SOCIAL MEDIA ISSUE & SOLUTION:-

Detection of Accessibility and Alteration Anomalies in Uploaded Image

[1]Santoshi Rudrakar, [2]Dr. Varsha Sharma
[1]M.Tech. Scholar, [2]Professor,
[1]School of Information Technology, UTD-RGPV Bhopal [2]School of Information Technology, UTD-RGPV Bhopal, India
[1]F-7/1, Professor Colony, Bhopal, India

Abstract :
In this era of Social Network, end users upload photos in wide range to share their activities and thoughts with social networking friends. These posts are belonging to family, friend(s) or their own (single). The Social Networking Sites provide facility to keep them updated by main features of Like, Comment or Share about their post about the reactions of their friends for the post by generating notification. In this research paper we have discovered the issue of downloading the photo from the end user's profile by the third party (Social Networking friends or anonymous). End users have no information about this (downloading) activity done by third party. Thus more issue arises in front of us such as image morphing, defamation as that third party uploads the same photo again on social media publicly or to the outside world on the Internet of the Social Network, leads to the cause of defamation. Beyond of all these three issues in this research paper we are enclosing some appropriate issues behind uploaded post of a genuine user with adequate solution.

Index Terms -
Social Networking Sites, Social Network issues, genuine uploader, image privacy, image protection, unauthorized access.

I. INTRODUCTION

This is the age of Social networking sites where users 2.51 billion out of the 7 billion population around the world according to a survey. These users interconnect with each other and they share their thoughts, images, videos post with their friends, mutual friends or publicly .The up loader have information about the reactions of these friend or social networking sites users on their profile via generating notification on the up-loader's profile thus user have knowledge about other users reaction through over his or her post as Like, Comment, Share, Tag.
Contrary, we are here to limelight some issues are on social network the friends or social media users can perform more activities than these four reactions. Unlike to these reactions the social media able to perform some more activity, as discussed in this survey paper are given below:

- View
- Download
- Share After Download

The Up-loader have knowledge about others activity on their post in profile. Since, the issues arise on these three additional activities of the social media user's activities that the Up-loader do not have any knowledge about:-

- Who has viewed?
- Who has downloaded?
- Who has shared indirectly after downloading the up-loader's post?

F. Stutzman [13] assess a suggestion for how for how to increase the privacy on social networking site users. To deal with identity theft, they advise to set user profiles more private as possible as just for "Friend only", that will be help to reduce the data breach risk on Social Networking websites. Unlike to such risk handling by sharing the post only for close friends might not be able to deal with the disclosing of the private post, the issue would be of downloading the uploaded image by one of among these special friends and indirectly shared to other Facebook users except the genuine uploader. The serious problem on which we are making that in light in this survey is genuine user is still unknown besides this much of privacy maintenance.

2. Literature Review

Furthermore there has been discussed some of supportive previous year's survey papers including with research papers too :-

2.1.Arjun K.P., and authors "PROvacy : Protecting Image Privacy in Social Networking Sites Using Reversible Data Hiding". IEEE, 2016 [1]

In this paper the aim is to propose an algo for Securing Image Privacy in Social Media Sites from Third Party (Unauthorized Users) .Consequently all these seven authors have been proposed method using through Reversible Data Hiding (RDH) technique for encrypting images by X. Zhang [12], Fig 1. In this proposed method as a user uploads an image, the front end software get in a few privacy data into the picture through out Reversible Data Hiding (RDH) method subsequently save encrypted picture into database system. for showing same post on friend's timeline, the algorithm for front end checks the image embedded privacy information matching point to friend's privacy information. If this both privacy information are same, then only the image is visible to the fries. Worthwhile, the Facebook user is not in a friend list so the picture is invisible. Hence, initial method is to be embedded and next one is processing the encrypted picture into database form, they are being able to secure the uploaded images on social network.

This technique, introduces to embedded image privacy information into the picture, furthermore the users including with only basis of this privacy information the social networking friends on the social media sites can view the picture. Reversible Data Hiding (RDH) technique for encrypting images. Hence only friends in a list of uploader can only access the image.

2.2 Joshua Wede, Smitha Sundareswaran, and Anna Cinzia Squicciarini. "Privacy Policy Inference of User-Uploaded Images on Content Sharing Site" . IEEE Journal 2015 [2]

This paper suggested a methodology to compose privacy setting on social media to the users for their uploaded images. The paper. "Privacy Policy Inference of User-Uploaded Images on Content Sharing Site" They proposed a two-level framework which works on the user's available history on the social networking sites, determines the best available privacy policy for the user's images being uploaded. The Adaptive Privacy Policy Prediction (A3P) algorithm for implementing the methodology has been used to deal with the default privacy setting by the social media providers. In This paper classification framework has been used that categorize the user uploaded images ,which might be belongs to similar policies, furthermore on the basis of policy prediction algorithm there is automatically generated the privacy setting for the newly uploaded images, as well as with user's assistance for social security.

There are some co-relevant real case taken from Indian famous newspaper The News Network as discussed below:-

2.3 Real Case: TNN | Jun 29, 2015, 12.09 PM IST [3]

On Sunday, Neha (name changed), a fourth-year engineering student at a private university, approached the Bajaj Nagar police. Accompanied by her friend, she registered a complaint against an unknown person for copying her image and posting it on an adult page on Instagram.

"It took her four days to muster courage to file a complaint with the police. The morphed photo was first noticed by her friend and by now, it has been circulated among a few of my friends," said Neha.

Though the police registered the case, they themselves are not sure how to handle such cases.

2.4 Case :TNN | Jun 29, 2015, 12.09 PM [3]

Another student of a private university in Jagatpura area lodged with police that her photo was copied from her Facebook account and circulated with a vulgar caption on WhatsApp. She too had filed a complaint but the police failed to trace the accused.

Rajendra Sharma, SHO, cyber cell police station, expressed inability in solving most of such cases.

He said, "The servers of most of the social media sites are based outside India, and so they are out of the ambit of Indian laws. The most effective remedy is awareness on handling social media accounts."

"Instagram has a help page through which a victim can approach the social media authorities and report the case. In cases related to WhatsApp, it is difficult to the track the origin," said Mukesh Choudhary, a cyber crime consultant to Rajasthan Police India.

Thus throughout these cases the conclusion is that, an unknown, unauthorized user of social network can download as well as upload the image publicly with the source of uploader's profile itself, consequently the uploader's image privacy infringement. Second another significant flaw is, all these activities of this unknown is still graved, the genuine user is unaware by all these bomb activities.

2.5 Analyzing Facebook Privacy Settings: UserExpectations vs. Reality by Yabing Liu Northeastern University Boston, MA, USA [5]

Through this study Yanbing Lin [5] illuminated approximately half of the shared post by the users follows the default privacy setting, this default privacy setting causes to exhibit the shared post for all Facebook users. In the survey Up-loader reported that the default privacy setting desired 20% of the time, the point of view of the users was that this setting is poorly chosen. Furthermore due to security reason for users extreme private photo which is shared by their own they altered the default private setting as more private just only for special friends since users expectations less than 40% of the time. This explosively urged for offering firmly configuring users privacy setting and new tools to manage privacy setting as user are having difficulties.

Involuntarily updating friend lists the consequences suggested that the social media might be automatically leveraged to aid users in selecting groups of friends to share post with. In this paper the author developed the Facebook application which will be used in social media to assist up-loaders generate friend lists conveniently.

2.6 Amanda J. Cox (2016)

There is proposed solution for privacy flaws discussed in the literature using the application of complex algorithms to have privacy preservation for PII. The algorithm avoids the involvement for a user, consequently this algorithm helps to accelerate weakness as social network user is unaware of plenty of PII changes had into their social network profile .

For achieving the goal there has been used a risk Matrix as a tool that that works on the color representation methodology to show the vulnerability level of the user, and suggest them to achieve high security privacy settings [8].

2.7 C. Marcum et al. [23]

Assessed that each user might be not understand and deal with the risk as well as some of the issues associated with making public to their personal data or post else importance of use of this information that may be highly confidential with respect to social engineering attacks. It is little complicated to maintain the security for the shared post as well as information.

2.8 Yabing Liu,et. al,(2011)[4]

Yabing Liu,et. al suggested a method for maintaining privacy using default and private tool. Worthwhile the full extention of privacy risks and issues is still not known and there is a little modification for incidence of undefined privacy setting as well the problems are faced by genuine users if they want to manage the account privacy.

Roshan Jabee and M. Afsar Alam , (2016) states that some Users were happy with privacy setting. The survey consequences presents that 23% social networking users were unsatisfied with privacy setting for social networking websites, furthermore 77% social networking site's users were happy with by default privacy setting by the way those users said that by default settings for privacy must be have more improvements.

User believes on the setting for privacy and shares photos on Facebook the consequences indicates as 41% of social networking users untrusted on setting for security of social networking websites and more 49% social media users believe the Facebook security setting in contrast 10% of the social networking users had no response. For their belief, they share post and 49% of social media users share photos. Minimum 75% of users never read the policy of privacy, so might be that is the reason that of them untrusted the Social sites providers are securing the personal data. 4.8 Users have knowledge about privacy threat and identity theft. Still 25% people have

experienced privacy breach and identity theft in social sites and 10% users had no response. Afterward by having inquires to them about their identity theft among them, 31% user respond positively.

By default privacy policy and setting in Facebook needs improvement. Around of 85% users wanted more enhancing privacy setting of Facebook.

Social networking sites privacy concerns become much more potential as the availability increased for globally shared personal information. Social networking sites providing high-level to be accessible and transparence in it. Furthermore users concern about sharing and posting their personal post and information as well over online platform in Facebook.

While Boyd (2007) stated that social site users exited to developing their existence online by the disclosure of their personal identity information subsequently. Several causes are there behind the increased vulnerability of personal information being used as the main object than purely intended on social networking sites [11].

2.9 Fuchs (2010)

Fuchs explains, the objective of privacy in Facebook is oriented on an individual perspective as well as understanding of automation of privacy. Fuchs (2010, p. 148) elaborates the issue "is that the users are not asked if they find targeted advertising necessary and agree to it". 'User consent' technique is used in this concept for Facebook's Privacy Policy [6].

Dumas, and co – authors (2014, p. 376) [5] suggest, "users should not bear the entire burden of their privacy protection", duly if Social Networking Sites made signed the agreement of terms and conditions. Social networking sites users handover their privacy on the movement of the "I accept**"** button, social sites less clues is pressed. Subsequently user's information and data is used as a commodity for sharing with third parties, specially to the advertisers.

This is work on privacy "wizards" [7], which uses machine learning algorithms to infer communities in the complementary to recent work. `

TABLE 1. CRITICAL ANALYSIS

S.No.	Classification	Objective	Method/ Approach	Tool/ Technology /Platform	Reference
[1]	Downloader's Anonymity	To Propose an algorithm for Protecting Image Privacy with respect to Unauthorized Users .	Reversible Data Hiding (RDH) technique for encrypting images by X. Zhang [5] , *Fig 1.*	Reversible Data Hiding (RDH)	Arjun K.P.1, [1]
[2]	Privacy Setting	To help users compose better privacy settings for their images.	A two-level framework which according to the user's available history on the site, determines the best available privacy policy for the user's images being uploaded.	Adaptive Privacy Policy Prediction (A3P) system	Anna Cinzia Squicciarini **[2]**
[3]	Real Cases On Image Morphing social sites as a source of image.	To make aware users about Their significant Images	Defamation issue by image morphing,	N/A	http://www.thehindu.com/news/ [3]

Table 2 shows the critical analysis of the above discussed research work.

3. Problem Definition

We evaluated the impact of presenting notifications on feedback that users provided with uploaded or shared. The notifications were based on qualitative comparisons of users' artefacts against a representation of both expert knowledge and a set of common misconceptions. Following are the problem for which this research work is proposed. We demonstrate that our approach can successfully be deployed in the social network profile to generate notifications that help the genuine user direct their attention more effectively to provide. Relevant feedback to their posts each and every movement about the post that we going to demonstrate. Now as such procedure or way is formally defined of social network multiple types of issues are encountered after the uploaded or shared post by up-loader, and issue of downloading, modifying or sharing by downloader (close friend) to third person as an unauthorized access without a single hint to the uploader, so in the following research work we are going to propose the new, simple and reliable procedure or technique for investigating issue behind shared post. We have described the problem definition using figure 2 as above.

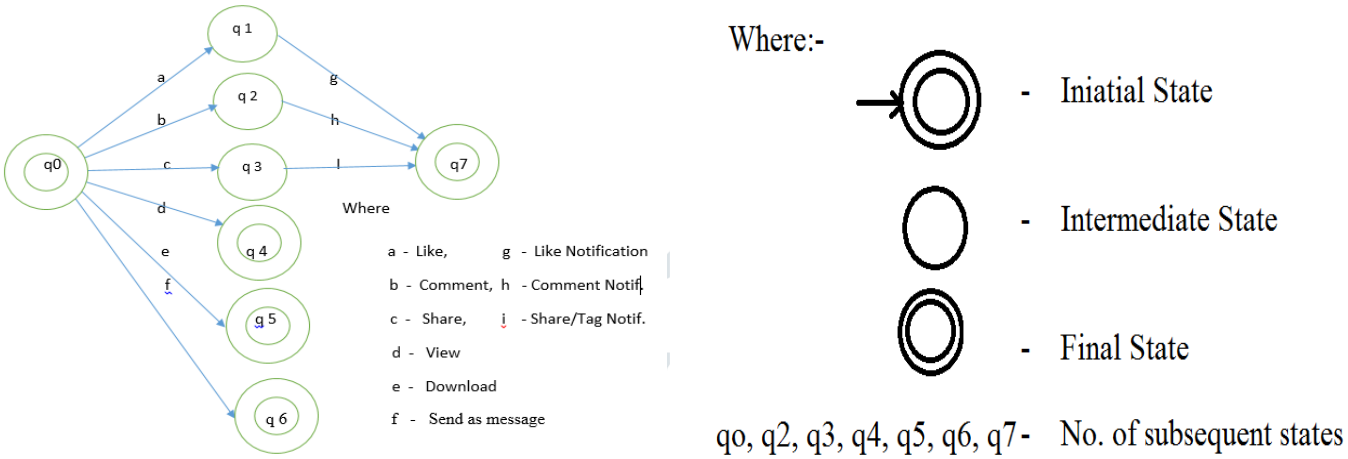

Figure: 2 Problem Definition for Existing System

In Figure 2 we shown that the q0 and q7 are accessor and uploader respectively for the image. Likewise q1, q2, q3, q4, q5, q6, are action states that would be performed by user B we named it as accessor. State q1, q2, q3 denotes to action Like, Comment, Share- Tag, respectively are intermediate states that ending on states q7 by notification, whereas the State q4, q5, q6, belongs to final state as unbeknownst to uploader. These problems are –

3.1.1. Viewed

There is seen by what amount of people and the certain people that have viewed post in other groups however, I'm not able to do that in any of my groups. I'd like exact instructions on how to perform this action.

3.1.2. Downloaded

There do not occurs the notification when the people downloading the particular post from uploader's post or timeline as unbeknownst to himself.

3.1.3. Private post converted as a public –

The uploader uploads certain post as private but it makes turn into public by downloader as if he/she is uploading that downloaded post as on his social network accountsub sequently private post converted as a public to his friends connected on Facebook which whom the genuine uploader may not be wanted to share. Without the uthorization as shown in figure 4. Private post converted as a public.

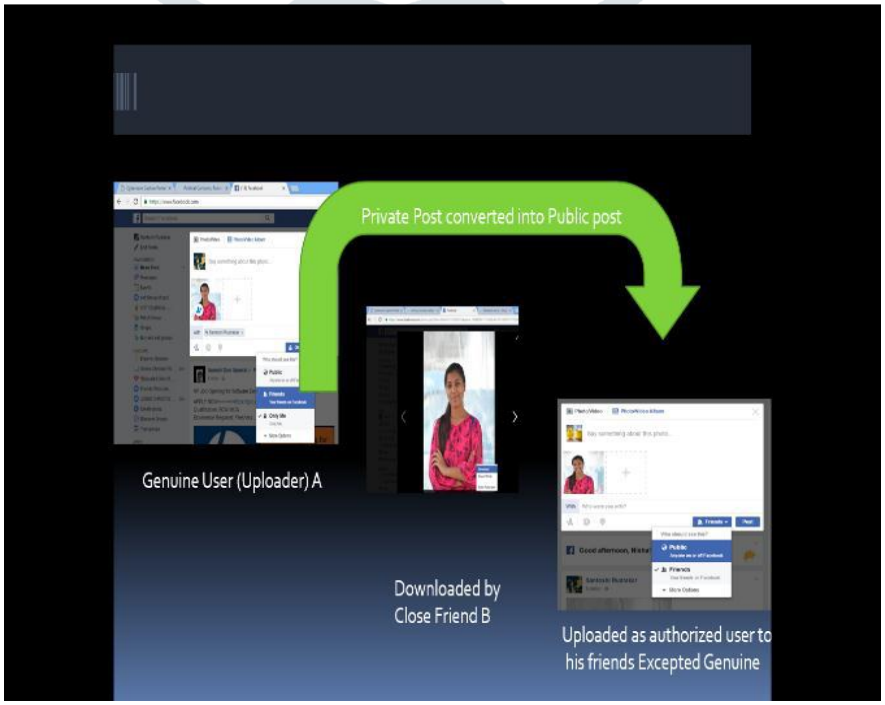

Figure 3. Private post converted as a public

4 Proposed Work

4.1. Identifying the special issue

As such procedure or way is formally defined for social network multiple type of issue are encountered after the uploaded or shared post by uploader, and issue of downloading, morphing or sharing by downloader (exist in friendlist) to third person as an unauthorized access without a single hint to the uploader, so in the following research work we will try to propose the new, simple and reliable procedure or technique that would be have adequate solution for issue behind shared post which will be prominent to keep awaken to the uploaders about their uploaded post.

4.2.Easy evidence collection and maintaining statistics for the particular post

We are going to identify the information of the downloader, by which we can get lots of facts and data that can be used as digital evidence and maintaining statistics for the particular post whoever performed whatever activity.

4.3. Solving the problem of anonymity [20]

As we stated the problem of anonymous downloading or image morphing and uploading that same shared post of genuine uploader by the downloader while this genuine uploader have no knowledge behind these anonymous activities of downloader [16]. In above section, in the research work we are going to deal with that problems of having none of the knowledge about the activity done as anonymously, and we have been assessing the adequate solution to overcome this problems.

5. Proposed Architecture

5.1. Architecture: In Figure 4 we shown that the q0 and q7 are accessor and uploader respectively for the image. Likewise q1, q2, q3, q4, q5, q6, are action states that would be performed by user B we

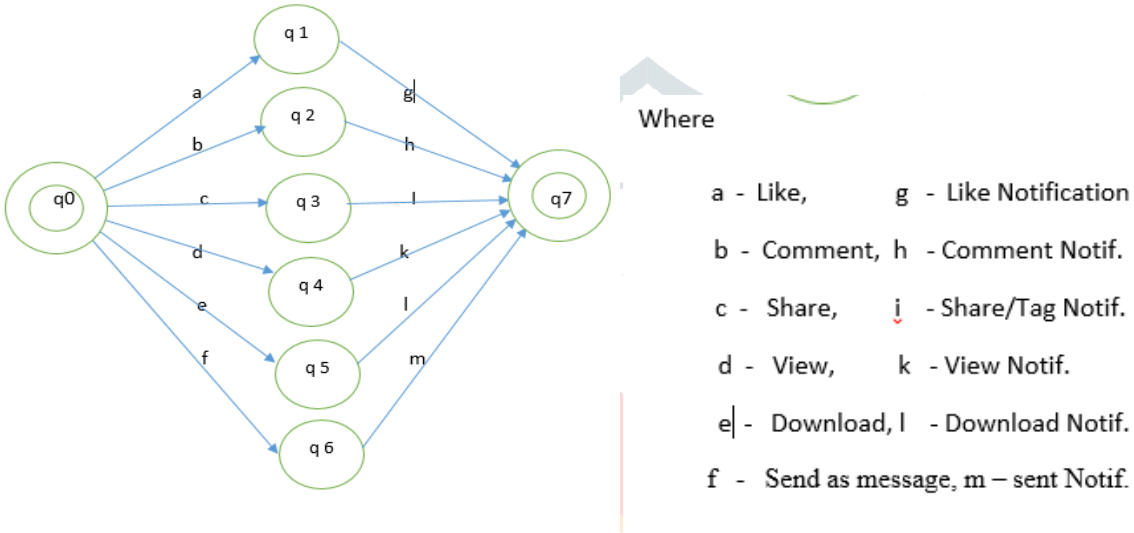

Figure 4.
Proposed Architecture

accessor. State q1, q2, q3 are denoting to action Like, Comment, Share and Tag, respectively are intermediate states that ends on states q7 by notification.

In the state diagram Figure 4 the States q4, q5, q6, have drawn further and ends on the q7 likely to be q1, q2, q3. So that uploader q7 must be have notification of these actions kl, m as post viewers, downloader, sender to the uploader respectively.

5.2. Advantages of Proposed System

Unlikely to existing system in this dissertation we are providing adequate solution for present issues in social media website whereas we are taking an example of Facebook as social networking site and have simulation using a website which is just used for presenting our implementation work. Within this proposed system there are following benefits pointed below-

1. The genuine uploader of an image user will have been notification about more action that would be going to performed on their uploaded post, these action are Download, View and Send Image as to particular friend.

2. The genuine uploader would have statistics about the Downloaders in their notification field, so that he / she would have information about that who one have downloaded their uploaded image permanently. If uploader deleted this shared image , from social media so that none of the social media friend do access it, while downloader have even exit that image as he downloaded that image and have it permanently, even though the uploader have no knowledge that someone(downloader's identity) have that erased image that had been shared on social media.

3. This additional notification statistics will be helpful for forensics investigation if there is any crime aspects with respect to the uploaded image. It will be reduce the investigation time if there is any kind of compliance or advisory report.

4. Notification Generation on Send as Particular Friend was very crucial issue that even if uploader posted an image with setting up visible privacy as available on Facebook as for Friends, subsequently the uploader was having notification about what like, comment, or sharing to that image. Issue was arising when the uploader's friend social media FriendList Sends that image as particular Friend who is not in the FriendList of uploader, consequently the Uploader's image converted into publicly even though besides of privacy settings. So our research work will be helpful to have knowledge about to whom all his/or her uploaded image has been sent.

6. Proposed Methodology

6.1. Elaboration for Flowchart

In this dissertation our methodology follows to previous concept even though it generates notification for View, Download, Send as message to the image on social media account as like as previous actions Like, Comment, Share and Tag follows to notification. We have given a working algorithm in 6.2 for the dissertation using figure 5 flow diagram for proposed

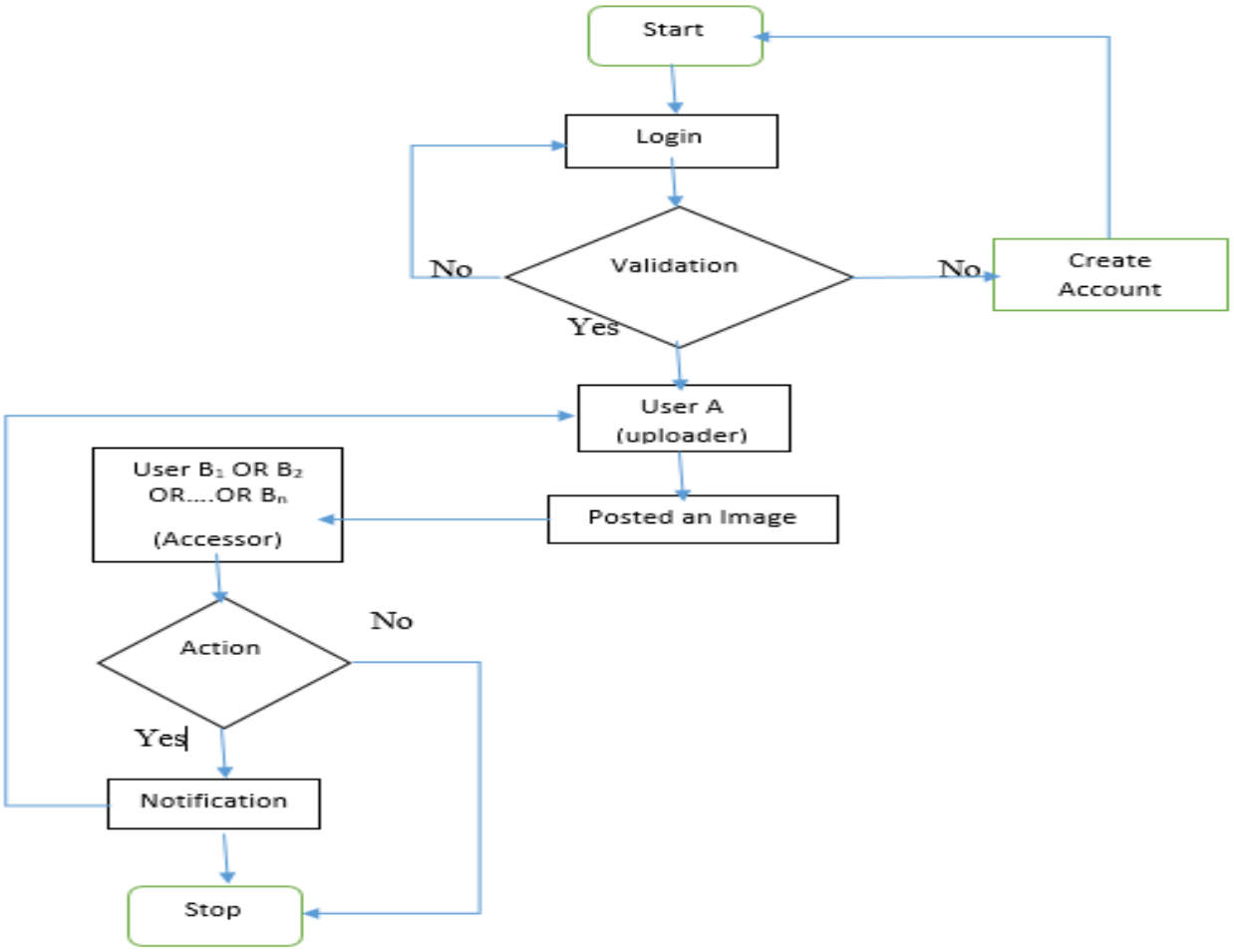

Figure 5. Flow Diagram for Proposed Method

method. Functionality methodology of our work is follows the flow graph in figure 5 and the algorithm consequently shown below in 6.2 as well.

6.2 Proposed Algorithm

1. Create an Account.
[in Social network website];
if does not exist.
2. Login to Account, If user valid.
3. Post an Image by User A (Uploader).
[for connected friends User B1 AND B2 AND-……. AND Bn.]
4. Generate Notification; For each Action ;
Where
Action := Download OR View OR Send as message to the Image.
[performed by User B1 OR B2 OR ……OR Bn]
else
Stop Process.
5. Repeat 3 to 4.
[for each Posted Image by Uploader].
6. Exit.

6.2 Result

In this experiment we are implementing scenarios for establish more security and awareness that is occurring in social media websites till today. We are providing the simulation on social media website Facebook. In our experiment the basic functionality is similar to the social media website Facebook. Consequently our implementation phases with following to flow diagram figure 5 and algorithm shown above in 6.2. The up-loader have been posted only for close friends. In this dissertation, we have given the adequate solution on privacy breaching of the uploaded post as unbeknownst to genuine uploader by notification generation method that is already enabled for some options especially in Facebook. To have furthermore security in uploaded post there can be enabled additional notification corresponding to exploding the uploaded image by generation notification so that uploader may take required action or report to cops and advisors.

To work in "Social Network Analysis on Special Issue and Solution" we want to improve the efficiency and effectiveness of evidence collection and going to collect the digital evidences from one computer system of a specific one, who visitor of social networking profile or shared post only, or much more modification done on it, In order to detect the specific activity with shared post and providing the anonymous identity to the genuine operator using notification.

1. Privacy issue on social networking site
2. Oriented on shared or uploaded post.
3. Anonymity identification.
4. Notify to the genuine Uploader to the specific activity, done by the certain people with their post.
5. Maintain the statistics.

7. Conclusion

This research has analyzed previous research which is dedicated for Social Networking sites issues some of these are privacy, image morphing, defamation anonymity detection issues, The users may be unaware about some of the bomb activities is done with their post by sharing post indirectly to the others users by downloading and sharing the genuine post except him/her. There might be serious disclosure while the Social Network provider doing their best to provide security to the users. With this dissertation it is come out the issue of anonymity of downloaders although the uploader has posted only for close friends.

8.REFERENCES

[1] Arjun K.P.1, Aswathy Achuthshankar2, Aswin Achuthshankar3, Soumya M.K.4, Sreenarayanan N.M.5, Priya V.V.6, Faby K.A.7 "PROvacy : Protecting Image Privacy in Social Networking Sites Using Reversible Data Hiding". IEEE , 2016.

[2] Anna Cinzia Squicciarini1, Member, IEEE, Dan Lin2, Smitha Sundareswaran3, and Joshua Wede4. "Privacy Policy Inference of User-Uploaded Images on Content Sharing Site" .IEEE Journal 2015.

[3] http://www.thehindu.com/news/1 SALEM, JUNE 29, 2016 10:05 IST, http://timesofindia.indiatimes.com/city/jaipur2 TNN | Jun 29, 2015, 12.09 PM IST.

[4] Krishna P.1 gummadi@mpi-sws.org Balachander Krishnamurthy Germany Yabing Liu 2 Northeastern University Boston, MA, USA ybliu@ccs.neu.edu MPI-SWS Saarbrücken/Kaiserslautern, "Analyzing Facebook Privacy Settings: User Expectations vs. Reality".

[5] Dumas, G.1, Serfass, D. G.2, Brown, N. A.3, and Sherman, R. A4. (2014). "The Evolving Nature of Social Network Research: A Commentary to Gleibs" (2014). Analyses of Social Issues and Public Policy, 374- 378.

[6] Fuchs, C. (2011). An alternative view of privacy on Facebook. Information, 2(1), 140-165.

[7] Alan Mislove1, bala@research.att.com Northeastern University Boston2, MA, USA amislove@ccs.neu.edu. ATandT Labs–Research Florham Park, NJ, USA.

[8] Amanda J. Cox1, Yeslam Al-Saggaf2, Kate McLean3 Charles Sturt University, Australia,"Social Networks Lack Cues To Impede Divulgence Of Personal Information" 10th International Conference on Culture, Technology, Communication. London, UK, 15-17 June 2016, pp. 63-72.

[9] Kosinski M.1, Stillwell D.2, and Graepel T.3 (2013). "Private traits and attributes are predictable from digital records of human behaviour". Proceedings of the National Academy of Sciences, 110(15), 5802-5805.

[10] Buccafurri , F.1, Fotia, L.2, Lax, G.3, and Saraswat, V4. (2016). "Analysis-preserving protection of user privacy against information leakage of social-network Likes". Information Sciences, 328, 340-358.

[11] Boyd, D. (2007). "Why youth (heart) social network sites: The role of networked publics in teenage social life". MacArthur Foundation series on digital learning–Youth, Identity, and Digital Media Volume (ed. David Buckingham). Cambridge, MA: MIT Press, 119-142.

[12] Zhang, C.1, Sun, J.2, Zhu, X.3, and Fang, Y4. (2010). "Privacy and security for online social networks: challenges and opportunities". Network, IEEE, 24, 13-18.

[13] Fred Stutzman1 , Jacob Kramer-Duffield2 ."Friends Only: Examining a Privacy-Enhancing Behavior in Facebook". Atlanta, GA, USA,April 10–15, 2010.

[14] Sowmya V¹, Sripriya N² ."Inference Rules of User Uploaded Imageson Social Network Sites".International Journal of Innovative Research in Science,Engineering and Technology Vol. 5, Issue 3, March 2016.

[15] Advances in Social Networks Analysis and Mining (ASONAM)", 2014 IEEE/ACMInte rnational Conference.

[16] Christopherson, K. M.. (2006). The positive and negative implications of anonymity in internet social interactions: On the internet, nobody knows you're a dog. Computers in Human Behavior. (journal article)

[17] Cain, Jeff, and Fink, Joseph L.. (2010). Legal and ethical issues regarding social media and pharmacy education..American Journal of Pharmaceutical Education, 74 (10), Article 184. (journal article)

[18] Hobgen, G.. (2007). Security Issues and Recommendations for Online Social Networks. (techreport)

[19] Hodge, Matthew J.. (2006). The Fourth Amendment and privacy issues on the 'new' internet: Facebook.com and MySpace.com. Southern Illinois University Law Journal, 31.

[20] Christopherson, K. M.. (2006). The positive and negative implications of anonymity in internet social interactions: On the internet, nobody knows you're a dog. Computers in Human Behavior. (journal article)

[21] Albert-Laszlo Barabasi. "Linked. The New Science of Networks", 2014.

[22] Duncan Watts. "The Science of a Connected Age", 2004 .

[23] Michael Hay, Gerome Miklau, David Jensen, Philipp Weis, et al.. "Anonymizing Social Networks" (2007) Security and Privacy, 2009 30th IEEE Symposium on.

[24] Anqi Andrew Huang, Jonathan Warman, Josh Wiseman, Eugene Letuchy," Scaling notifications of events in a social networking system " (2013).