

**Communique of the 2nd International Conference and Workshop of
Computer Networks, Infrastructure Management and Security (CoNIMS)
Research Group of the Department of Computer Sciences, Faculty of
Science, University of Lagos, Nigeria held at Arthur Mbanefo Digital
Research Centre, University of Lagos, Nigeria
between 22nd – 24th October, 2019.**

1.0 Introduction

Computer Networks, Infrastructure Management and Security (CoNIMS) Research Group of the Department of Computer Sciences, Faculty of Science, University of Lagos held her second edition of International Conference and Workshop at Arthur Mbanefo Digital Research Centre, University of Lagos, Nigeria between 22nd – 24th October, 2019. The theme of the second Annual conference was “*Emerging Security Issues in E-Services in the 21st Century*”.

2.0 Overview

The conference, which was scheduled for three days, had on the first day a hands on workshop on *Cyber Security*. The workshop was presented by Mr Emmanuel Obongha Okoi of CYSEC. Mr. Okoi is a Certified Ethical Hacker from both Buckmark Institute of Technology, Kenya Nairobi and India Koffi Anan ICT Centre of Excellence in ACCRA, Ghana. The presenter used one of the main cybersecurity tools - kali-linux-2018.4-amd64 for the training, which was well attended by nearly all the participants. The remaining two days witnessed the presentation of papers.

A total number of fifty-seven participants attended the conference. This figure included the members of local organizing committee, principal officials of the university, volunteers, as well as postgraduate students. Thirty-five of these participants were from the University of Lagos, three participants from the Federal University of Technology, Minna (FUT Minna), three participants from the Administrative Staff College of Nigeria (ASCON) Badagry, one participant from the Federal University of Technology Akure (FUTA) and one participant from the Federal College of Education, Technical (FCE,T) Akoka.

Prof. Adenike Osofisan chaired the opening ceremony. The Vice-Chancellor, University of Lagos, Professor Oluwatoyin T. Ogundipe, was unavoidably absent. The Dean, Faculty of Science, Professor Adedotun A. Adekunle who was the Host also presided over the opening ceremony. The Keynote speaker was Mr. A.P.S Arogundade the President, Information Technology Systems and Security Professionals (ITSSP); he was, however, represented by Dr. (Mrs)

Titilola Akinlade. The lecture, titled "*Emerging Security Issues and Challenges of Cloud Computing in Nigeria*", was well delivered and caught the attention of the audience which later culminated into questions, comments and contributions from various participants during the question and answer session. A welcome address was delivered by Professor Charles O. Uwadia the conference Chair and research group leader.

The technical session was divided into six groups as follows: *Cyber Security, IT & National Development, Social Networks, Network Intelligence, Network Safety and IoT & Big Data*. The first two sessions were held on Wednesday, 23 October 2019 immediately after the opening ceremony, while the remaining four sessions were held on Thursday 24, October 2019. Each of the six sessions was chaired by Dr. T. Akinlade, Dr. F.A. Oladeji, Dr. O.A Sennaike, Mr. B. Aremo, Dr. O.B. Okunoye and Dr. A.P Adewole. A total of 10 minutes was allocated to each of the presenters after which questions were randomly taken from the participants. Relevant and appropriate comments and observation were allowed after the presentation.

3.0 Highlights of workshop

As previously stated, the main conference was preceded by a one-day workshop on Cyber Security on Tuesday, 22 October 2019. The workshop was conducted by Mr Emmanuel Okoi. He started by introducing himself and what his company does in the area of Cyber Security. He explained various tools being used for ethical hacking. Apart from ethical hacking, he briefly explained network security, penetration testing, websites vulnerability checks, system threat/virus and network assimilations.

He thereafter assisted the participants to install kali-linux-2018.4-amd 64 and other allied software tools that were used for the training. The workshop provided immense opportunity for the participants to learn how cyber criminals are using the tools nefariously for their selfish interests. During the workshop, participants were able to learn different techniques being used by Cybercriminals to unethically hack into public and private networks. He also exposed how genuine and fake Uniform Resource Locators (URLs) can easily be identified.

Mr Emmanuel Okoi used the occasion to admonish all the participants on the need to abide by the moral and legal requirements of the training. He enjoined the trainees to be wary of unethical or sharp practices during and after the training. He alluded to the fact that a well-trained Cyber Security expert could make money illegally if the acquired knowledge is used unethically. He,

therefore, cautioned all on the damage such action could cause to the reputation and image of anyone caught in the act. Finally, the trainer solicited collaboration in the area of research as he promised to leverage his practical knowledge to support and enhance research in the area of information security.

The feedbacks from the audience satisfactorily revealed that the workshop was well organised and the participants immensely benefited from the hands-on training.

4.0 Highlights of Plenary Sessions

A total of fifteen papers (15) were finally accepted for the conference after favourable reports and acceptance recommendations were received from at least two independent reviewers. The conference was split into six (6) plenary sessions as follows: session 1 was themed “Cyber Security”. Two papers titled – *A framework for the performance evaluation of e-mail spam detection* and *A digital forensics investigation model that incorporates digital chain of custody for its integrity and authenticity* were presented.

The second session was themed “IT & National Development”. During this session, two papers were presented. A paper titled “*Development of a framework for the determination of an asset as Critical National Information Infrastructure (CNII)*” authored by Victor E. Kulugh et. al., was presented by Mr. Kulugh who was the lead author. During this session, a very interesting paper which generated many questions and contributions from participants was presented. The paper which was titled “*Electronic Voting: A framework for a secure Biometric-Based System*” was presented by a participant from the Federal University of Technology, Akure (FUTA).

The third session which was slated for the second day was themed “Social Networks”. This session featured two presenters in persons of Miss Oni and Mr. Soliu who were both from University of Lagos. The title of their papers are- *Email urgency classifier Using Natural Language Processing and Naïve Bayes* and *Filtering Political Sentiment in Social media using textual information respectively*.

The fourth session was themed “Network Intelligence”. This session featured two presenters. Mr. Umoru Lateef from the Federal University of Technology, Minna (FUT Minna) presented a paper titled *Towards Hybridization of Genetic Algorithm (GA) and Artificial Neural Network (ANN) for the detection of Advanced Persistent Threats (APT)* while Mr. Fasipe Timilehin from University of Lagos presented a paper titled *A convolutional Neural Network Library*.

The fifth session was themed “Network Safety”. Three papers were slated for presentation but one of the presenters was unavoidably absent.

IoT and Big Data was the theme of the final session. Four papers were expected for presentation, but one of the presenters did not show up. One of the presenters was from FUT Minna, while the remaining two presenters were from University of Lagos.

5.0 Highlights of Keynote Speech

Since the theme of the conference was *Emerging Security Issues in E-Services in the 21st Century*, the Keynote Speaker was very apt in the choice of his speech’s title. The following are key issues noted in his speech titled *Emerging Security Issues and Challenges of Cloud Computing in Nigeria*.

- i. Ubiquitous Cloud computing is becoming the standard for service provisioning for businesses and individuals. However, this is bedevilled with myriad of challenges which range from security issues with the cloud environment to securing the data on the cloud.
- ii. It is challenging to ensure that privacy of data is maintained and data loss or leakage is prevented.
- iii. It is important to state that most security issues on the cloud could be tailored to personal gain or cyber warfare.
- iv. The Nigerian infrastructure deficiencies favour cloud computing for many businesses. Thus, the businesses in Nigeria are faced with these myriad of security challenges that cloud computing has.
- v. The security threats could result in loss of control of the electronic business platform or service disruption. These challenges could further be classified as follows:
 - Service availability and performance
 - Outsider attack
 - Malicious Insider
 - Multitenancy
 - Loss of control and Data loss
 - Service disruption
- vi. Cloud security is a challenge that user and business must take seriously. It can no longer be assumed that security of the cloud services solely lies on the cloud service provider.
- vii. Every cloud user must take deliberate steps and actions to ensure its services or activities are performed in such a manner that does not give the cybercriminals access to their information.

- viii. Nigerians, like every other people in the world that use cloud services, are exposed to the enormous risks that using cloud computing presents.

The population of Internet users has made cloud computing become the beehive for businesses and socialization for individuals. If this is not properly harnessed, one might not get out easily without a sting.

In achieving the stability of cyberspace, the following issues should be seriously taken into consideration:

- i. Efforts should be made to promote mutual awareness and understanding among the various cyberspace communities working on issues related to international cybersecurity. This is achievable by contributing to an essential global task of supporting the security and stability in, and of, cyberspace through norms coherence and policy.
- ii. Cyberspace is a bio-electric environment that combines people, processes and technology. Since threat actors carry out their activities in an apparently seamless environment, therefore, securing things vulnerable through ICT (information & other things such as control systems) is very essential and urgently required.
- iii. Cybersecurity is considered a hub for achieving new norms of collaboration, ensuring privacy, achieving critical infrastructure, preventing cyber war, ensuring adequate security of things, preventing cybercrime, sustaining technology and law and allowing systemic risk and resilience are sacrosanct.

6.0 Feedbacks on Conference Evaluation

In line with the global practices of conference organisation, a feedback mechanism was put in place to receive objective assessment of the conference from the participants. The intention was to have an unbiased appraisal of the conference in order to improve on the quality of the next one slated for October, 2020.

With respect to the participants' evaluation of the conference, 8 out of 19 participants rated the conference "More than Satisfactory" while 11 of 19 gave a rating of "Satisfactory". 15 of 19 participants rated the conference location and facilities as "More than Satisfactory".

The appropriateness of presentations in line with the conference's theme was confirmed by 18 of 19 participants who responded to the questionnaire and rated it as "More than Satisfactory".

18 of 19 participants rated the overall organization of the conference "More than Satisfactory". The conference workshop, breakfast/lunch and Dinner were

mostly rated “More than satisfactory”. 13 of 16 participants rated the Cyber-Security Workshop as “More than Satisfactory”. However, the conference registration process was rated “Satisfactory” with comments “Can be improved”. The feedbacks received from participants were undoubtedly remarkable improvement over the maiden edition of the conference that was held in October, 2018. A summary of this analysis is shown in Table 1.

Table 1: Summarized Analysis of Conference Review

Description	Responses	Distribution	Percentage
Overall evaluation of the Conference	More than Satisfactory	8 out of 19	42%
	Satisfactory	11 of 19	58%
Conference location and facilities	More than Satisfactory	15 of 19	78.9%
Most Valuable (Workshop)	Percentage of those who rated the Workshop as the most valuable aspect of the conference	10 of 18	56%
Least Value	Percentage of those who rated Dinner as least valuable	1 of 16	6.25%
	Percentage of those who rated security as least valuable	1 of 16	6.25%
	Percentage of those who rated the workshop as least valuable	1 of 16	6.25%
presentations in line with the conference’s theme	Percentage of those who rated the presentations appropriate for the conferences	18 of 19	95%
Overall Organization	Percentage of those who scored the conference organization below 4	1 of 19	5.3%
Conference Registration	Percentage of score of 3 and/or below	4 of 19	21%
Audio/Video/Multimedia	Those who gave a score of 3 and/or below	1 of 19	5.3%
Cyber-Security Workshop	Those who gave a score of 3 and/or below	3 of 16	18.75%
Breakfasts/Luncheons	Those who gave a score of 4 or 5	14 of 19	73.68%

Dinner	Those who gave a score below 5	5 of 16	26.32%
Improvement areas	Timing, publicity, electricity/Power, add a touch of culture, invite more institutions and departments		
Conference publicity (“Learnt about this conference”)	- 4 of 18 - Banners and Fliers - 5 of 18 - Email - 7 of 18 - Word of mouth / direct invitation - 2 of 18 - others		

7.0 Recommendations and conclusions

While appreciating the efforts of the chairman of the conference and the organising committee for the noticeable improvements made and success recorded in 2019 CoNIMS’ conference, the following observations were, however, made in order to improve the quality and credibility of the conference in the subsequent years.

- i. Early notification of the conference programme. Members were advised to notify academic and industrial communities as early as possible in order to attract appreciable number of paper submission. Planning of the conference should commence at least six months prior to the date.
- ii. Annual Best 3 papers award. It came to the surprise of the organisers that this very important aspect of the conference was conspicuously but inadvertently omitted. The conference Chair therefore advised CoNIMS’ members on the inclusion of this in the subsequent year in line with the global academic practices in many international conferences.
- iii. Poster presentation category. In order to avoid discouraging prospective authors whose researches are still in progress, poster presentation had been suggested. It was, however, agreed that this category of work will not appear in the conference proceedings.

- iv. Student participation and encouragement. Special appreciation to the conference Chair for encouraging two of his undergraduate students to submit and present their final year project reports during the conference. Other members were challenged and encouraged to motivate their students to present their project work in the next conference.
- v. Early conversion of selected and reworked conference papers into a journal articles as being proposed by CoNIMS' research group.

8.0 Appreciation

Computer Networks, Infrastructure Management and Security (CoNIMS) Research Group of the Department of Computer Sciences, University of Lagos, appreciates the support received from her sponsors towards the success of her 2019 conference.

Signed

Prof. Charles O. Uwadia

Leader, CoNIMS Research Group