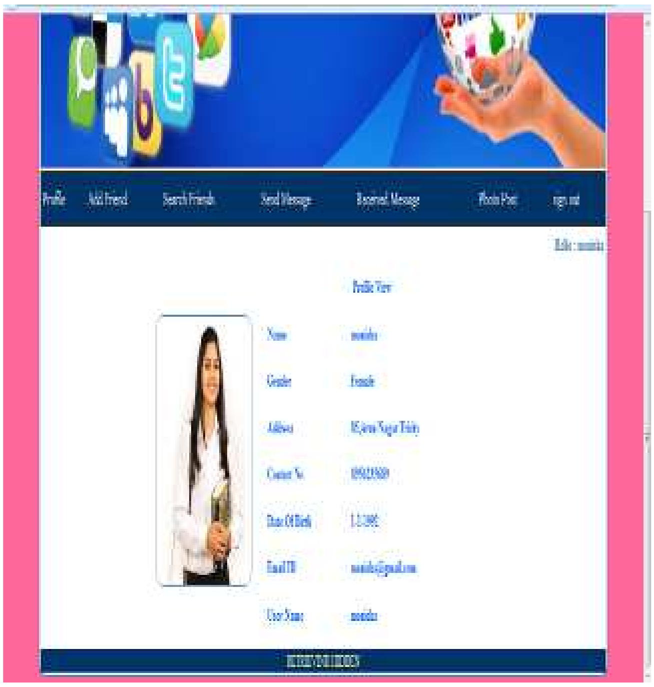


User Login

User Name monika

Password •••

Fig: 4.2.2 User Login

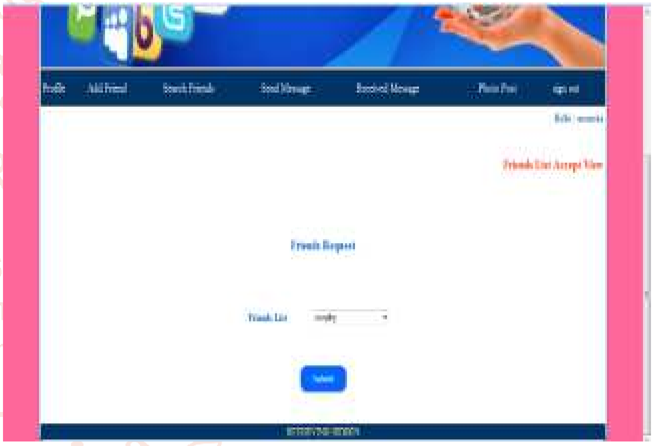


Hello : monika

Profile View

Name	monika
Gender	Female
Address	[illegible]
Contact No	[illegible]
Date Of Birth	[illegible]
Email ID	[illegible]
User Name	monika

Fig: 4.2.3 Profile View



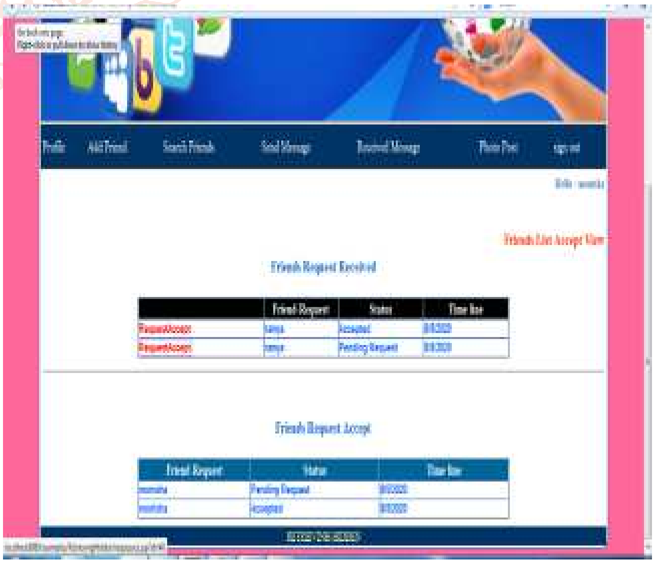
Hello : monika

Friends List Accept View

Friends Request

Friends List [illegible]

Fig: 4.2.4 Friend Request



Hello : monika

Friends List Accept View

Friends Request Received

	Friend Request	Status	Time line
RequestAccept	tanya	Accepted	[illegible]
RequestAccept	tanya	Pending Request	[illegible]

Friends Request Accept

Friend Request	Status	Time line
monika	Pending Request	[illegible]
monika	Accepted	[illegible]

Fig: 4.2.5 Friend Request Accepted

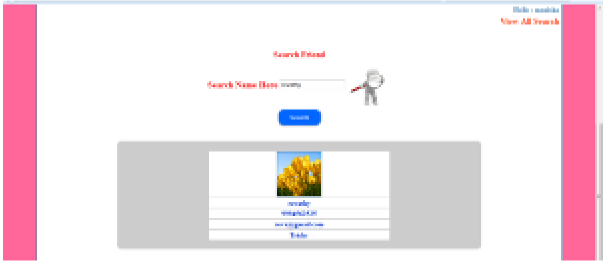


Fig: 4.2.6 Search Friend

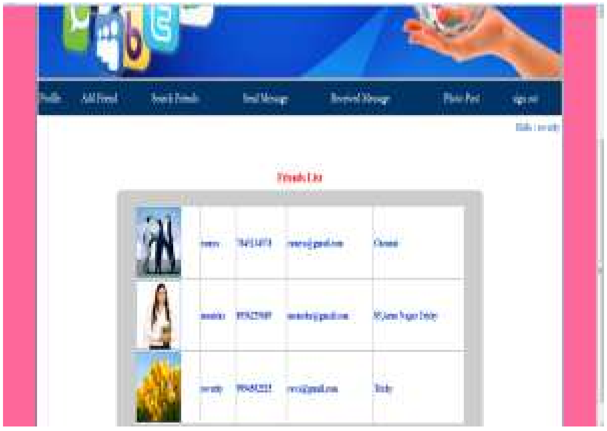


Fig: 4.2.7 Friend List

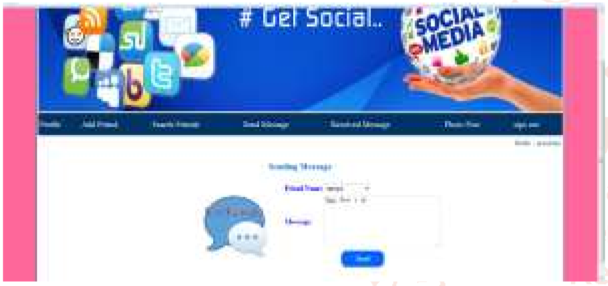


Fig: 4.2.8 Send Message

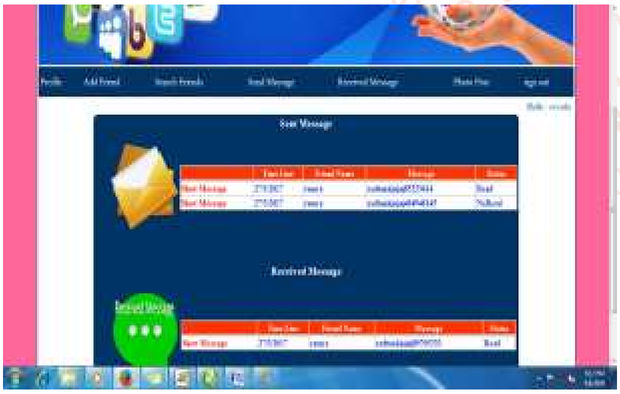


Fig: 4.2.9 View Message

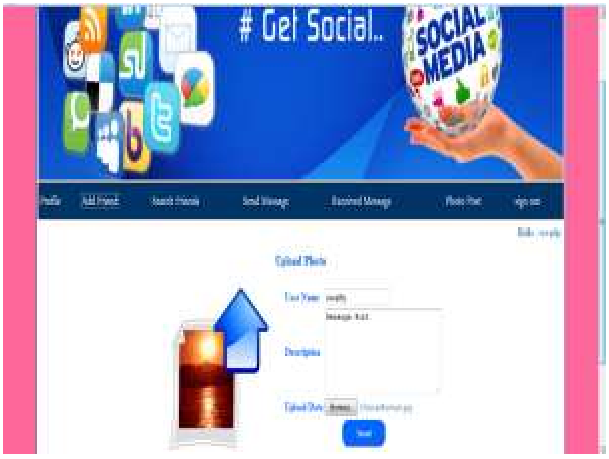


Fig: 4.2.10 Photo Post

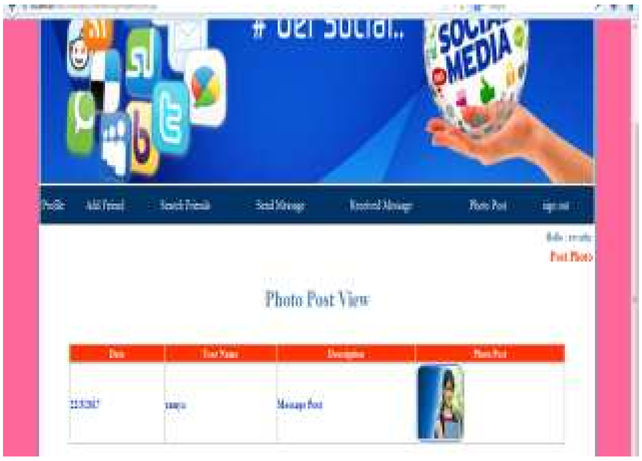


Fig: 4.2.11 Post View

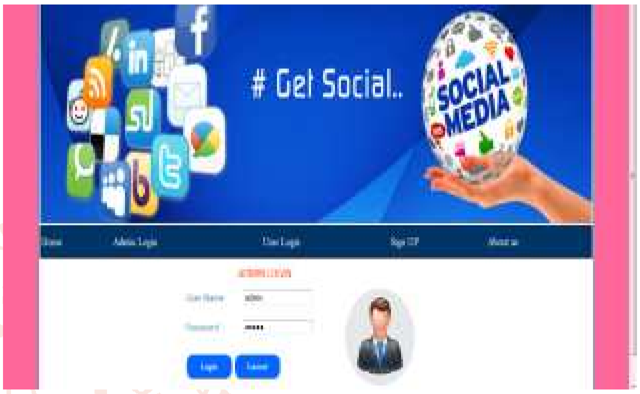


Fig: 4.2.12 Admin Login

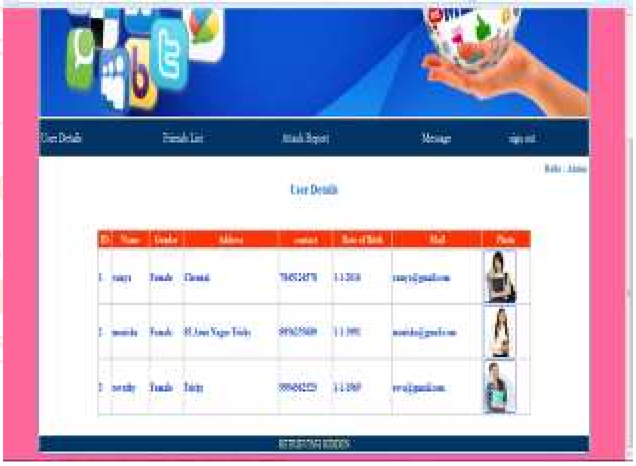


Fig: 4.2.13 User details

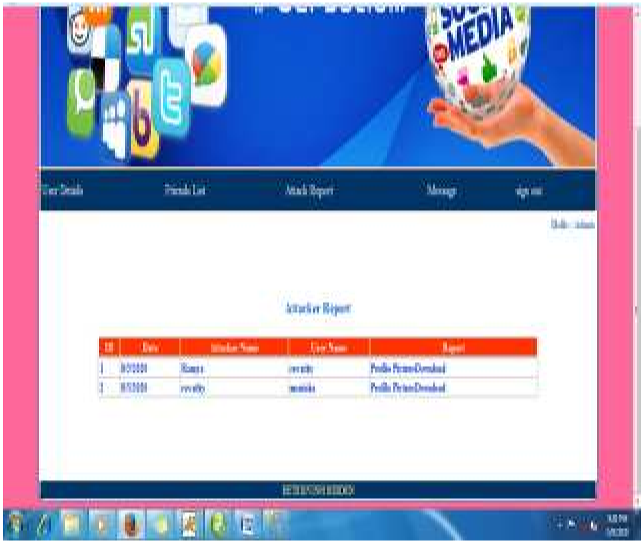


Fig: 4.2.14 Attacker Report

5. CONCLUSION

This project suggests a new approach to tackle these security and privacy problems with a special emphasis on the privacy of users with respect to the application provider in addition to defense against intruders or malicious users. In order to ensure users' privacy in the face of potential privacy violations by the provider, the suggested approach adopts a decentralized architecture relying on cooperation among a number of independent parties that are also the users of the online social network application. The second strong point of the suggested approach is to capitalize on the trust relationships that are part of social networks in real life in order to cop e with the problem of building trusted and privacy-preserving mechanisms as part of the online application.

FUTURE ENHANCEMENT

Google’s all algorithms are focused on improving the user experience. If users, have ever cared to closely look at the Google’s algorithms, you already know that they will rank a website that takes care of the user’s needs first. As it was believed that Search Engine involves too much of technicalities. But if you understand Search Engine or have worked as an Search Engine professional, you would know it is an art to its core. The Search Engine professionals today understand that mere technical knowledge is not enough in this user-friendly virtual world. A creativity is required for an Search Engine professional to catch the interest of a user.

REFERENCES

[1] B. Erçahin, Ö. Akta^3, D. Kilinç, and C. Akyol, ``Twitter fake account detection,'' in Proc. Int. Conf. Comput. Sci. Eng. (UBMK), Oct. 2017, pp. 388_392.

[2] F. Benevenuto, G. Magno, T. Rodrigues, and V. Almeida, ``Detecting spammers on Twitter,'' in Proc. Collaboration, Electron. Messaging, Anti- Abuse Spam Conf. (CEAS), vol. 6, Jul. 2010, p. 12

[3] S. Gharge, and M. Chavan, ``An integrated approach for malicious tweets detection using NLP,'' in Proc. Int. Conf. Inventive Commun. Comput. Technol. (ICICCT), Mar. 2017, pp. 435_438.

[4] T. Wu, S. Wen, Y. Xiang, and W. Zhou, ``Twitter spam detection: Survey of new approaches and comparative study,'' Comput. Secur., vol. 76, pp. 265_284, Jul. 2018.

[5] S. J. Soman, ``A survey on behaviors exhibited by spammers in popular social media networks,'' in Proc. Int. Conf. Circuit, Power Comput. Tech- nol. (ICCPCT), Mar. 2016, pp. 1_6.

[6] A. Gupta, H. Lamba, and P. Kumaraguru, ``1.00 per RT #BostonMarathon # prayforboston: Analyzing fake content on Twitter,'' in Proc. eCrime Researchers Summit (eCRS), 2013, pp. 1_12.

[7] F. Concone, A. De Paola, G. Lo Re, and M. Morana, ``Twitter analysis for real-time malware discovery,'' in Proc. AEIT Int. Annu. Conf., Sep. 2017, pp. 1_6.

[8] N. Eshraqi, M. Jalali, and M. H. Moattar, ``Detecting spam tweets in Twitter using a data stream clustering algorithm,'' in Proc. Int. Congr. Technol., Commun. Knowl. (ICTCK), Nov. 2015, pp. 347_351.

[9] C. Chen, Y. Wang, J. Zhang, Y. Xiang, W. Zhou, and G. Min, ``Statistical features-based real-time detection of drifted Twitter spam,'' IEEE Trans. Inf. Forensics Security, vol. 12, no. 4, pp. 914_925, Apr. 2017.

[10] C. Buntain and J. Golbeck, ``Automatically identifying fake news in popular Twitter threads,'' in Proc. IEEE Int. Conf. Smart Cloud (SmartCloud), Nov. 2017, pp. 208_215.

[11] C. Chen, J. Zhang, Y. Xie, Y. Xiang,W. Zhou, M. M. Hassan, A. AlElaiwi, and M. Alrubaian, ``A performance evaluation of machine learning-based streaming spam tweets detection,'' IEEE Trans. Comput. Social Syst., vol. 2, no. 3, pp. 65_76, Sep. 2015.

[12] G. Stafford and L. L. Yu, ``An evaluation of the effect of spam on Twitter trending topics,'' in Proc. Int. Conf. Social Comput., Sep. 2013, pp. 373_378.

[13] M. Mateen, M. A. Iqbal, M. Aleem, and M. A. Islam, ``A hybrid approach for spam detection for Twitter,'' in Proc. 14th Int. Bhurban Conf. Appl. Sci. Technol. (IBCAST), Jan. 2017, pp. 466_471.

[14] A. Gupta and R. Kaushal, ``Improving spam detection in online social networks,'' in Proc. Int. Conf. Cogn. Comput. Inf. Process. (CCIP), Mar. 2015, pp. 1_6.

[15] F. Fathaliani and M. Bouguessa, ``A model-based approach for identifying spammers in social networks,'' in Proc. IEEE Int. Conf. Data Sci. Adv. Anal. (DSAA), Oct. 2015, pp. 1_9.

[16] V. Chauhan, A. Pilaniya, V. Middha, A. Gupta, U. Bana, B. R. Prasad, and S. Agarwal, ``Anomalous behavior detection in social networking,'' in Proc. 8th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT), Jul. 2017, pp. 1_5.

[17] S. Jeong, G. Noh, H. Oh, and C.-K. Kim, ``Follow spam detection based on cascaded social information,'' Inf. Sci., vol. 369, pp. 481_499, Nov. 2016.

[18] M. Washha, A. Qaroush, and F. Sedes, ``Leveraging time for spammers detection on Twitter,'' in Proc. 8th Int. Conf. Manage. Digit. EcoSyst., Nov. 2016, pp. 109_116.

[19] B. Wang, A. Zubiaga, M. Liakata, and R. Procter, ``Making the most of tweet-inherent features for social spam detection on Twitter,'' 2015

[20] M. Hussain, M. Ahmed, H. A. Khattak, M. Imran, A. Khan, S. Din, A. Ahmad, G. Jeon, and A. G. Reddy, ``Towards ontology-based multilingual URL _ltering: A big data problem,'' J. Supercomput., vol. 74, no. 10, pp. 5003_5021, Oct. 2018.