RETRIEVING HIDDEN FRIENDS A COLLUSION PRIVACY ATTACK AGAINST ONLINE FRIEND SEARCH ENGINE

N. SRINIVASA RAO, BANDARU YESURAJU

Assistant Professor, **DEPT. of MCA, SKBR PG COLLEGE, AMALAPURAM, Andhra Pradesh**

Email:-naagaasrinu@gmail.com

PG Student of MCA, SKBR PG COLLEGE, AMALAPURAM, Andhra Pradesh

Email:-yesraju1081@gmail.com

Abstract

Online Social Networks (OSNs) offer a number of applications that allow humans to engage with their family, friends, and even strangers. One such program, friend search engine, which allows the general public to query individual users' friend lists, has recently gained popularity. In this research, we suggest a sophisticated collusion attack in which a victim user's friendship privacy can be jeopardized by a series of precisely crafted requests issued in concert by numerous malicious requestors. The proposed collusion attack's effect is proven using synthetic and real-world social network data sets.datasets

1. INTRODUCTION

Online social networks (OSNs), such as Facebook and Twitter, have grown in popularity in recent years and have become an integral part of many people's everyday lives. The OSNs offer a variety of applications that allow users to share information and engage with one another. One of the most popular applications is the buddy search engine, which allows users to browse through other users' friend lists. OSNs tend to release as many of a user's friends as possible in order to promote their sociability and attract additional users, as it is considered that the greater the number of shared friends displayed, the more probable the requestor and the queried user would be. connectlater.

This search engine, however, may reveal more friendship information than a questioned person is prepared to divulge, which is deemed a privacy infringement. A few researchers have discovered such an issue by crawling an OSN at random using the friend search API [1]. They also determined that, in the absence of proper countermeasures, it was possible to find all users' friendships in the OSN without using many queries [2], [3]. If such a breach of privacy is not handled properly, OSN users may experience panic and hesitate to continue using the service.usingtheOSNs.

In [4,] we designed a privacy-aware buddy display strategy that not only successfully preserves users' friendship privacy but also increases the sociability of the OSN. This technique is one of the most advanced studies on safeguarding user privacy for friend search engines, and it has been proven to successfully block attacks from independent attackers. However, collusion attacks, in which numerous malicious requestors share their knowledge and issue queries at the same time, may render the protection system ineffectual. We concentrate in this research on the design of collusion attacks against users' friendship privacy in OSNs.Themajor contributionsof thispaper arelistedasfollows.

To begin, we believe we are the first researchers to investigate advanced privacy vulnerabilities such as collusion attacks against friend search engines in OSNs. Second, an in-depth analysis of querying a small scale complete graph as well as a general network in various circumstances has been provided, which clearly shows the underlying reasons for why and how the suggested attack is built..

Inparticular,weobservethedefensescheme's[4]asymmetricdisclosureofusers'symmetricfriendships. By taking advantage of it, we design an advanced collusion attack, in which multiple maliciousrequestors closely coordinate with one another to launch their queries on different but related users in welldesigned orders. The design logic can be generally applied to launch attacks against any friendship privacypreserving solutions that disclose the symmetric friendship in an asymmetric way. Third, theproposedcollusion attack is designed to carefully select which users to query, which can significantly reduce the totalamount ofqueryeffort.

Fourth, we implement and run our proposed assault approach on one synthetic data set and three large scale real-world data sets to assess its effectiveness. The results of the experiments show that the proposed assault approach works efficiently and effectively on big scale data sets. By comparing the suggested collusion assault to a naive direct attack, we discover that our technique outperforms both the success rate and the number of malicious requestors required to violate a user's friendship privacy. Finally, our research on this advanced collusion attack helps us better understand the attack design and sheds information on the future design of a more secure privacy-preserving friend search engine.

PROBLEMSTATEMENT

To begin, we believe we are the first researchers to investigate advanced privacy vulnerabilities such as collusion attacks against friend search engines in OSNs. Second, an in-depth analysis of querying a small scale complete graph as well as a general network in various circumstances has been provided, which clearly shows the underlying reasons for why and how the suggested attack is built.

PURPOSE

Collusion assaults are described as attacks involving numerous malicious entities with the goal of gaining more than the entities benefit from individually conducted attacks. The many entities could be generated by a single attacker or by multiple real attackers. In comparison to individuals

Collusion attacks can employ more complex attack tactics and frequently target system weaknesses that individual attacks cannot detect.

OBJECTIVE

The suggested system includes To begin, the system is, to the best of our knowledge, the first researchers to explore advanced privacy techniques such as collusion attacks against friend search engines in OSNs.Second, an in-depth analysis of querying a small scale complete graph as well as a general network in various circumstances has been provided, which clearly shows the underlying reasons for why and how the suggested attack is built.isdesigned.

2. LITERATURESURVEY

2.1 INRODUCTION

Literature survey is the most important step in software development process. Before developing thetool, it is necessary to determine the time factor, economy and company strength. Once these things aresatisfied, ten next steps are to determine which operating system and language used for developing the tool.Once the programmers start building the tool, the programmers need lot of external support. This supportobtained from senior programmers, from book or from websites. Before building the system the aboveconsiderationr taken into fordevelopingthe proposed system.

2.2 RELATEDWORK

1. AnalysisofKey-

ExchangeProtocolsandTheirUseforBuildingSecureChannelsAUTHORS:R.

Canettiand H. Krawczyk

We provide a formalism for analyzing key exchange protocols that incorporates earlier definitional approaches and resulting in a security definition with some significant analytical benefits:
(i) any key-exchange protocol that meets the security definition can be supplemented with symmetric encryption and authentication features to offer provably secure communication channels (as defined here); and (ii) the definition allows for simple modular proofs of security: one can design and prove securityof key-exchange protocols in an idealized model where the communication links are perfectly authenticated,and then translate them using general tools to obtain security in the realistic setting of adversary-controlledlinks. We exemplify the usability of our results by applying them to obtain the proof of two classes of key-exchangeprotocols,Diffie-Hellmanandkey-transport,authenticatedviasymmetricorasymmetrictechniques.

2. MapReduce:SimplifiedDataProcessingOnLargeClusters

AUTHORS:J.DeanandS.Ghemawat

3. Map Reduce is a programming model and an implementation for processing and creating huge datasets that may be applied to a wide range of real-world activities. The computation is specified by the user in terms of a map and a reduce function, and the underlying runtime system automatically parallelizes the computation across large-scale clusters of machines, handles machine failures, and schedules inter-machine communication to make the best use of the network and disks. Over the last four years, Google has implemented over ten thousand distinct Map Reduce programs internally, and an average of one hundred thousand Map Reduce jobs are executed on Google's clusters every day, processing a total of more than twenty petabytes of data per day.

4. ScalableSecurityfor PetascaleParallel FileSystems

AUTHORS:A.W.Leung,E.L.Miller,andS.Jones

Petascale, high-performance file systems often hold sensitive data and thus require security, butauthentication and authorization can dramatically reduce performance. Existing security solutions performpoorly in these environments because they cannot scale with the number of nodes, highly distributed data,and demanding workloads. To address these issues, we developed Maat, a security protocol designed toprovidestrong,scalablesecuritytothesesystems.Maatintroducesthreenewtechniques.Extendedcapabilities limit the number of capabilities needed by allowing a capability to authorize I/O for any numberof client-file pairs. Automatic Revocation uses short capability lifetimes to allow capability expiration to actas global revocation, while supporting non-revoked capability renewal. Secure Delegation allows clients tosecurely act on behalf of a group to open files and distribute access, facilitating secure joint computations.Experimentsonthe MaatprototypeintheCephpetascale filesystem showan overheadaslittle as6--7%.

5. ScalablePerformanceOfThePanasasParallel FileSystem

AUTHORS:B.Welch,M.Unangst, and B.Zhou

The Panasas file system uses parallel and redundant access to object storage devices (OSDs), per-file RAID,distributedmetadatamanagement,consistentclientcaching,filelockingservices,andinternalclustermanagement to provide a scalable, fault tolerant, high performance distributed file system. The clustereddesign of the storage system and the use of client-driven RAID provide scalable performance to manyconcurrent file system clients through parallel access to file data that is striped across OSD storage nodes.RAIDrecoveryisperformed inparallelbytheclusterofmetadatamanagers, anddeclustereddataplacement yields scalable RAID rebuild rates as the storage system grows larger. This paper presents performancemeasures of I/O, metadata, and recovery operations for storage clusters that range in size from 10 to 120storage nodes, 1 to 12 metadata nodes, and with file system client counts ranging from 1 to 100 computenodes.Production installationsareaslargeas500 storagenodes, 50metadata managers,and 5000clients.

3.EXISTINGSYSTEM

Collusionattackscanbedefinedasattacksthatinvolvemultiplemaliciousentitiesaimingatobtaining greater gain than what the entities benefit from individually launched attacks. The multiple entitiescan be fake accounts created by a single attacker or by different real attackers. Compared to individualattacks, collusion attacks can use more complicated attack strategies and often exploit system vulnerabilitiesthatcannot be discoveredbyindividual attacks.

LIMITATIONOFEXISTINGSYSTEM

Thefollowing arethemain limitations of theexistingsystem. Theyare as follows:

1. Thereis nofilteringsystem tofind PrivacyAttack.
2. Lesssecuritydue NoURLBased attackDetection.

4.PROPOSEDSYSTEM

In the proposed system,First,tothe bestof our knowledge, the systemisthe first researchersstudying such advanced privacy attacks as collusion attacks against friend search engine in OSNs.Second,in-depthanalysishasbeenprovidedonqueryingasmallscalecompletegraphaswellasageneralnetworkin various scenarios, which well explains the fundamental reasons of why and how the proposed attack isdesigned.

ADVANTAGESOFTHEPROPOSEDSYSTEM

Thefollowing aretheadvantages of theproposedsystem,theyareasfollows:

1. Thesystemprovidestheflexibilityforindividualuserstodeterminethenumberoffriends,sayk,todisplayin responseto friend queries.
2. Particularlyfocuson the design of collusion attacksagainst users’friendshipprivacyinOSNs

5. SOFTWAREPROJECTMODULES

Implementation is the stage where the theoretical design is converted into programmatically manner.In this stage we will divide the application into a number of modules and then coded for deployment. ThefrontendoftheapplicationtakesJSP,HTMLandJavaBeansandasaBack-EndDatabasewetookMy

SQLdatabase.Theapplicationisdividedmainlyintofollowing2modulesandinsidethesemodulesthereareseveral other sub modules present. Theyare as follows:

5.1 OSNServerModule

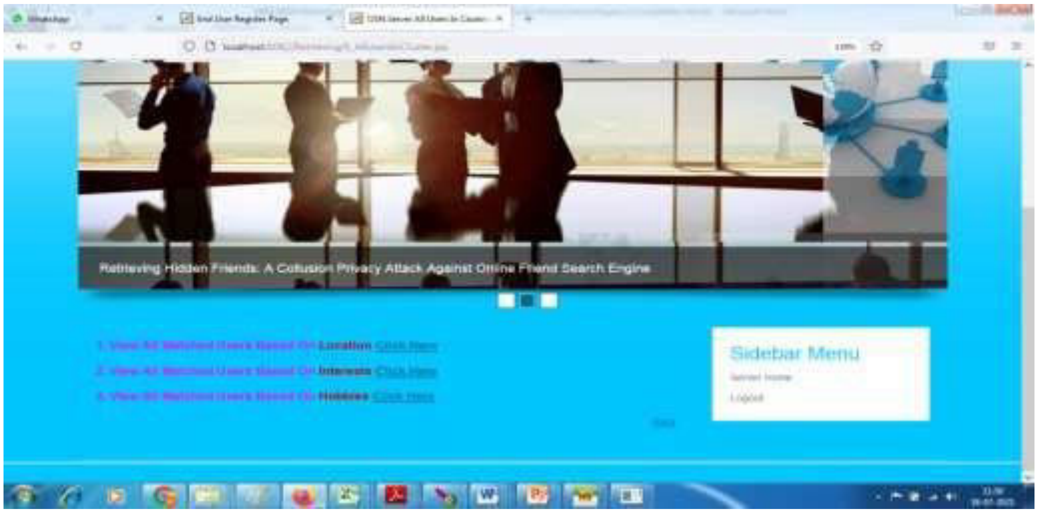
Inthismodule, theAdminhas tologinbyusingvaliduser name andpassword. Afterlogin successfulhecanperform some operations such as View All Users And Authorize,View Friend Request and Response,ViewAll Matched Users,View All User Post Posts,View All Posts Recommended Details,View All FriendRecommended Details,View All Collusion Attacker Details,View Posts Scores Results ,View CollusionAttackerResults

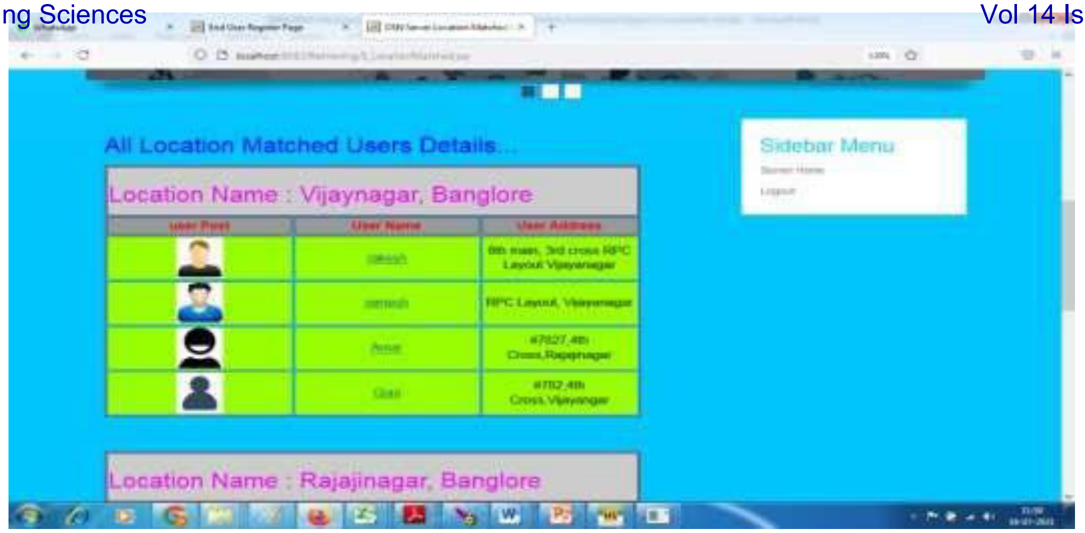
5.2 UserModule

In this module, the Admin has to login by using valid user name and password. After login successful he canperform some operations such as View All Users And Authorize,View Friend Request and Response,ViewAllMatchedUsers,ViewAllUserPostPosts,ViewAllPostsRecommendedDetails,ViewAllFriend Recommended Details,View All Collusion Attacker Details,View Posts Scores Results ,View CollusionAttackerResults

6. OUTPUTRESULTS

AdminViewstheMatchedusers


Retrieving Hidden Friends: A Collusion Privacy Attack Against Online Friend Search Engine
1. View All Matched Users Based On Location Click Here
2. View All Matched Users Based On Interests Click Here
3. View All Matched Users Based On Hobbies Click Here
Back
Sidebar Menu
Server Home
Logout



All Location Matched Users Details...

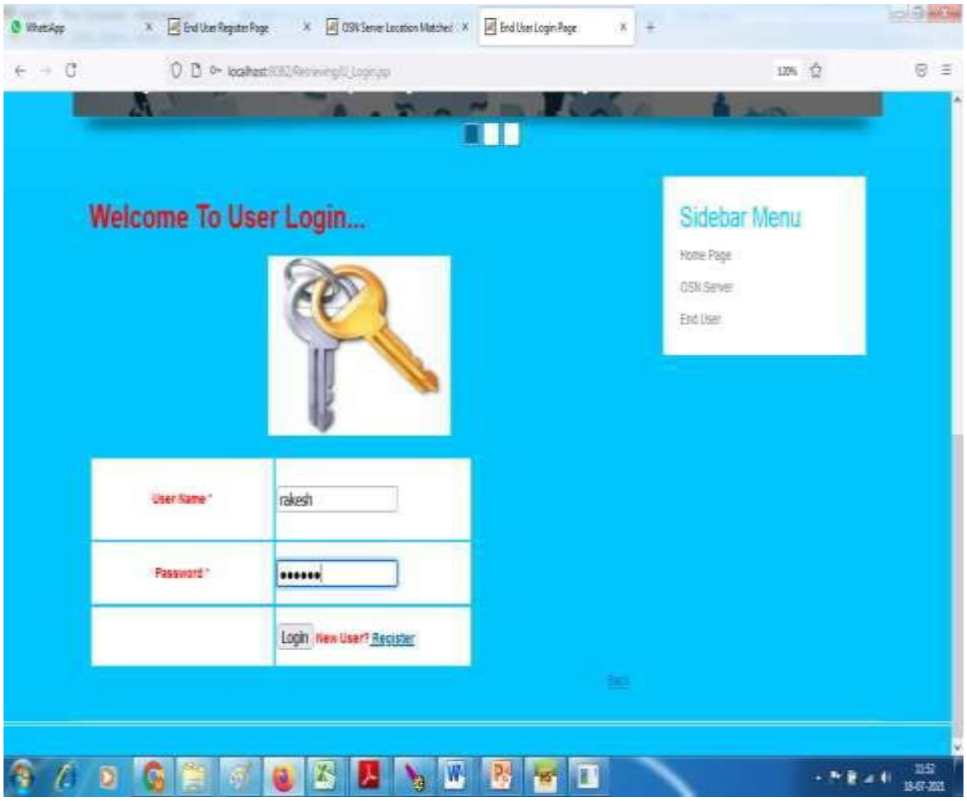
Location Name : Vijaynagar, Banglore

user Post	User Name	User Address
	rakesh	6th main, 3rd cross RPC Layout Vijayanagar
	ramesh	RPC Layout, Vijayanagar
	Arun	#7827,4th Cross,Rajajinagar
	Ojas	#782,4th Cross,Vijayangar

Location Name : Rajajinagar, Banglore

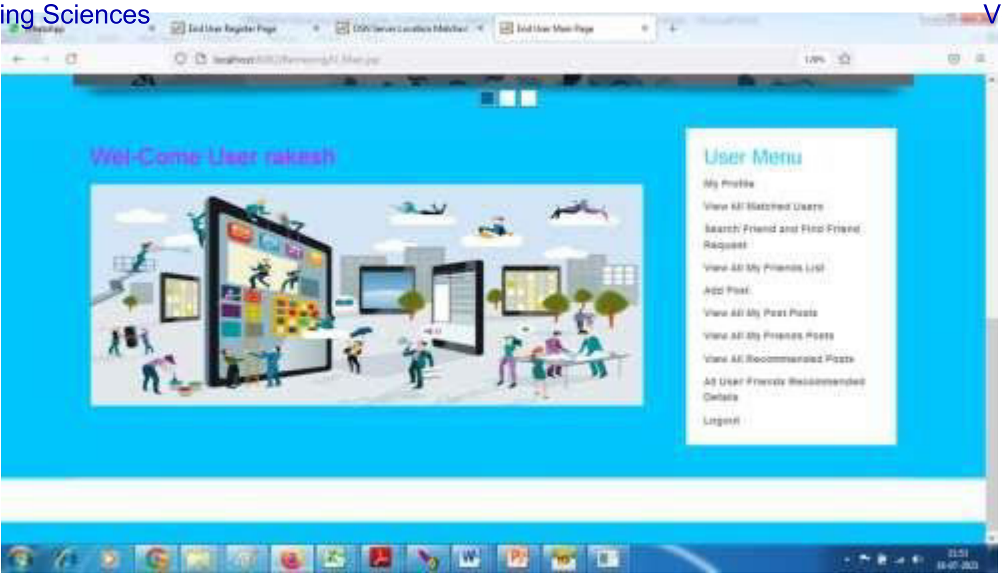
RepresentstheMatchedUsers

UserLogin



Welcome To User Login...

User Name *	rakesh
Password *	••••••
	Login New User? Register

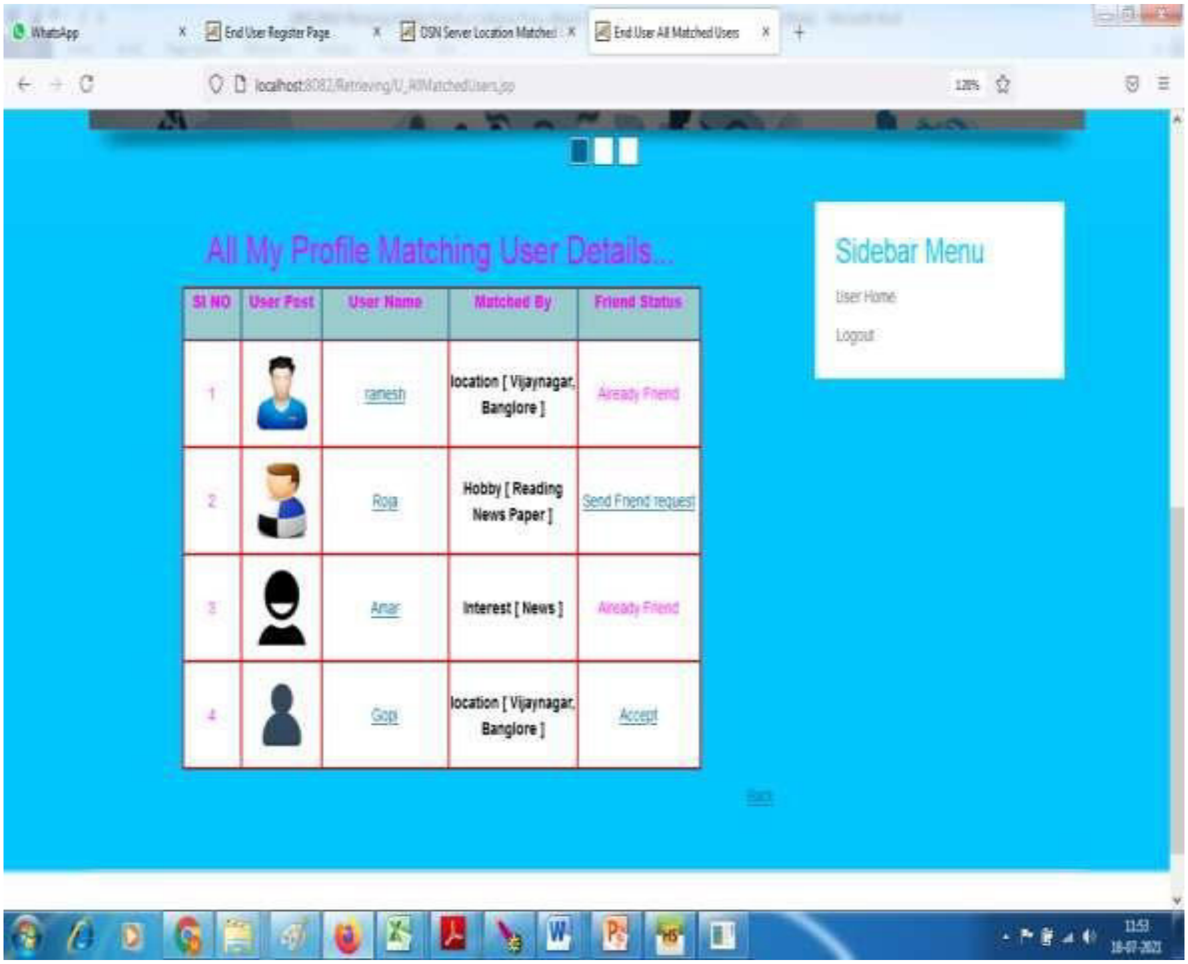


Wel-Come User rakesh

End User Register Page
DSN Server Location Matched
End User Main Page
User Menu
My Profile
View All Matched Users
Search Friend and Find Friend Request
View All My Friends List
Add Post
View All My Post Posts
View All My Friends Posts
View All Recommended Posts
All User Friends Recommended Details
Logout

RepresentstheUserLoginandHomePageVie

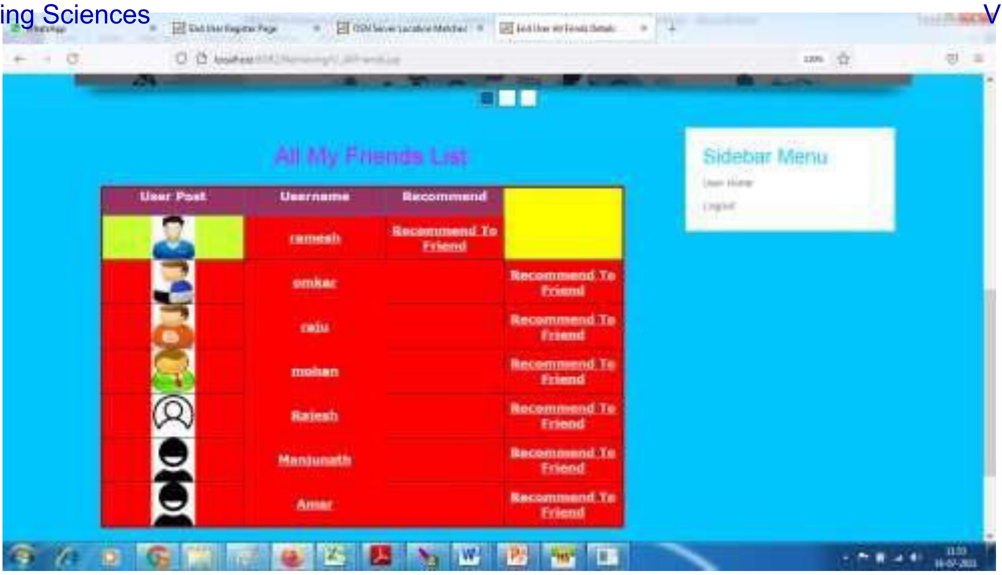
w All Friends basedon profilekeywordmatching



WhatsApp
End User Register Page
DSN Server Location Matched
End User All Matched Users
localhost:8082/Retrieving/U_AllMatchedUsers.jsp
120%
Sidebar Menu
User Home
Logout
Back
11:53
18-07-2021

All My Profile Matching User Details...

Sl NO	User Post	User Name	Matched By	Friend Status
1		ramesh	location [Vijaynagar, Banglore]	Already Friend
2		Roja	Hobby [Reading News Paper]	Send Friend request
3		Amar	Interest [News]	Already Friend
4		Gopi	location [Vijaynagar, Banglore]	Accept



All My Friends List

User Post	Username	Recommend	
	ramesh	Recommend To Friend	
	omkar		Recommend To Friend
	raju		Recommend To Friend
	mohan		Recommend To Friend
	Rajesh		Recommend To Friend
	Manjunath		Recommend To Friend
	Amar		Recommend To Friend

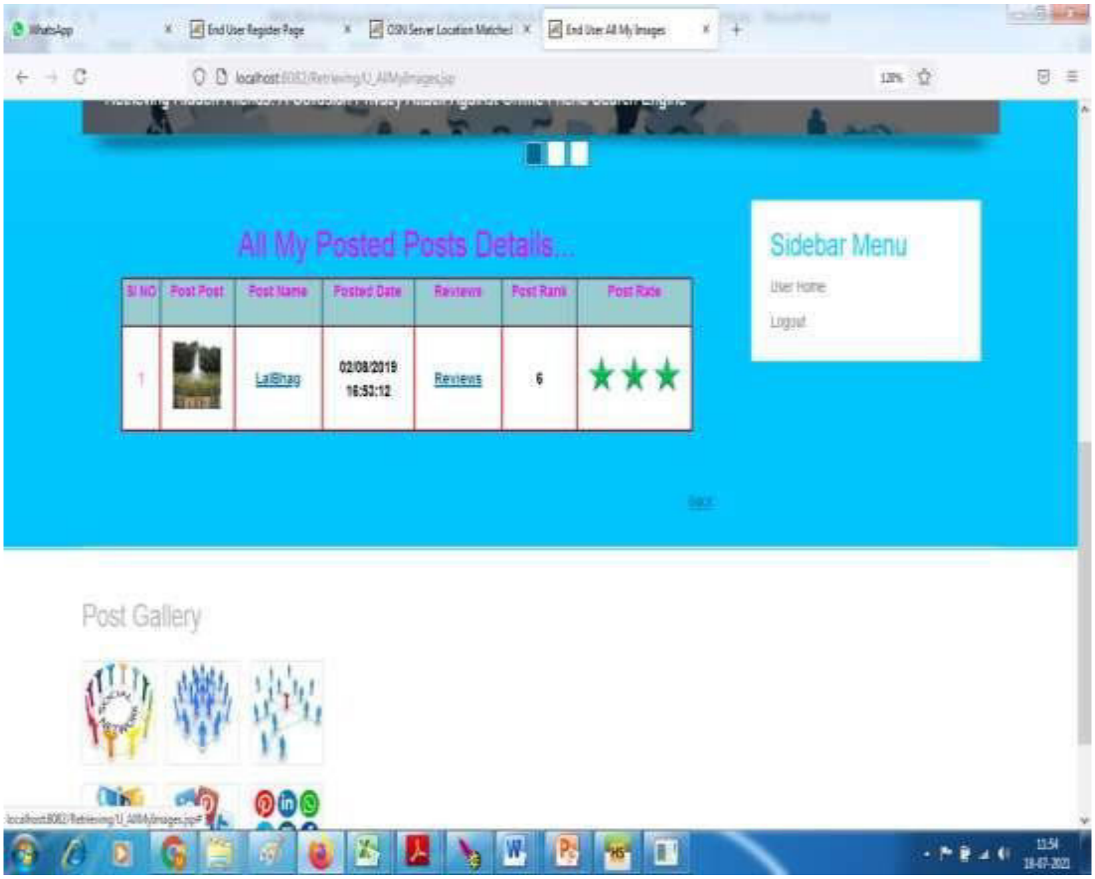
Sidebar Menu

User Home

Logout

RepresentstheAllFriendsandrecommendationsUs

ercan ViewHis PostDetails


WhatsApp
End User Register Page
OSN Server Location Matched
End User All My Images
localhost:8082/Retrieving/U_AllMyImages.jsp

All My Posted Posts Details...

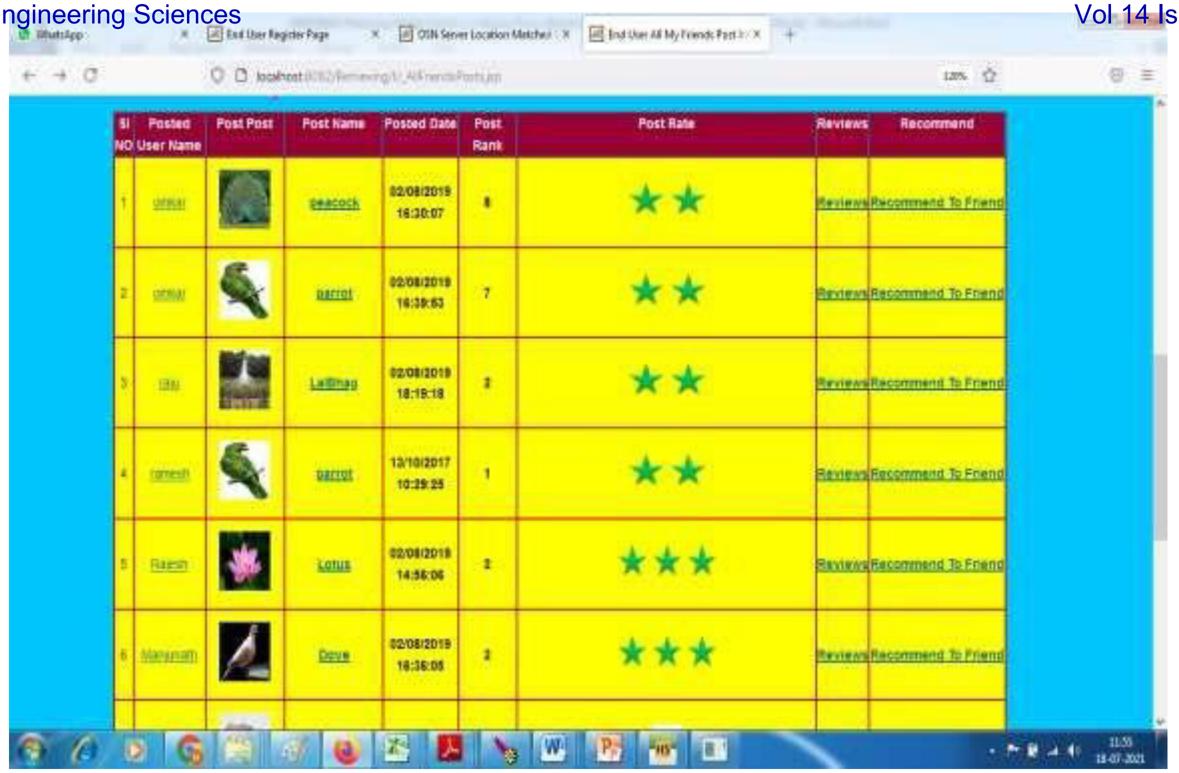
Sl NO	Post Post	Post Name	Posted Date	Reviews	Post Rank	Post Rate
1		LalBhag	02/08/2019 16:53:12	Reviews	6	★★★

Sidebar Menu

User Home

Logout

Post Gallery



Sl NO	Posted User Name	Post Post	Post Name	Posted Date	Post Rank	Post Rate	Reviews	Recommend
1	omkar		peacock	02/08/2019 16:30:07	8	★★	Reviews	Recommend To Friend
2	omkar		parrot	02/08/2019 16:39:53	7	★★	Reviews	Recommend To Friend
3	Raju		LalBhag	02/08/2019 18:19:18	2	★★	Reviews	Recommend To Friend
4	ramesh		parrot	13/10/2017 10:29:25	1	★★	Reviews	Recommend To Friend
5	Rajesh		Lotus	02/08/2019 14:56:06	2	★★★	Reviews	Recommend To Friend
6	Manjunath		Dove	02/08/2019 16:36:06	2	★★★	Reviews	Recommend To Friend

Representstheuserownpostandhis/herFriendspost

7. CONCLUSION

In this proposed work, we have proposed an advanced collusion attack strategy where multipleattackers with very limited initial knowledge (i.e. only the victim node) can successfully penetrate thedefense and violate victim node's privacy settings on friend search engine. In particular, we start this studywith a simple and small social clique model, aiming to deeply understand users' friendship types and revealthe fundamental reasons why collusion attacks can be done successfully. Based on observations made fromthis model, we further propose to classify social network users into non-popular users and popular users;develop different attack strategies against them; and illustrate the attack effectiveness in a general socialnetwork through different scenarios. Experiment results show that our proposed collusion attack strategy hasachieved high successratebyusinglimitednumber ofmalicious requestors.

8. REFERENCES

[1] "Friendlistapi." [Online].
Available:https://developers.facebook.com/docs/reference/fql/friendlist

[2] J.Bonneau,J.Anderson,F.Stajano,andR.Anderson,"Eightfriendsare enough:socialgraphapproximationvia publiclistings,"in Proceedingsof ACMSNS'09,2009, pp.13–18.

[3] A.Yamada,T.H.-J.Kim,,andA.Perrig,“Exploitingprivacypolicyconflictsinonlinesocialnetworks,”in Technical report, 2012.

[4] N.Li,“Privacy-awaredisplaystrategyinfriendsearch,”inProceedingsofIEEEInternationalConference on Communications (ICC), Communicationand Information Systems Security Symposium,2014, pp. 951–956.

[5] R. Fogues, J. M. Such, A. Espinosa, and A. Garcia-Fornes, “Open challenges in relationship-basedprivacy mechanisms for social network services,” International Journal of Human-Computer Interaction, vol.31, no. 5, pp. 350–370, 2015.

[6] L. Guo, C. Zhang, and Y. Fang, “A trust-based privacy-preserving friend recommendation scheme foronline social networks,” IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 4, pp. 413–427, 2015.

[7] Z. Feng, H. Tan, and H. Shen, “Relationship privacy protection for mobile social network,” in AdvancedCloudand BigData (CBD), 2016InternationalConferenceon.IEEE,2016, pp.215–220.

[8] N. Li, N. Zhang, and S. Das, “Relationship privacy preservation in publishing online social networks,” inProceedingsoftheThirdIEEEInternationalConferenceonSocialComputing(SocialCom’11),MIT,Boston,US, 2011.

[9] B. Zhou and J. Pei, “Preserving privacy in social networks against neighborhood attacks,” in Proceedingsofthe24thIEEE InternationalConferenceonDataEngineering(ICDE’08),2008, pp.506–515.

[10] J. Cheng, A. W. Fu, and J. Liu, “K-isomorphism: Privacy preservation in network publication againststructuralattack,”in SIGMOD’10, 2010.

[11] S. Das, O. Egecioglu, and A. E. Abbadi, “Anonymizing edge-weighted social network graphs,” inTechnicalReport CS-2009-03,Computer Science,TheUniversityofCalifornia, SantaBarbara,2009.

[12] M.Hay,G.Miklau,D. Jensen,D.Towsley,andP.Weis,“Resisting structuralreidentificationinanonymizedsocial networks,”in PVLDB’08,2008.

[13] B. Zhou, J. Pei, and W. Luk, “A brief survey on anonymization techniques for privacy preservingpublishingof socialnetwork data,”SIGKDD Explorations,vol. 10, no.2, pp.12–22, December2008.

[14] E.ZhelevaandL.Getoor,“Preservingtheprivacyofsensitiverelationshipsingraphdata,”inProceedings of the 1st ACM SIGKDD International Workshop on Privacy, Security, and Trust in KDD,PinKDD2007,InConjunctionwiththe13thACMSIGKDDInternationalConferenceinKnowledgeDiscoveryandData Mining,KDD,(PinKDD’07),San Jose,CA, USA, 2007.

[15] L. Liu, J. Wang, J. Liu, and J. Zhang, “Privacy preserving in social networks against sensitive edgedisclosure,” in Technical Report CMIDA-HiPSCCS 006-08, Department of Computer Science, University ofKentucky,KY, 2008.