# Deterring Sybil Attack in Online Communication System via Peer-to-peer Audio Visual Communication System

**[1]Lawal Olawale Nasiru., [2]Yekini Nureni Asafe., [3]Oloyede Adetokunbo Olamide, [4]Akinsola Adeniyi Folusho**
[1,3]Dept of Computer Engineering, Yaba College of Technology. [2,3]Dept of Computer Technology, Yaba College of Technology

**ABSTRACT**

**In recent time the use of communication gadgets (mobile phones, laptop, desktop etc.) and service for online communication between two parties over a long distance has become sine-qua-non. Some criminal minded people are using this online communication method to deceive their prey via proxy communication where individual claiming to be discussing is not really the one. In this paper, we focus on prevention of identity impersonation attacks in an Online Communication System. Peer-peer Audio Visual Communication System is design to enhance security through online communication system by revealing the identity of the communicators and records the communication if necessary. Embedded application system was design for mobile and desktop devices for audio visual charting using modern IT devices**.

**Keywords:** Audio Visual Communication System, Online Communication, Sybil Attacks.

Date of Submission: July 24, 2017 Date of Acceptance: Aug 07, 2017

## I. INTRODUCTION

In this era of synchronous and asynchronous virtual communication many criminals minded people has been using proxy approach to communicative with people towards perpetuating online crime by Sybil attack. The Sybil attack in computer security is an attack wherein a reputation system is subverted by forging identities in peer-to-peer networks [1,2].

An identity of an individual is the set of information known about that person., a person's identity can be a set of a name, an address, a driver's license, a birth certificate, a field of employment, etc. This set of information includes items such as a name which is used as an identifier. Impersonators claimed to have identity of the person been impersonated for the purpose of committing crime. Several cases of online fraud are associated with identity theft and impersonation via online communication.

This research work is focus on prevention of identity impersonation attacks in an Online Communication System. This study is to design a peer-peerAudio Visual Communication System to enhance security through online communication system by revealing the identity of the communicators and records the conversation of the two parties. The application system services will include system control protocols for setting up calls between two parties, reveal the pictures of the communicators, and recording their conversation if necessary.

## II. BACKGROUND TO THE STUDY

There is no doubt that use of mobile phones, computer gadgets, and Information Technologies has become means of communication among individuals, business organizations and governments across the globe. Several criminal activities have been attributed to the use of online communication system via mobile phones and other IT tools and services. Some of these activities are: spamming, credit card frauds, ATM frauds, phishing, identity theft and other related cyber-crimes [3].

Security in online communication denotes protection from online criminal activities (Adams & Blandford). Use of online communication can cause many security risks, such as loss of confidentiality and availability, the exposure of critical data, and vandalism of public information services due to identity theft [4].Usually, online communication security issues have been attributed to users' poor knowledge of security measures, improper behaviours, and lack of education [5]. In recent years, even though users' security knowledge and skills have grown, security issues such as information manipulation by impersonator and loss of confidentiality still happen from time to time [6].

## III. METHOD

This study carried out and investigation to justify the need for this research work. We conducted investigation through face-to-face communication with system administrator of online learning platform and security outfit to examine level of security threat and criminal activities in an online communication and learning system. Our investigation revealed that an attempt to obtain sensitive information from people by disguising as a trustworthy entity in an electronic communication is very rampart. Hence we concluded to design an embedded Peer-peer Audio Visual Communication System that will reveal the identity of both communicators and possibly record discussion during conversation.

The main consideration in the design of this application is based on the requirement to display user real-time pictorial identity. The application is design with keen compliance with the flowchart in figure I.

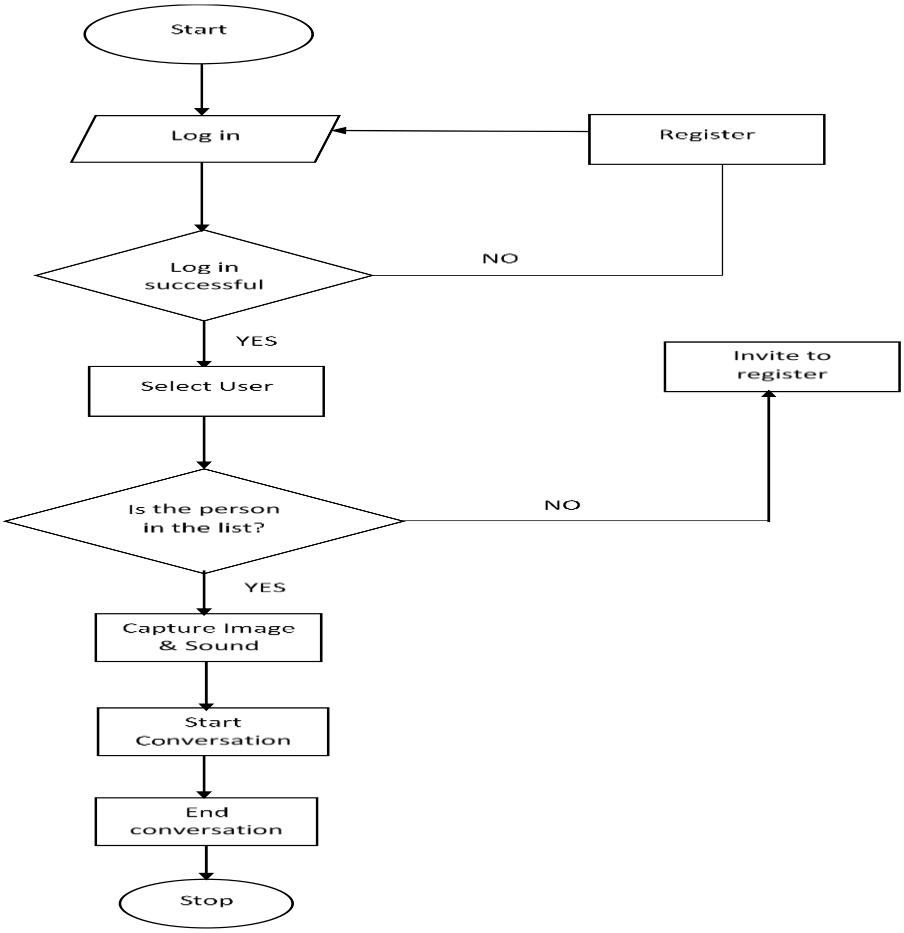
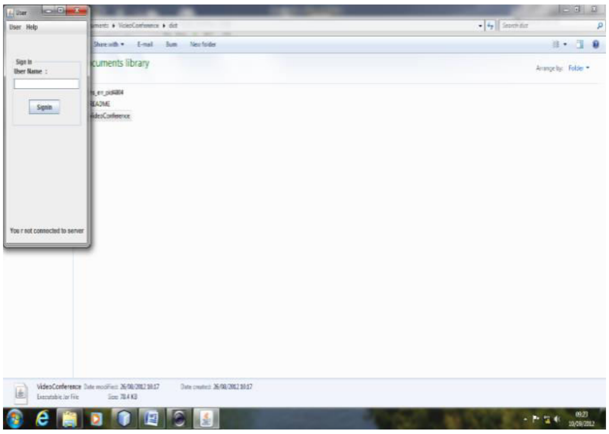


Figure I. Proposed System Flowchart

The application is PEER TO-PEER system. After the application have been installed on both party's communication devices there must be connection via wired or wireless connection.

The application was designed and tested to conform with the researcher focus to enhance online communication toward prevention of impersonation crime in an online communication. The diagrams figure II-VI gives the pictorial representation of each phases of testing and implementation.



You r not connected to server

Figure II. User Interface of the proposed system

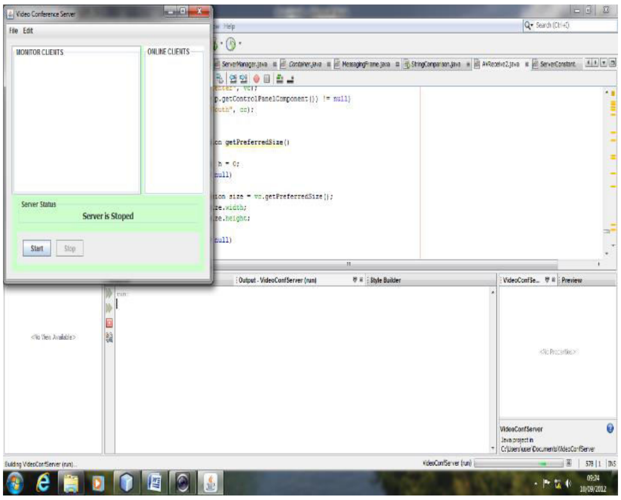


Figure III. User Interface After Log in

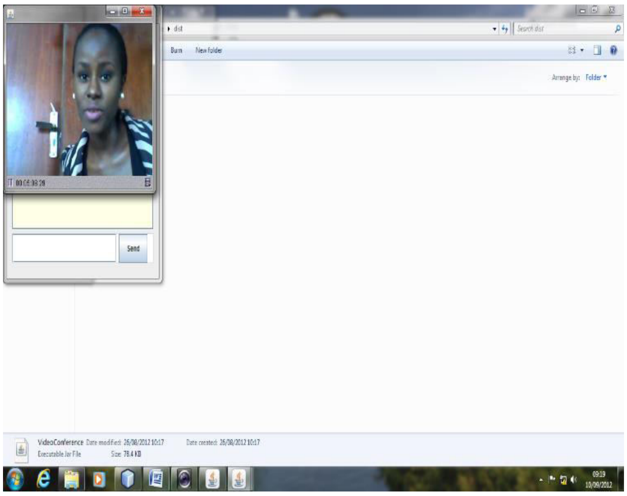


Figure IV. User Interface Showing Peer I

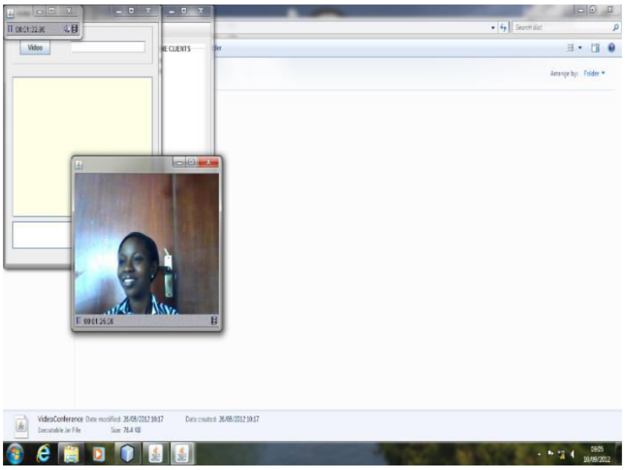


Figure V. Figure IV. User Interface Showing Peer II

## CONCLUSION

In this research work we proposed a strategy to deter Impersonation in an Online Communication. The solution is to achieve the required security towards prevention of identity impersonation attacks in an Online Communication System. Peer-peer Audio Visual Communication System was designed to enhance security through online communication system by revealing the identity of the communicators and records the conversation if necessary. This application system can be used by business organization to deter impersonation in any synchronous communication system.

### Reference

[1.] Wang, Liang; Kangasharju, Jussi (2012). "Real-world sybil attacks in BitTorrent mainline DHT". IEEE GLOBECOM. Retrieved 30 September 2013.

[2.] Wang, Liang; Kangasharju, Jussi (2013). "Measuring Large-Scale Distributed Systems: Case of BitTorrent Mainline DHT" (PDF). IEEE Peer-to-Peer. Retrieved 30 September 2013.

[3.] Yekini N. Nureni, Aigbokhan E. Edwin, Akinwole A. Kikelomo, Alakiri O. Harrison 2016: E-Infrastructure and E-Services Security Platform Using Multifactor Cybercrime Deterrent System: A Conceptual Model iSTEAMS Multidisciplinary Cross-Border Conference Accra Ghana 2016

[4.] Graf, F. (2002), Providing security for eLearning. Computer & Graphics, 26(2), 355-365.

[5.] Weippl, E., & Ebner, M. (2008). Security privacy challenges in e-learning 2.0. In World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education (Vol. 2008, No. 1, pp. 4001-4007).

[6.] Dietinger, T. (2003). Aspects of e-learning environments (Unpublished doctoral thesis).
Institute for Information Processing and Computer Supported New Media (IICM), Graz University of Technology, Austria.