2ND CONIMS INTERNATIONAL CONFERENCE & WORKSHOP

University of Lagos, Nigeria. | Oct. 22-24, 2019

ACCEPTED PAPERS

S/N	TITLE	AUTHORS	ABSTRACT
1	BIG DATA AND BIG DATA ANALYTICS: A LITERATURE-BASED RESEARCH ON PRIVACY AND SECURITY -A DECADE TOUR	Sule, A. A., Okunoye, O. B., and Oyefolahan I. O.	*Over time, there has been an increase in the the world's interest in big data and analytics as data forms a major asset of every operable organization today. However, with the high volume of data generated at regular intervals, security and privacy in all dimensions of big data becomes a major concern. Since its inception, numerous literatures have been researched in the field of big data analytics security and privacy. Therefore, a study is required to provide a proper understanding of the security and privacy requirements of Big Data Analytics and ensure that the full potential of data is exploited.* *This paper seeks to perform a literature-based research on privacy and security with respect to big data and big data analytics over the past 1o years by visiting several authoritative journals for articles related to big data and analytics' privacy and security. The study gives a comprehensive review of big data and its related security and privacy concerns. At the end, it was discovered that although so much has been done to provide the needed security to data, more work still needs to be done to cope with the technological advancements and the rapid increase in data generation from different computing environment.*
2	DEVELOPMENT OF A FRAMEWORK FOR THE DETERMINATION OF AN ASSET AS CRITICAL NATIONAL INFORMATION INFRASTRUCTURE (CNII)	Mbanaso, U. M., Nnanna, N.A., Dandaura, E.S., Kulugh, V.E.	Globally, cyberattacks directed at critical national infrastructure are on the increase even as the spectrum of prospective perpetrators is expanding. The most worrisome are malicious activities backed by one nation state against other nations perceived as rivals. The prolonged effect of such coordinated attacks on a nation's critical assets or services include: crippling the economy, undermining national security and putting the well-being of citizens of the affected nation in serious jeopardy. Sadly, cyber threats and vulnerability landscapes are becoming more complex as perpetrators evolve new strategies daily. Since most Critical National Infrastructures (CNIs) are increasingly dependent on cyber technologies to function effectively, adequate care must be taken to identify and effectively protect CNIs from any form of malicious activity. In Nigeria, the 2o15 Cybercrime Act empowers the President to designate certain assets or services as a Critical National Information Infrastructure (CNII) and accord such adequate protection. However, till date, there is practically no established model for the determination of what actually constitutes national asset or service in Nigeria. This paper presents the development of a framework for the determination of what asset or service can qualify to be designated as CNII. The research methodology adopted was document scan and synthesis of subject matter frameworks, cybersecurity frameworks, standards, reports and models, followed by critical review of selected reputable articles. These helped to frame and refine the

			development of the framework core. Based on the analysis, CNII determination rely heavily on causal factors of criticality and dependency. The criticality and dependencies factors indicate the importance of an asset, service or function which can be on the basis of computation of the variables. The novelty of this work besides the methodical approach, provides new insights and guidance to the proper assessment and how to determine and designate an asset or infrastructure as CNII in Nigeria. It provides guarantee for efficient and transparent process in the designation of CNII organisations that is not arbitrary. As far as publicly known, there is no published article on the criteria for selecting and qualifying an infrastructure or asset as a critical sector. Thus, the framework can strengthen existing national efforts towards the CNII protections, and invariably ensuring a better CNII resilience against cyberattacks.
3	ELECTRONIC VOTING: A FRAMEWORK FOR A SECURE BIOMETRIC-BASED SYSTEM	Adewale, O.S, Boyinbode, O.K, and Salako, E.A	*The fraudulent activities such as rigging, impersonation, vote buying/selling, results' repudiation and alteration among the corrupt politicians, voters and election officers have negatively provided platforms for an unwanted contestant to win an election. The roles of computer technology cannot be over-emphasised in tackling the aforementioned security challenges in the election. Scholarly published studies were reviewed to identify shortcomings and provide an avenue for a highly secure e-voting system. This paper presented an architectural framework of a secure electronic voting system using fingerprint and visual semagram techniques in addressing the challenges in enrolment, authentication, secrecy, confidentiality and integrity. A metadata fusion technique was applied to fuse voter's fingerprint and randomly generated voter's identification number (V_{in}) scores while visual semagram technique was used to conceal the sensitive election results against fraudsters' attacks.*
4	TOWARDS HYBRIDIZATION OF GENETIC ALGORITHM (GA) AND ARTIFICIAL NEURAL NETWORK (ANN) FOR THE DETECTION OF ADVANCED PERSISTENT THREATS (APT)	Umoru, L.C. and Ojeniyi, J.A.	*Advanced Persistent Threat(APT) is defined as an attack targeted on organizations for the main purpose of stealing data that are of importance in the organization or to cause a particular damage. As the name implies, it is advanced i.e. APT uses different forms of vulnerabilities that are identified within the organization. Attackers are capable of detecting the attacks that have been previously known and therefore the efficiency of these systems is more than the efficiency of the APT detection system. Hence, the need for several artificial intelligence methods to be worked on and proven predictions for the detection of APTs. The paper aims to develop a hybridized technique using Genetic Algorithm (GA) and Artificial Neural Network (ANN) in the detection of APT. The study imports technical indicators inform of datasets of which is represented by 21 input variables based on 1781 URL of past time spans of different lengths, and is collected before the day of prediction of APT. It is used to generate more diverse subsets of input which is then culled down to a manageable number of effective ones by Genetic Algorithm (GA) and passed onto Artificial Neural Network (ANN) to make prediction. At the end, the results shows*

			that highest rate to detect APT is achieved by GA with ANN in comparison to Modified Mutual Information based Feature Selection (MMIFS), Learning Fuzzy Classifier System (LCFS) and Firefly Swarm Algorithm (FFSA) techniques
5	A FRAMEWORK FOR PERFORMANCE EVALUATION OF EMAIL SPAM DETECTION	Agbo, O.J. and Abdulmalike, D.M.	*Spam involve the use of electronic messaging systems otherwise referred as email to transmit unsolicited bulk messages indiscriminately to an un-intended recipient. However, there has been a continuous influx of these bulk messages to recipients" email box by scammers with different motives which are negatively intended to wreak havoc on the recipients. It is this difficulty in stopping the spam from entering this mail box that has necessitated this research into this studying and designing an improved spam email filtering and detection algorithms using different supervised machine learning techniques. This paper aims to evaluate some existing algorithms model from supervised machine learning and propose a spam detection framework that will automatically choose the near best model from among the different filtering specifiers that performed the classification based upon intelligently identified heuristics from the email profile and features. A review on content-based spam filtering machine learning technique was carried out which narrowed our research to few supervised machine learning like KNN, SVM, Decision Trees, Naive Bayes, Logistic Regression and Neural Network (Perceptron). The parametric and nonparametric machine learning was also carried out to determine the quantities and sizes of the data. A supervised ml model framework for training and testing of data was designed and the classifier evaluates email data into a refined form by separating the Ham from Spam using zero and one respectively. The model result is displayed producing the near best classifiers model algorithms. Though, this is still an ongoing research model and is aimed at producing the best classifier model algorithms that will drastically reduce the spam penetration window into the email box.*
6	A DIGITAL FORENSICS INVESTIGATION MODEL THAT INCORPORATES DIGITAL CHAIN OF CUSTODY FOR CONFIDENTIALITY, INTEGRITY, AND AUTHENTICITY	Koleoso, R.A., Ajayi, O. O, Oladeji, F.A and Uwadia, C.O	*Digital Forensics Investigation Models (DFIMs) are designed to assist investigators in handling Digital Evidence (DE) related to computers and other digital media. Researchers have proposed various DFIMs to ensure that the integrity of the DEs being scrutinized remains intact. Many of these models focused on the integrity of the DE, while ignoring authenticity. They also did not consider maintenance of a Digital Chain of Custody (DCoC) which can be used to keep track of the DE. To address these shortcomings, this paper proposed an investigation model named Digital Forensic Investigation - Digital Chain of Custody (DFI-DCoC). The proposed model incorporated DCoC as a way of ensuring the Integrity and Authenticity (IA) of DEs during the investigation process. Furthermore, the model introduced a parameter that specified the number of participating actors involved in the investigation process; this is used to prevent the transfer of responsibility to person(s) not listed within the process. The model thus used a combination of 2-Stage authorization and hashing to maintain IA of both the DE and DCoC. Results show that the proposed DFI-DCoC model*

			encompasses more DFI activities than other compared models while also able to guarantee the Integrity and Authenticity of the DE and DCoC
7.	EMAIL URGENCY CLASSIFIER USING NATURAL LANGUAGE PROCESSING AND NAÏVE BAYES	Oni, A., Ogude, C. and Uwadia, C.O.	*Emails are today's most commonly used means of communication. It is one of the Internet's greatest inventions. Billions of emails are transferred daily for various purposes. The Harvard Business Review states that after an interruption (e-mail or other), it takes 2o minutes to regain full focus. This is backed by the argument of Loughborough University that when interrupted by phone, tasks take 33 percent longer to complete. Hence, people are constrained on how to manage their time effectively; this is because a piece of time-critical information may be received and needed to be worked upon urgently. Large organizations receive thousands of emails every day; they cannot decide on which email to respond to first because the emails are already in a hierarchy, based on the time they were received. Hence, emails that are time-critical or require urgent response may be pushed to the bottom of the list. The aim of this paper is to present a model that can interpret human language and efficiently discern between urgent and not urgent emails. When emails are sent, the model prioritizes which emails should be responded to by the receiver based on the level of urgency and importance of the content of the email*
8	SECURING DRUG DISTRIBUTION AND CONSUMPTION ANALYSIS USING THE BLOCKCHAIN TECHNOLOGY	Oladeji F.A., Azeez N.A, Okenna C., Okafor J., and Odejinmi O.	*Reported cases of fake drug consumption is on the increase as many users have fallen victim of the purchase and use of fake drugs that is branded with a particular company logo on it. In Nigeria today as early 2o19, people are generally afraid of buying drugs so as not to fall victims. In order to curb to sale of fake drugs and protect the consumer's interest, there is need to put a chain link in the channelling of those drugs right from the Agency in charge of food and drug eg. NAFDAC, to the Manufacturer, to the Pharmacy and then the Consumer. Blockchain maintains high security and if any part of the chain is broken or altered the entire chain is affected. This paper focuses on securing the authenticity of every drug you purchase by showing the chain which the drug has passed through right from the National Agency until it gets to the final consumer of the drug, likewise acts a way the National Agency can better assist its populate in terms of subsidy removal for drugs mostly consumed during certain climate period.*
9	ON QUANTUM CRYPTOGRAPHY FOR NETWORK SECURITY	Rufai, A.U. and Okenna, C	*The factorization of large integers into their primes is the algorithm in secret and public key cryptography, these is however said to be intractable. Thus, with the application of quantum physics into cryptography, quantum cryptography can be created. Quantum cryptography exploit effects of quantum mechanics { quantum tunneling, entanglement principles, superposition, wave-function concept, Heisenberg uncertainty principle, photon polarization, in the performance of cryptographic tasks, thereby guarantees a secure communication. Security proofs noted that, quantum cryptography if appropriately implemented, even the most powerful eavesdropper cannot decrypt the message from a cipher. Thus, the goal of quantum cryptography is to establish a secure key in an insecure*

			communication environment. Among the application areas of quantum cryptography, quantum key distribution (QKD) has gained much popularity, however others include: randomness generation, quantum money, delegated quantum computation and secure two and multi-party computation. Quantum key distribution (QKD) focuses on the secure communication between two distant parties and guarantees the security of a transmitted message between them. Which helps solves the problem encountered in one time pad key distribution problem. This paper covers the strengths, weaknesses, and methodology of quantum cryptosystems, the basic concepts as regards to quantum cryptography, its application area, various limitations and finally the future direction in which the quantum cryptography is headed towards.
9	*ISSUES AND CHALLENGES USING WI-FI IN INTERNET OF THINGS (IOT) SMART CITY*	Oladeji F.A., Ogun, A. and Afolorunso, A.	*The Internet of Things smart city offers many benefits, promoting advanced and efficient communication through the laptops, desktops, cars and computer peripherals, through the interconnectivity of a variety of analog and digital data collection devices such as vehicles, physical devices and embedded systems. Wi-Fi is a critical element of a smart city based on wireless technology that employs radio frequency to permit devices to connect to the Internet. Wi-Fi is based on wireless technology hence smart city projects around the globe adopt Wi-Fi technology as a platform for internet access. However, the danger that exists with using unsecure Wi-Fi could outweigh the benefits that an IoT smart city brings if not properly managed. This papaer aims to identify the issues and challenges using Wi-Fi in IoT smart city.*
10	DESIGN AND IMPLEMENTATION OF AN INTERNET-DRIVEN INDOOR FIRE ALARM SYSTEM USING INTERNET OF THINGS CIRCUITRY (ARDUINO)	Oladeji, F.A. and Sojorin, S.	*Fire accidents have been known as the dangerous tragedy that could cause destruction, property and life losses. In many disasters, fires have become recurrent, destructive and most influential disasters if compared to other hazards. The use of fire alarms is very crucial as they aid in alerting the public when a fire outbreak occurs which can help save lives and reduce damages. Internet of things is the intelligent connectivity of physical devices to increase the economic value and improve the quality of life. It is driven by a combination of sensors, connectivity, people and process. The use of IoT with fire alarms can reduce human intervention to the minimal, fire can be detected early using sensors and an alarm can be triggered automatically. Although this approach may have its downside like the IoT would need to be connected to the internet, the sensors can be triggered by light hence causing a false alarm, sensors may be damaged in the fire, etc. This project focuses on designing an IoT fire alarm system for computer laboratories. The IoT system would be interfaced with a mobile solution that monitors the temperature of the room, detect a fire, alert the fire services via SMS sending the fastest route to the place of the fire, turn off electrical appliances and sound an alarm*
11	DIGITAL FORENSICS INVESTIGATION MODEL THAT INCORPORATES DIGITAL CHAIN OF	Koleoso, R.A., Ajayi, O. O, Oladeji, F.A and Uwadia, C.O	*Digital Forensics Investigation Models (DFIMs) are designed to assist investigators in handling Digital Evidence (DE) related to computers and other digital media. Researchers have proposed various DFIMs to ensure that the integrity of the DEs being*

	CUSTODY FOR CONFIDENTIALITY, INTEGRITY, AND AUTHENTICITY		*scrutinized remains intact. Many of these models focused on the integrity of the DE, while ignoring authenticity. They also did not consider maintenance of a Digital Chain of Custody (DCoC) which can be used to keep track of the DE. To address these shortcomings, this paper proposed an investigation model named Digital Forensic Investigation - Digital Chain of Custody (DFI-DCoC). The proposed model incorporated DCoC as a way of ensuring the Integrity and Authenticity (IA) of DEs during the investigation process. Furthermore, the model introduced a parameter that specified the number of participating actors involved in the investigation process; this is used to prevent the transfer of responsibility to person(s) not listed within the process. The model thus used a combination of 2-Stage authorization and hashing to maintain IA of both the DE and DCoC. Results show that the proposed DFI-DCoC model encompasses more DFI activities than other compared models while also able to guarantee the Integrity and Authenticity of the DE and DCoC*
12	A CONVOLUTIONAL NEURAL NETWORK LIBRARY	Fasipe, T.M., Ogude, C. and Uwadia, C.O.	*This paper presents a convolutional neural network library created from scratch using Python programming language. The library was tested by creating models to perform image recognition on three different datasets, the mnist, fashion mnist and the cifar-10 datasets. The models created were able to achieve 98%, 89% and 84% test accuracy on the datasets respectively. Cython was used to help optimize some operations in the very expensive convolution operation and this reduced training time by 50%. Batch normalization was also used to help train the models with very high learning rates. Finally, Dropout was used to reduce overfitting and help the models generalize.*