Mitigating Cybercrime and Online Social Networks Threats in Nigeria

Adu Michael K, Alese Boniface K and Adewale Olumide S.

***Abstract*: Many internet and Online Social Networks (OSN) users in Nigeria are victims of criminal activities perpetrated by those who take advantage of anonymity of their identities to harm users both in the virtual and in the real world on daily basis. Numerous security risks that exist in these networks include privacy violations, identity theft, and sexual harassment among others. A review of some of the different security and privacy risks which threaten the wellbeing of online social networks users including children is presented. This paper proposes a design that authenticate and uniquely identify every internet user most especially those on social networks. This paper further elicits inability to identify perpetrators as one of the reasons for the growing menace. A system that enables internet users' activities to be monitored in order to curb threats to online social networks in Nigeria is offered. It requires redefining the operations of Internet Service Providers (ISPs) that provide access for users on the internet and the National Communication Commission (NCC), a government body that oversees the information and communication system in Nigeria. A central database (cloud) is proposed to be hosted by the National Communication Commission with users' "activity log" feature. Users can send a request on any suspecting associate (pal) on social networks to get confirmation on genuine identity of the individual.**

Index Terms*:* Activity log, Anonymity, Cloud, Online Social Networks, Security and Privacy Risks,

I INTRODUCTION

In Nigeria, Social Networking sites such as facebook, Google+, Linkedln, Twitter et cetera, have gained a lot of popularity especially among the younger generations. Many of the users of social networks today are not aware of the threats associated with it. As a result of the larger user base and large amount of information available in social networks, it has become a potential channel for attackers and criminals to exploit.The threats include Identity Theft, Social Network Spam, Social. Network Malware, and Physical Threats. Social Networks can be described as web applications that allow users to create their semi-public profile. Semi-public profile is a profile that some information is public and some is private, it enables communication with those who are friends and thereby build an online community. Most importantly, it enables direct communication with these associates (pals) without restriction. Therefore large amount of their private information is shared in this social network space. The information shared ranges from bio-data information, contact information, comments, images, videos, et cetera

Today, threats to Online Social Networks (OSN) are so pervasive that even academic community has not been able to provide or even suggest a holistic approach to curb the crimes often associated with internet with particular emphasis in this paper, on social networks. Efforts have been expended on identity protection that has not provided the needed results. In recent studies and from day-to-day experiences, many online social network users expose personal and intimate details about themselves, their friends, and their personality whether by posting photos or by directly providing information such as a home address and a phone number. As the use of online social networks becomes progressively more embedded into the everyday lives of users, personal information becomes easily exposed and abused. Information harvesting, by both the online social networks operators and by third-party commercial companies has recently been identified as a significant security concern for Online Social Networks (OSN) users.

II THREATS OF SOCIAL NETWORKS

The threats to social networks are becoming major setbacks for the technology of internet and its applications. The perpetrators use the online social networks (OSN) infrastructure to collect and expose personal information about users and their friends. They often lure users into clicking on specific malicious links. They include inference attacks, de-anonymization attacks, link reconstruction attacks, click jacking, Sybil attacks, socware, fake profile and identity clone attacks et cetera.

Manuscript received March 20, 2014; revised April 3, 2014..

Adu Michael Kolade. Author is with the Department Computer Science, Federal Polytechnic, Ado-Ekiti, Nigeria. Phone: +2348066714060 Email: memokadu@yahoo.co.uk

Alese Boniface Kayode. Author is with the Department Computer Science, Federal University of Technology, Akure, Ondo State, Nigeria. Phone: +2348034540465 Email: bkalese@futa.edu.ng

Adwale Olumide Sunday. Author is with the Department Computer Science, Federal University of Technology, Akure, Ondo State, Nigeria. Phone: +2348039617525Email: adewalekalese@futa.edu.ng

ISBN: 978-988-19252-0-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

III INTERNET FRAUD

Cybercrime generally can be defined as a crime committed or facilitated via the Internet. It is any criminal activity involving computers and networks. It can range from fraud to unsolicited emails (spam). It can include the distant theft of government or corporate secrets through criminal trespass into remote systems around the globe [1]. Cybercrime incorporates anything from downloading illegal music files to stealing millions of dollars from online bank accounts. It also includes non-monetary offenses, such as creating viruses on other computers or posting confidential business information on the Internet. Knowing the facts, trends, and growth is critical to crime prevention efforts and protecting personal data in public and private sectors. This also helps in the creation of tools and strategies to combat cyber criminals. By virtue of the tools being used today to commit cybercrimes, criminals are now more anonymous and thereby difficult to identify.

Threats to Online Social Networks

A. Native Trust

This crime is often perpetrated on children who are more susceptible to trusting social network friends without question. The said friend's profile may really be a mask for sinister intentions. Not only the children are affected by this act, it is not uncommon for adults too to build up relationship with friends they do not know but trust. The criminals here can steal money and information from their unsuspecting victims.

B. Click Jacking

Click jacking is a malicious technique which tricks users into clicking on something different from what they intended to click. This method involves manipulating unsuspecting user to click an option that triggers the attackers' intention [2].

This often can results into attacker posting spam messages on to facebook or other social network account of the user. This illegal act involves the hacking of a personal account using an advertisement for a viral video or article. Once the user clicks on this, the program sends an advert to the person's friend through their account [3].

C. Cyber bulling

Cyber bulling (also refer to as cyber abuse) can be in form of posting rumors or lies about the victim in a public forum, using text messages or emails to send threatening messages, uploading videos to youTube that embarrass their victims or sharing the victim's personal information in a public forum et cetera. It is simply bulling that takes place within technological communication platforms, such as emails, chats, mobile phones conversations, and online social networks by an attacker who uses the platform to harass his victim by sending repeated hurtful messages, sexual remarks, or threats. By publishing embarrassing pictures or videos of the victim; or by engaging in other inappropriate behavior e.g spreading cruel rumors about the victim and sharing embarrassing pictures with the victim's network of friends. Cyber bulling usually affects children and teenagers

D. Fake Profile

Fake profiles are automatic or semi-automatic clone profiles that mimic human behaviors in online social networks. In many cases, fake profiles can be used to harvest personal user data from OSNs. By initiating friend requests to other users in the OSN, who in many cases accept the requests, the fake profile can gather a user's private data which should be exposed only to the user's friends.

E. Identity Clone Attacks

Using this technique, attackers duplicate user's online presence in the same network, or across different networks, in order to deceive the cloned user's friends into forming a trusting relationship with the cloned profile. The attacker can use this trust to collect personal information about the user's friend or to perform various types of online fraud [4]

F. De-Anonymization Attacks

In many online social networks like Twitter and Myspace, users can protect their privacy and anonymity by using pseudonyms. De-anonymization attacks use techniques such as network topology and user group memberships to uncover the user's real identity.

G. Online Predators

The image of Internet predators in the media is of an adult man seducing and tempting innocent young boys and girls through the collection of personal data and the impersonation of being a friend to these youngsters, all the while hiding his sexual intentions until the actual meeting, which likely involves rape or kidnapping.

H. Inference Attacks

Inference attacks in online social networks are used to predict a user's personal and sensitive information that the user has not chosen to disclose, such as religious affiliation and sexual orientation. This type of attacks can be implemented using data mining techniques combined with publicly available OSN data, such as network topology and users' friends' data. They tested their techniques and inferred different Facebook user's attributes, such as educational information, personal tastes and preference, and geographic information. The majority of unprotected information can be mined for targeted advertising and can be a means to more harmful end such as identity theft.

V PREVIOUS ATTEMPTS AT SOLVING CYBERCRIME AND SOCIAL NETWORK THREATS

Cybercrime prevention can be achieved fairly quickly and in a cost-effective manner when armed with a little technical advice and common sense. Many cybercrime attacks can be avoided. Similar to target hardening for a residence or a business (for example, lights, locks, and alarms), the more difficult it is for a cyber-criminal to successfully attack a target, the more likely he or she is to leave it alone and move

ISBN: 978-988-19252-0-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

on to an easier target. Previous research works have identified the following as the basic ways that cybercrime can be prevented [5]

- Keep computer system up-to-date
- Secure configuration of the system
- Choose a strong password and protect it
- Keep firewall turned on
- Install or update antivirus software
- Protect personal information
- Read the fine print on website privacy policies
- Review financial statements regularly

Online social network users are facing prevalent and varied security and privacy threats. There are many software solutions and techniques today which have been put in place to assist OSN users in defending themselves against these threats. The following recommendations have been put forward to help users who want to protect themselves in any of the OSN accounts.

Remove Unnecessary personal information:
Adjust privacy and Security Setting
Do not Accept Friend Requests from Strangers.
Do Not Trust Your OSN Friends

VI PROPOSED INVENTION

The pace of technology requires that users should be ever-vigilant about the threats to online social networks however the ultimate solution is a holistic approach to identify and make prosecution of offenders possible. The motivation for this research work is borne out of the fact that any attempt at preventing cybercrime must identify the tool being used by the criminals, which is the internet. However, it seems no critical work has been done to reveal the identity of criminals rather preventive measures are being proposed by researchers. The criminals too are working hard if not harder to beat every preventive hurdle on their way. It is therefore reasonable that any enduring method of preventing this crime must reveal the identity of the perpetrators. The more anonymous they are, the more difficult to prevent [6]. Potential risky behaviors may include direct online communication with strangers, use of chat rooms for interactions with strangers, sexually explicit talk with strangers, giving private information and photos to strangers, etc. All children living with these kinds of issues are at a higher risk of sexual abuse on the internet or through online initiated encounters. Regardless of whichever way the crime is committed, the criminal has unique identity that can also be associated with the machine on which the crime is being performed. The goal of this research is to identify how to trace these identities and addresses to their owners. However, this may be an almost unachievable task as the internet itself does not reside on a particular machine and Internet users have access to various tools with which they can hide their identity on the internet.

These tools includes; Proxies, tunnels, VPN (Virtual Private Network) and Virtual machine which an internet user may employ in order to hide any trace of his activities on the internet. Despite all these challenges, the best method/approach to curbing cyber crimes is to initiate control from the time and the source of internet service connectivity. This is proposed in this work. This source is usually the internet service providers (ISP) that provide internet service to their subscribers in different forms. This system requires that Internet Service Providers (ISPs) to register every internet subscriber at first attempt to surfing the internet. Once it is done by any ISP, registration is no longer necessary when trying to use the internet through another ISP. The information collected about any individual is hosted in a centralized database maintained by the National Communication Commission (NCC) in a cloud. Collecting information that truly validates an individual involves; Collecting subscribers Bio-data (e.g. Full name, Age, etc), Full address of residence, Biometric Information (e.g. Fingerprint), National Identity Card Number and a Passport Photograph.

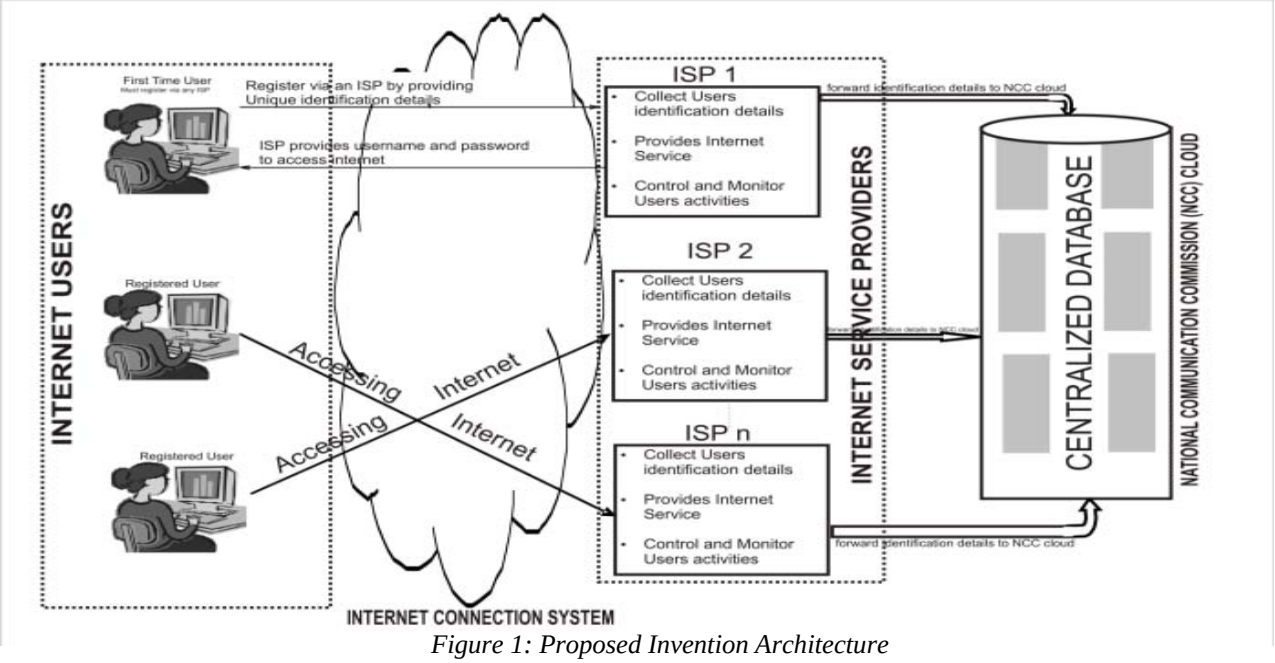

Figure 1: Proposed Invention Architecture

ISBN: 978-988-19252-0-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

VII SYSTEM IMPLEMENTATION

Implementing this work, a small scale ISP is created using a laptop with wireless data card. A Virtual Router application is developed and configured to mimic a real life router device and to suit the project implementation needs. A signup portal is also created to allow internet users to register with the ISP and have easy sign in on subsequent connections "this is preferable instead of asking the user to go through many processes before browsing which could be frustrating". The signup asks users for unique identification information which will include the users' bio data and government issued identification number like National Identity card, voters card et cetera. It can as well accept any form of biometric authentication such as finger print. After the signup, the a user will now have a unique username and password "chosen by him" that he can now use for authentication before having access to the internet which will be used to reference him with an IP address that his system is using thereby attaching him to any criminal report related to his record and the IP address at any point in time at the National Communication Commission (NCC) cloud which is the central database for all ISPs. The database will have an admin panel where detailed information about all users' activities can be sort for and accessed on demand.

To fully monitor the users' activities on the social network, an "activity log" feature will be added to it. The activity log will save all the users browsing history (e.g list of websites visited, names used in social networks accounts, chat history, messages, et cetera) in a central server with the National Communication Commission (NCC). This will make it easy for the security admin to search for any suspected browsing activity and the user that perpetrated the act using the activity history to find the original details of the fraudster.

In case of taking precautions and being on a safer side, a user suspecting an associate (pal) on social network can send a request to NCC to confirm if the person he is dealing with online is not an impostor using fake profile.

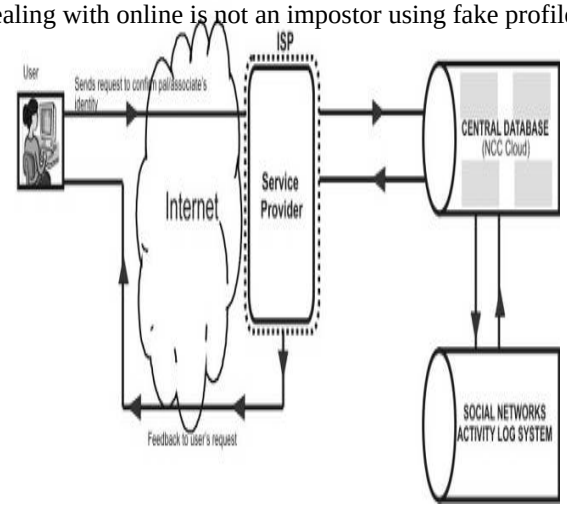

Figure 2: System Architecture with Activity Log feature for Online Social Networks Monitoring

VIII FUNDAMENTAL ISSUES

There are some fundamental issues that may agitate the minds of stakeholders concerning the proposed solution to Online Social Networks threats in Nigeria. These issues are practically technical. Modalities for addressing them are discussed as follows:

A. First issue

What happens if a criminal minded individual get access to another person's password and username?

In order to handle this, first and foremost users are expected to keep their username and password safe. Also, the system has an additional security level that sends a random generated pin code to the mobile device, email, facebook, twitter, in fact anything that can receive message that the user added while signing up. So after entering username and password, one will be asked to enter the security number received before he can be logged in fully for internet access.

B. Second issue

What happen if a user phone is down and cannot surf the internet, cannot check mail, facebook and so on?

Again, this intelligent system makes provision for user to select where he wants the security pin code to be sent and afterwards gives him a link to a *'dynamic login page'* that is linked and allowed to the mail or social network gateway. Once a correct username and password of the gateway is entered, the internet access will be given and the user's information logged.

IX CONCLUSION

Online social networks have become part of our everyday life and on the average most internet users spend more time on social networks than in any other online activities. Users enjoy using online social networks to interact with other people through the sharing of experiences, pictures, videos, and other types of information. Nevertheless, online social networks have been having a dark side issue with hackers, fraudsters, and online predators, all fond of using online social networks as a platform for procuring their next victim. In this paper, we have presented scenarios which threaten online social networks users and can jeopardize their identities, privacy and well-being both in the virtual world and in the real world. Moreover, we have emphasized certain threats which challenge the safety of children and teenagers inside the online social network cyberspace. We equally highlighted some remedies to these threats, and a range of solutions which aim to protect the online social network user's privacy and security. More importantly however, this paper proposes a design for monitoring internet users' activities in order to curbing threats associated with social networks. It requires redefining the operations of Internet Service Providers (ISPs) which will now mandate users to be authenticated before accessing internet, maintaining

ISBN: 978-988-19252-0-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

activity log that save all users' browsing history such as list of websites visited, names use in social network, chat history, messages, et cetera. A user suspecting an associate (pal) on social network can send a request to NCC to confirm if the person he is dealing with online is not an impostor using fake profile. Therefore, this paper proposes a holistic approach to curbing cybercrime and threats to online social networks.

REFERENCES

[1] Babu M., and Parishatb M.G. "What is Cybercrime" http://www.ncpc.org/resources/files/pdf/internet-safety , 2012.

[2] Benevenuto, F. Rodrigues T., Almeida V., and Goncalves M. "Detection Spammers and Content Promoters in Online Video Social Networks", In proceedings of the 32nd International ACM SIGIR Conference on Research and Development in Information Retrieval, pages 620-627. ACM , 2009.

[3] ContentWatch, "Social Networking Challenges Every Parent Should know" http/www.netnanny.com, 2013.

[4] Acquisti A.and Gross R., "Imagined Communities Awareness, Information Sharing and Privacy on the Facebook" in 6th Workshop on Privacy Enhancing Technologies, 2006.

[5] Brenner J. and Aaron S.. "Online Adults are Social Networking Site Users", http://pewinternet.org/Reports/2013/social-networking - sites/Findings.aspx,2013

[6] Danezis G., 'Better Anonymous Communications' PhD thesis, University of Cambridge, 2004.

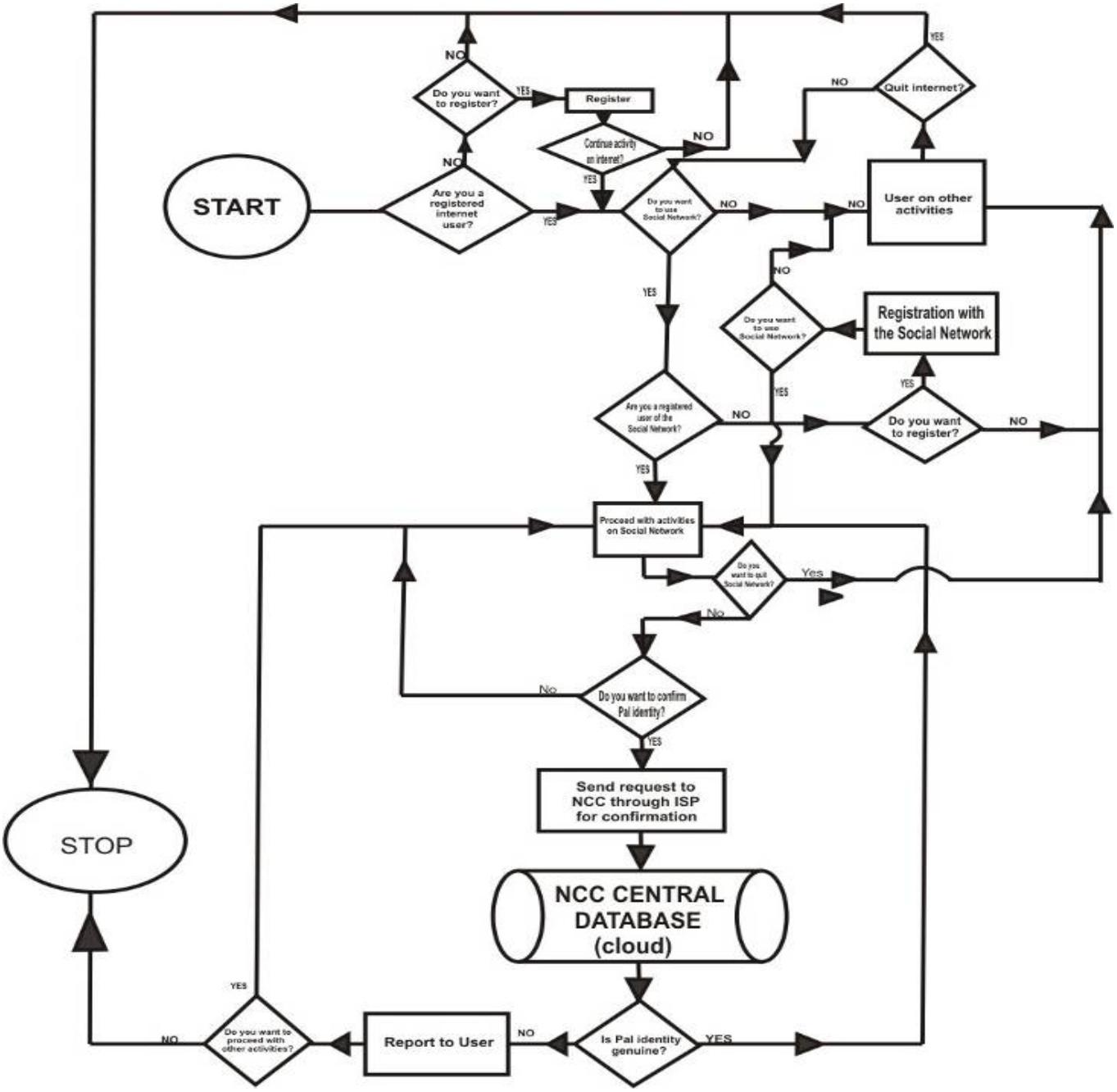

Figure 3: Flow diagram illustrating users' activities on the internet

ISBN: 978-988-19252-0-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)