



Nigeria Section
4TH INTERNATIONAL
CONFERENCE

MAY
17TH - 19TH
2022

 Nile University of Nigeria

Hybrid Event(In-person & Virtual)

NIGERCON 2022

Disruptive Technologies for Sustainable Development

P R O C E E D I N G S



Proceedings of the
**2022 IEEE 4th International
Conference on Disruptive Technologies
for Sustainable Development
(NIGERCON)**

May 17-19TH, 2022.

Proceedings

IEEE Catalog Number: CFP22NIG-ART

ISBN: 978-1-6654-7978-3

Online ISSN: 2377-2697

<https://attend.ieee.org/nigercon-2022/>

Volume Editors

Kennedy Chinedu Okafor

Ifeyinwa E. Achumba

Steve A. Adeshina

Omowunmi Mary Longe

Faruk Nasir

Ikechukwu Ignatius Ayogu

Copyright and Reprint Permission:

Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For reprint or republication permission, email to IEEE Copyrights Manager at pubs-permissions@ieee.org.

All rights reserved. Copyright ©2022 by IEEE.

ISBN: 978-1-6654-7978-3

Online ISSN: 2377-2697

Program Committee

Kouzou Abdellah	University of Djelfa
Otuoze Abdulrahaman Okino	IEEE
Steve Adeshina	Nile University of Nigeria
Steve Adeshina	Nile University of Nigeria
Mudathir Akorede	University of Ilorin
Abdullateef Aliyu	Phase 3 Telecom
Ikechukwu Ayogu	Federal University of Technology, Owerri, Imo State
Longe Babatope	IEEE
Gloria Chukwudebe	Federal Univer of Technology Owerri
Folasade Dahunsi	Federal University of Technology Akure
Udoka Eze	Federal University of Technology, Owerri
Irene Samy Fahim	Nile University Egypt
Fina Faithpraise	University of Calabar
Ibikunle Francis	Landmark University Otta
Francis Ibikunle	Landmark University Otta
Achumba Ifeyinwa	Federal Univer of Technology Owerri
Charles Ikerionwu	Federal Univer of Technology Owerri
Ogechukwu Iloanusi	University of Nigeria, Nsukka
Agajo James	Federal University of Technology, Minna
Okokpujie Kennedy	Convenant University
Uche Mbanaso	Nasarawa State University Keffi
Faruk Nasir	Sule Lamido University
Agha Francis Nnachi	Tshwane University of Technology
Aniedu Nzubechukwu	UNIZIK Nnamdi Azikiwe University
Oluwaseun Adeniyi Ojerinde	Federal University of Technology Minna
Kennedy Chinedu Okafor	Federal University of Technology, Owerri, Nigeria
Lanre Olatomiwa	Federal University of Technology, Minna, Nigeria
Adeniran Oluwaranti	Department of Computer Science & Engineering, OAU
Longe Omowunmi	University of Johannesburg, Johannesburg, South Africa
Atanda Raji	Cape Peninsula University of Technology Center for Distributed Power and Electronics Systems
Thomas Sadiq	Nile University
Tunde Salihu	IEEE Nigerian Section
Aderonke Thompson	Federal University of Technology, Akure
Kingsley Chiwuike Ukaoha	University of Benin UNIBEN
Edwin Albert Umoh	Federal polytechnic Kaura-Namoda,

Preface

Preface

NIGERCON 2022

This volume contains the papers presented at the 2022 IEEE Nigeria 4th International Conference on Disruptive Technologies for Sustainable Development (NIGERCON) held on May 15-17, 2022, in Abuja. The highly multidisciplinary Conference brought together all experts, researchers, and innovators from business, industry, academia, and government agencies to discuss concepts and experimental results.

We are honored to welcome experts, researchers, professionals, innovators from academia, and the industrial circle to join the conference. NIGERCON 2021 aims to provide a high-quality forum for communications of research achievements, ideas, and experience of application in all fields of Communications Technology and Computer Science. Participants can develop ideas, catch research directions, and accelerate theoretical research, technology development, application, and innovation in certain subjects.

This year we received over 236 paper submissions and 149 high-quality papers were accepted for presentations at an acceptance rate of 0.66. We utilized the talents and experience of reviewers working at Universities and Institutions from around the world. Each contributed paper was rigorously peer-reviewed by 108 external reviewers, with a total of 627 reviews. Experts were drawn from a large pool of technical committee members as well as other international reviewers in related fields.

IEEE Nigercon22 Participating authors spread across 23 Countries namely: Algeria, China, United States, United Kingdom, Uganda, Sri Lanka, South Africa, Saudi Arabia, Rwanda, Norway, Nigeria, Niger, New Zealand, Namibia, Malaysia, Indonesia, India, Hungary, Ghana, Germany, France, Egypt, and Cyprus.

Â

We would like to express our gratitude to all authors, whose research results have been published in Nigercon2022 Proceedings and IEEE Xplore digital library for their in-depth evaluations. Our high standards are maintained through a top-rated peer-review process.

Â

Furthermore, we would like to thank all the authors and attendees for participating in the Conference. We hope that Nigercon2022 inspires and entices you to submit your contributions to upcoming IEEE Nigeria Section Conference.

Â

We wish you a stimulating and fruitful time at the Conference and a memorable experience in Abuja city.

Â

Â

Engr. Prof. Gloria Chukwudebe, *Federal University of Technology, Owerri, Nigeria*

NIGERCON 2022 Technical Program Chair

Â

Â

April 10, 2022

Kennedy Chinedu Okafor
Longe Omowunmi
Faruk Nasir
Ignatius. Ayogu

Additional Reviewers

Abdulkarim, Abubakar
Abioye, Emmanuel Abiodun
Abo-Al-Ez, Khaled
Abubakar Sadiq, Ahmad
Adedigba, Adeyinka
Adetokun, Bukola
Adetoro, Ayodeji
Adewale, Ajao
Adeyanju, Ibrahim
Agbachi, Eugene
Agbolade, Olaide
Airoboman, Abel
Ajani, Ayodeji
Akande, Oluwatobi
Akinbolati, Akinsanmi
Akinlabi, Ayo
Akinsanmi, Akinbolati
Akumu, Aloys Oriedi
Almaktoof, Ali
Ambafi, James Garba
Aminou Moussavou, Akim Anges
Aniedu, Azubuike
Anyasi, Francis
Atimati, Ehinomen
Ayeleso, Ayokunle
Ayinla, Lukman
Ayogu, Ikechukwu

Badeji-Ajisafe, Bukola
Balyan, Vipin
Bara'U Gafai, Najashi

Calafate, Carlos
Chowdhury, Mahabubur Rahman

Dahunsi, Folasade
David, Michael
Dodo, Usman
Dogo, Eustace Manayi

Elesemoyo, Isaac
Emmanuel, Osaji
Essiet, Ima
Eteng, Idongesit

Euphemia, Nwokorie

Fadamiro, Akinwale Oluwaseyi
Folorunso, Taliha

Hawahu, Abdulsalam

Ibikunle, Francis
Ibrahim, Oladimeji
Ifada, Emmanuel
Ikerionwu, Charles
Iloanusi, Ogechukwu
Imam-Fulani, Yusuf Olayinka
Imoize, Agbotiname
Imoru, Odunayo
Innocent, Engr Dr. Onyeyili
Innocent, Onyeyili

Jimoh, Abdulramon

K.V.N., Kavitha
Kamanzi, Janvier
Krishnamurthy, Dr.Senthil
Krishnamurthy, Senthil

Lawan, Sani
Leke, Collins
Longe, Omowunmi Mary
Luta, Doudou

Ma'Arif, Alfian
Mansour, Khloud M.
Melodi, Adegoke
Mnguni, Elvis
Mohammed, Olatunji
Moloi, Katleho

Noma-Osaghae, Etinosa
Nwagu, Martins
Nweke, John
Nwohu, Mark

Obiyemi, Obiseye
Oghorada, Oghenewvogaga
Okafor, Kennedy Chinedu
Okojie, Daniel
Oladeji, Akinola
Olanite, Olanrewaju

Olarinoye, Gbenga
Olatomiwa, Lanre
Olawuyi, Adedayo
Olayanju, Sunday
Oloyede, Abdulkarim
Oluwole, Osaloni
Omoruyi, Osemwegie
Orimogunje, Abidemi
Oshiga, Omotayo
Otuoze, Abdulrahaman
Oyekola, Oluwaseun

Popoola, Olugbemiga Solomon

Ratshitanga, Mukovhe
Rufa'I, Nabila

Salawudeen, Ahmed Tijani
Salihu, Ibrahim
Samuel, Isaac
Sanni, Shereefdeen Oladapo
Sanusi, Kamilu
Shoukat, Abdullah
Sowande, Olugbenga
Sur, Samarendra Nath
Surajudeen-Bakinde, Nazmat
Susan, Ajagun

Theophilus Leonard, Alumona
Thomas, Sadiq
Thompson, Aderonke
Tijani, Salawudeen
Tola, Omokhafe

Ukwandu, Elochukwu
Umoh, Edwin
Usman, A D

Yahaya, Enesi

Table of Contents

High Impedance Fault Modelling and Simulation of 33kV/11kV Distribution Network Using MATLAB	1
<i>Iniobong Abasi-Obot, Gaddafi Shehu, Abdullahi Kunya and Yusuf Jibril</i>	
QoS-Aware Earliest Due Date First Scheduling Algorithm for LTE Networks	5
<i>Abdulhakeem Abdulazeez, Ahmad Saifullahi Tijjani and Aminu Mohammed</i>	
Prioritized Quality of Service-Aware Downlink Scheduling Algorithm For LTE Network...	10
<i>Abdulhakeem Abdulazeez, Mahmud Muhammad Yahaya, Isah Bala Yabo, Abdulkarim Bello, Maniru Malami Umar and Aminu Mohammed</i>	
The Study of Efficacy of Gaussian Mixture Model In Image Tracking System Using the Canny Optical Flow Technique	15
<i>Zinat Alabi Abdulkadir, Oluwole Abiodun Adegbola, Peter Olalekan Idowu and David Olugbenga Aborisade</i>	
A Spatio-Temporal Non-Concurrent Data Gathering and Energy Replenishment in Wireless Rechargeable Sensor Networks (ST-NCDR)	21
<i>Shamsuddeen Abdullahi Mikail, Usman Aliyu Danjuma, Abdoulie Momodou Sunkary Tekanyi, Kabir Abubilal Ahmad and Aminu Muhammad Abba</i>	
Quantity vs. Quality of Monolingual Source Data in Automatic Text Translation: Can It Be Too Little If It Is Too Good?	26
<i>Idris Abdulmumin, Bashir Shehu Galadanci, Shamsuddeen Hassan Muhammad and Garba Aliyu</i>	
Control of Dual Stator Induction Generator Based Wind Energy Conversion System	31
<i>Ibrahim Abdulwahab, Adamu Saidu Abubakar, Abdulrahman Olaniyan, Bashir Sadiq and Shehu Faskari</i>	
A Three-Step One-Time Password, Textual and Recall-Based Graphical Password for an Online Authentication	36
<i>Haruna Adamu, Abdulmalik Danlami Mohammed, Solomon Adelowo Adepoju and Abisoeye Opeyemi Aderiike</i>	
Effect of Training Algorithms and Network Architecture on the Performance of Multi-Band ANN-Based Path Loss Prediction Model	41
<i>Quadri Ramon Adebowale, Nasir Faruk, Kayode S. Adewole, Abubakar Abdulkarim, Abdulkarim A. Oloyede, Haruna Chiroma, Olugbenga. A. Sowande, Aliyu D. Usman, Yusuf Olayinka Imam-Fulani, Abduljalal Yusha'U Kassim and Lawan S. Taura</i>	
A Model for Network Virtualization with Open Flow Protocol in Software Define Networks	46
<i>Oluwashola David Adeniji, Abiodun Adedayo and Sunday A. Ajagbe</i>	
Development of an IoT Based Data Acquisition and Automatic Irrigation System for Precision Agriculture	51
<i>Emmanuel Adetiba, Ayodele Ifijeh, Victoria Oguntosin, Toluwani Odunuga, David Iweala, Ayoola Akindele, Abdultaofeek Abayomi, Obiseye Obiyemi and Surrendra Nigeria Thakur</i>	

Multi-class classification and modeling of the hospitalization status of COVID-19 patients	56
<i>Taiwo Adetiloye, Emmanuel Dansu and Akinkunle Akinola</i>	
Techno-economic Analysis of Hybrid Energy System Connected to an Unreliable Grid: A Case Study of a Rural Community in Nigeria	61
<i>Saheed Adetoro, Mark Nwohu and Lanre Olatomiwa</i>	
An Overview of Configurations and Dispatch Strategies in Hybrid Energy Systems	66
<i>Saheed Adetoro, Lanre Olatomiwa, Jacob Tsado and Solomon Dauda</i>	
Development A Web-Based System for Real Time Prediction of Drought In Northern Nigeria Using Markov Chain Technique	71
<i>James Agajo, Thomas Sadiq and Gafai Najashi</i>	
Modeling and Dynamic Analysis of hybrid synchronous machine	76
<i>Eugene Agbachi, Linus Uchechukwu Anih and Simon Emeka Obe</i>	
Cultural BAT Optimization Algorithm: An Improved Variant of BAT Algorithm	81
<i>Kulu Amalo Ahmadu, Sabo Birninkudu Ibrahim and Bala Boyi Bukata</i>	
Reaching Function Based PID Control of Electromagnetic Levitation System	88
<i>Mohammed Ahmed</i>	
FES-Supported Revived STS with FLC	94
<i>Mohammed Ahmed</i>	
Impact of Distributed Generations on Power Systems Stability: A Review	99
<i>Abel Airoboman and Adeleke Aderibigbe</i>	
Review of the Performance of the Power Sector in Some Selected African Countries	104
<i>Abel Airoboman, Ayodeji Salau and Megha Chhabra</i>	
Proposed Automatic Number Plate Recognition System using machine learning	109
<i>Faridah Abdul Aiyelabegan, Chukwu Chibuzor Emmanuel, Sadiq Thomas, Fatima Adam Imam, Halima Haruna Ginsau and Fidelis Onah</i>	
A Review of Planning of Integrated Energy System in Nigeria	114
<i>Abimbola Ajagun, Xiaorong Sun and Xueping Pan</i>	
A Low-Cost Orthosis Using a Compliant Spring Mechanism for Post-Stroke Hand Rehabilitation	119
<i>Oluwasegun Akinniyi, Kayode Ayodele, Morenikeji Komolafe, Matthew Olaogun, Daniel Owolabi, Muhsin Fajimi, Michael Macaulay and Kolawole Ogunba</i>	
Technical Losses Computation of a Typical Nigerian Radial Distribution Feeder using the Forward/Backward Sweep Approach	123
<i>Mudathir Akorede, Oladimeji Ibrahim, Abdulrahman Otuoze, A. S. Oladeji, A. O. Zubair and M. O. Tijani</i>	
Application of UAV-Assisted 5G Wireless Communication: A Case Study of the Nigerian Environment	128
<i>Christopher Akinyemi Alabi, Oluwaseun Olayinka Tooki, Agbotiname Lucky Imoize and Nasir Faruk</i>	

LPG Leakage and Smoke Detector System with a wide Range of Mobile Notification and Auto Power Supply Cut-off	133
<i>Ridwan Alabi, Isah Abubakar, Usman Dodo, Jesse Zarmai, Abdullahi Sada, Mustapha Dodo and Timothy Akoji</i>	
Supervised learning based intrusion detection for SCADA systems	141
<i>Oyenyi Akeem Alimi, Khmaies Ouahada, Adnan M. Abu-Mahfouz, Suvendi Rimer and Kuburat Oyeranti Adefemi Alimi</i>	
Machine Learning Based Intrusion Detection on Complex Nested Transactional SQL Queries	146
<i>Garba Aliyu, George Thandekkattu, Idris Abdulmumin, Usman A. Baba, Aminat Bolatito Yusuf and Mustapha Nasir</i>	
Development of An Enhanced Home Automation System For Energy Saving Using GSM, IoT and Bluetooth Technologies	151
<i>Haruna Abubakar Aliyu, Adegboye Araoye Babatunde, Tola Omokhafa James, Lanre Olatomiwa and Umar Suleiman Dauda</i>	
A Review of Deep Learning Techniques for Network Intrusions Detection	156
<i>Funso Alowolodu, Adebayo Adetunmbi, Josephine Mebawondu and Jacob Mebawondu</i>	
Proactive Fuzzy-Based Backup Channel Selection Scheme for Spectrum Handoff in Cognitive Radio	161
<i>Emmanuel Alozie, Faruk Nasir, Abdulkarim A. Oloyede, Olugbenga A. Sowande, Agbotiname Lucky Imoize and Abubakar Abdulkarim</i>	
Tech Mining Analysis: Renewable Energy Forecasting Using Artificial Intelligence Technologies	165
<i>Mutaz Alshafeey and Csaba Csáki</i>	
Power quality factors mitigation on NORED distribution network: A case study of JEDS Campus, Ongwediva	170
<i>Helena Amadhila, Odunayo Imoru and Tom Wanjekeche</i>	
Implementation Of a Web Application For Stakeholder Inclusion For Sustainable Waste Management	175
<i>Emmanuel Chukwudi Amadi, Gloria Chukwudebe, Ikerionwu Charles, Kennedy Chinedu Okafor and Ignatius Ikechukwu Ayogu</i>	
Fault Analysis of South Eastern Nigerian Power System Network	180
<i>Ejikeme Amako and Jessica Onwuzuruike</i>	
A Comparative analysis of the phases of a three-phase Prepaid meter on some selected Loads	185
<i>Henry Amhenrior</i>	
An Interference Management System for a Shared Spectrum Access Network	190
<i>Ehinomen Atimati, David Crawford, Robert Stewart, Ifeyinwa Achumba, Longinus Ezema and Uchenna Diala</i>	
Magnet Varieties and its Characteristics on the Performance of Dual Stator Permanent Magnet Machine	195
<i>Chukwuemeka Awah</i>	

Magnetic Materials' Impact on Loss and Efficiency Profiles of Dual Stator Permanent Magnet Machine	200
<i>Chukwuemeka Awah</i>	
Performance Evaluation of Feature Selection Techniques for Credit Default Prediction	205
<i>Ikechukwu Ignatius Ayogu, Olugbemiga Solomon Popoola, Olamatanmi Josephine Mebawondu, Chukwuemeka Christian Ugwu and Adebayo Olusola Adetunmbi</i>	
A Modified Visual Simultaneous Localisation and Mapping (V-SLAM) Technique for Road Scene Modelling.....	210
<i>Jibril Abdullahi Bala, Steve Adeshina and Abiodun Musa Aibinu</i>	
Fuzzy Logic based Fed Batch Fermentation Control Scheme for Plant Culturing	215
<i>Jibril Abdullahi Bala, Taliha Abiodun Folorunso, Majeed Soufian, Abiodun Musa Aibinu, Olayemi Mikail Olaniyi and Nimat Ibrahim</i>	
A Fuzzy Logic Control Scheme for Electric Automotive Water Pumps	220
<i>Jibril Abdullahi Bala, Ndukwe Okpo Kalu, Suleiman U. Hussein and Taliha Abiodun Folorunso</i>	
Smell Agent Optimization Based Supervisory Model Predictive Control for Energy Efficiency Improvement of a Cold Storage System	225
<i>Adesola Bankole, Stephen Moses and Tahir Ibitoye</i>	
The Computer Farmer Concept: Human-cyberphysical Systems for Monitoring and Improving Agricultural Productivity in Nigeria.....	230
<i>Kosisochukwu Pal Nnoli, Mbadiwe Samuel Benyeogor, Oladayo Olufemi Olakanmi and Doris Augustine Umanah</i>	
Energy-Mix Dynamic for Optimization of Power Generation Strategy and Expansion In a developing Economy Growth	238
<i>Lucky Braide and D. C. Idoniboyeobu</i>	
Power Allocation Optimization in NOMA System for User Fairness in 5G Networks	243
<i>Chekwas Chikezie, Michael David and Abraham Usman</i>	
Selected Microcontrollers and Sensors Analysis for Electrical Energy Metering Circuits ...	247
<i>Folasade Dahunsi, Denis Awosika, Sodiq Eniola and Charles Udekwe</i>	
Accuracy Assessment of Machine Learning Algorithm(s) in Thyroid Dysfunction Diagnosis	252
<i>Kwetishe Joro Danjuma, Gregory Maksha Wajiga, Etemi Joshua Garba, Asabe Sandra Ahmadu and Olumide Babatope Longe</i>	
Optimization of Standalone Hybrid Power System Incorporating Waste-to-electricity Plant: A Case Study in Nigeria	257
<i>Usman Dodo, Evans Ashigwuike and Jonas Emechebe</i>	
Municipal Solid Waste Generation Forecast using an ARIMA Model: A Focus on Abuja City, Nigeria.....	262
<i>Usman Dodo, Evans Ashigwuike and Jonas Emechebe</i>	
Multi-Label Classification of Hate-speech Severity on Social Media using BERT Model ...	267
<i>Bakwa Dunka Dirting, Chukwudebe Gloria A, Nwokorie Euphemia C and Ikechukwu Ignatius Ayogu</i>	

Smart Irrigation System: A Water and Power Management Approach	272
<i>Michael Edodi, Olugbenga Ogidan and Akinwumi Amusan</i>	
Assessing the Vulnerabilities of Internet Users to Cyber-Attacks using their Password Login Patterns	279
<i>Ojonukpe Sylvester Egwuche, Mutiu Ganiyu and Akeem A. Abiona</i>	
Decision Support Platform for Production of Chili Using IoT, Cloud Computing and Machine Learning Approach.....	283
<i>Olakunle Elijah and muazu Jibrin Musa</i>	
Development of LoRa-Sigfox IoT Device for Long Distance Applications	288
<i>Olakunle Elijah, Sharul K. A. Rahim, Mu'Azu Jibrin Musa, Yahaya Otuoze Salihu, Mohammed Joda Bello and Man-Yahaya Sani</i>	
IoT-Based Wearable Human Protection System	293
<i>Chijioko Emem, Olugbenga K Ogidan and Momoh-Jimoh Salami</i>	
Review of Agricultural Unmanned Aerial Vehicle Obstacle Avoidance System.....	298
<i>Uche Emmanuel</i>	
A Blockchain-Based Peer-To-Peer Energy Trading Platform For Distributed Energy Resources	302
<i>Edmund Enyinnia, Joseph Dada and Omitola Olusegun</i>	
A Drowsiness Detection Decision Support System using Self Organising Map	307
<i>Temitayo Fabunmi, Adedayo Ojo and Saheed Lekan</i>	
COVID-19 Vaccination Acceptability Survey among Staff and Students in Nigerian Universities	311
<i>Fina Faithpraise, Faithpraise B. Otoni, Agnes U. Enang, Effiong O. Obisung, Eme J. Effiong and Emmanuel Inah</i>	
IPSODAC: Automated Protection of Images in Social Networks Using Sensitive Object Detection and Access Control	316
<i>Olorunjube Falana, Carolyn Tinubu, Dada Aborisade, Charles Ugwunna and Ibukunoluwa Salau</i>	
Blended Learning Environments: An Exploratory Study of e-Learning Implementation in Nigeria Tertiary Institutions Due to COVID-19 Pandemic.....	332
<i>Hussain Habeebllahi Farayo, Abdulkarim. A. Oloyede, Nasir Faruk, Salisu Garba, Abdulkadir Idris and Hussaini Alhaji Hassan</i>	
CDMA Deployment in Developing Countries: What Went Wrong in Nigeria?	336
<i>Nasir Faruk, Abdulkarim Oloyede, Shamsudeen Adeniyi, Abdulazeez Kanya Rislan and Salisu Garba</i>	
Analysis of GSM, Wi-Fi and LPWAN communication technologies for Smart energy metering circuits	341
<i>Dahunsi Folasade, Ijadunola Hameed, Adegoke Melodi and Akinlolu Ponnle</i>	
Impact of Energy Literacy on Energy Consumption, Expenditure and Management	346
<i>Tlotlo Shenaz Force and Omowunmi Mary Longe</i>	

Deployment, Standardization and Regulatory Challenges Of 5G Services In Africa: Nigeria As A Case Study.....	351
<i>Idris Mohammed Garba, Omotayo Oshiga and Lawal Bello</i>	
Smart Gunshot Detection and Reporting Framework	356
<i>Ibrahim Hamidu, Muhammad Aliyu Suleiman and Ibrahim Abdullahi</i>	
Digital Smart-Grid Mobile-Renewable Energy-Services Usage in Nigeria 5G-Readiness Arrangement	359
<i>Abdullahi Hassan Birnin Kudu, Wan Rozaini Sheik Osman and Hapini Awang</i>	
A Web-Based Hybrid Blockchain Network Model for Securing University Academic Records	362
<i>Ibeneme-Sabinus Ifeoma and Emmanuel Amadi</i>	
Fault Diagnosis in a Three-phase Induction Motor Using Enhanced Park Vector Approach	367
<i>Sunday Igoche, Babatunde Adegboye, Odunayo Imoru and Tola Omokhafa</i>	
The Role Of Energy Harvesting In 5G Wireless Networks Connectivity	373
<i>Abdullahi Ijala Danjuma, Sadiq Thomas and Bukola Babatunde Adetokun</i>	
Spectral Efficiency Bounds of Cell-Free Massive MIMO Assisted UAV Cellular Communication	378
<i>Agbotiname Lucky Imoize, Hope Ikoghene Obakhena, Francis Ifeanyi Anyasi, Michael Adedosu Adelabu, Kavitha K.V.N and Nasir Faruk</i>	
Large-scale Signal Attenuation and Shadow Fading Measurement and Modelling for Efficient Wireless Network Design and Management	383
<i>Joseph Isabona, Rotimi Kehinde, Agbotiname Lucky Imoize, Stephen Ojo and Nasir Faruk</i>	
Integrating Local Search Methods in Metaheuristic Algorithms for Combinatorial Optimization: The Traveling Salesman Problem and its Variants	388
<i>Jeremiah Isuwa, Abdullahi Mohammed, Sahabi A. Yusuf, Nuruddeen I. Muhammad, Baffa S. Garko and Muhammad Y. Haruna</i>	
Benefits of Smart Devices and Grid-tied Minigrids on the Nigerian Electricity Supply Industry	393
<i>Preye Ivry, Muhammad Buhari and Muhammad Mubarak</i>	
Secret message protection using fuzzy logic and difference expansion in digital images.....	398
<i>Ntivuguruzwa Jean De La Croix, Chaidir Chalaf Islamy and Tohari Ahmad</i>	
Implementation of an Embedded Masked Face Recognition System using Huskylens System-On-Chip Module	403
<i>Okokpujie Kennedy, Anicho-Okoro Chiamaka, Okokpujie Imhade Princess and Okesola Julius Olatunji</i>	
Synthesis and Optical Properties of Graphene as Electron and Hole Transporting Layer in Solar Cells	410
<i>M.A Haruna Ladan, A.D.A Buba, Madina Umar and Ahmad Umar</i>	
Electrical Properties and the Microscopic and Spectroscopic Analysis of Two-Dimensional Graphene	415
<i>M.A Haruna-Ladan, A.D.A Buba, Madina Umar and Ahmad Umar</i>	

Application of Firefly Algorithm to the Optimal Siting and Sizing of D-STATCOM in Distribution Networks.....	420
<i>Mela Lashiru Ibn Lele, Ganiyu Bakare, Aliyu Usman and Mustapha Musa</i>	
Modelling and Optimization of Smart Traffic Light Control System.....	425
<i>Nosike Maduka, Isah Ajibade and Mannir Bello</i>	
The conceptualisation of a Configurable Consent Architecture for Personal Data Release .	430
<i>Uche Mbannaso and Adetola Sogbesan</i>	
Design and Implementation of a 5 kVA Solar Photovoltaic System for the Electronics Laboratory in Covenant University.....	435
<i>Emmanuel Mbaya, Koto Omiloli, Kingsley Anagor, Ekong Kennedy, Emuesiri Esisio, Oghorchukwuyem Obiazi, Olisaemeka Isife, Joachim Notcker, Ayokunle Awelewa and Isaac Samuel</i>	
A Smell Agent Optimization Approach to Capacitated Vehicle Routing Problem for Solid Waste Collection	440
<i>Olusesi Meadows, Mohammed Mu’Azu and Ahmed Salawudeen</i>	
A Linear Quadratic Regulator Based Speed Control for Remote-Controlled Racing Cars ..	445
<i>Olusesi Ayobami Meadows, Arthur Rodriguez and Ahmed Tijani Salawudeen</i>	
Network Intrusion Detection Models based on Naives Bayes and C4.5 Algorithms.....	450
<i>Olamatanmi Josephine Mebawondu, Olugbemiga Solomon Popoola, Ikechukwu Ignatius Ayogu, Chukwuemeka Christian Ugwu and Adebayo Olusola Adetunmbi</i>	
Techno-Economic Analysis of Hybrid PV-Wind-Diesel-Battery Standalone and Grid-Connected Microgrid for Rural Electrification in Zimbabwe.....	455
<i>Simbarashe Mhandu and Omowunmi Longe</i>	
LOAD FREQUENCY CONTROL OF A MICROGRID USING FRACTIONAL ORDER PID CONTROLLER.....	460
<i>Chibuoke Michael, Omokhafa Tola, Nwohu Ndubuka and Ambafi James</i>	
Machine Learning Approach to Anti-Money Laundering: A Review	466
<i>Habiba Nasir Mohammed, Nasir Shehu Malami, Sadiq Thomas, Faridah Abdul Aiyelabegan, Fatima Adam Imam and Halima Haruna Ginsau</i>	
Impact of Solar Photovoltaic Generation (SPVG) on Distribution Networks: A case study of Minna town 33/11kV Injection substation.	471
<i>Haruna Mohammed, Mark Nwohu, James Ambafi and Abubakar Ahmad</i>	
A Design-to-Test Technique for Inclusion Coefficients in AI-Driven Systems.....	476
<i>Yusuf Mshelia, Simon T. Apeh, Charles Ikerionwu, Nachamada Blamah, Azubuike I. Erike and Florence Elei</i>	
Learning from Small Datasets: An Efficient Deep Learning Model for Covid-19 Detection from Chest X-ray Using Dataset Distillation Technique	481
<i>Aminu Musa, Fatima Muhammad Adam, Umar Ibrahim and Abubakar Yakubu Zandam</i>	
Effect of Inspired CR-NOMA Power Allocation on Bit Error Rate For Three User NOMA system	487
<i>Abdullahi Musa Auyo, Suleiman Aliyu Babale and Lawal Muhammad Bello</i>	

Optimal Deployment of DG and D-STATCOM using Month Flame Optimization Algorithm in Radial Distribution System	492
<i>Musa Mustapha, Bakare Ayinde Ganiyu, Yau Shuaibu Haruna and Adulkadir Isa Itopa</i>	
Data Clustering for Optimal Photovoltaic-Distributed Generation Placement in an Active Distribution Network	497
<i>Franklin Nkado, Ifedayo Oladeji, Fredrick Nkado and Ramon Zamora</i>	
Comparison between PV and PQ Operating Modes of DG on Stability and Voltage Profile Enhancement of Distribution Systems	502
<i>Fredrick Nkado and Franklin Nkado</i>	
Design of Intelligent and Secure Hospital Appointment Scheduling System	507
<i>Adamu Noma, Kabiru Musa, Hussaini Mamman, Abdulkadir Mato, Abdulkarim Yusuf and Mohammed Sambo</i>	
A LINDDUN-Based Privacy Threat Modelling for National Identification Systems	512
<i>Livinus Obiora Nweke, Mohamed Abomhara, Sule Yildirim Yayilgan, Debora Comparin, Olivier Heurtier and Calum Bunney</i>	
Large-Scale Solar Power in Nigeria: The Case for Floating Photovoltaics	520
<i>Oyinlolu A. Odetoeye, Francis A. Ibikunle, Paul K. Olulope, Uchenna N. Okeke and John O. Onyemenam</i>	
The Role of Power Electronics In Renewable Energy System	525
<i>Oghorada Oghenewogaga, Bukola Babatunde Adetokun, Bawa Garshima Gamiya and Ahmed Bolaaji Nagode</i>	
Web-Based Automated Control and Monitoring Of Water Distribution System	530
<i>Ohugbenga Ogidan, Moses Olla and Isaac Odey</i>	
Automated temperature scanner sensor in comparison with mercury-in-glass thermometer	535
<i>Ohugbenga Kayode Ogidan, Olusola Oloruntoba, Olusola Babalola, Oluwatobiloba Ajagunna and Moses Ajewole</i>	
An IoT Solution for Air Quality Monitoring and Hazard Identification for Smart City Development	541
<i>Reginald Ogu, Gloria Chukwudebe, Ifeyinwa Achumba, Nkwachukwu Chukwuchekwa and Chinomso Okoronkwo</i>	
A Survey on Electronic Voting On Blockchain	546
<i>Kelechi Ohammah, Sadid Thomas, Obadiah Ali, Sadiq Mohammed and Yusuf Sahabi Lolo</i>	
Evaluation of Thermal Comfort in a Multi-Occupancy Office using Polak-Ribiére Conjugate Gradient Neuro-Algorithm	550
<i>Adedayo Ojo and Moses Onibonoje</i>	
Performance Analysis of BFGS Quasi-Newton Neuro Algorithm for the Design of 30 GHz Patch Antenna for 5G Applications	555
<i>Adedayo Ojo and Moses Onibonoje</i>	
Cost Optimization of Hybrid Solar / Heat Pump Water Heating System: Model Formulation	560
<i>Ayodeji Okubanjo, Godswill Ofualagba and Patrick Oshevire</i>	

Efficacy of some Unpopular PathLoss Propagation Models in the VHF and UHF Bands ..	565
<i>Lagodo Hafis Olajuwon, Nasir Faruk, Abdulkarim A. Oloyede, Olugbenga Sowande, Abubakar Abdulkarim, Lukman A. Olawoyin and Yinusa A. Adediran</i>	
Semantic relation evaluation of data science articles for cybersecurity using network of mention	570
<i>Taiwo Olaleye, Folurera Ajayi, Adewale Aromolaran, Ilesanmi Solanke, Segun Akintunde and Jonhbosco Agbaegbu</i>	
Adoption of Photovoltaic Technologies in Nigeria: A Study of Issues, Problems and Solutions.....	579
<i>Olanrewaju Olanite and Mark Nwohu</i>	
Development of Bluetooth Enabled Switching Device for Handoff Selection in Multiple Operators Enabled SIM Card System	584
<i>Mutiat Olanrewaju, Abiodun Musa Aibinu, Samuel Adakole and Afeez Olalekan Azeez</i>	
Combating Network Intrusions using Machine Learning Techniques with Multilevel Feature Selection Method	589
<i>Tosin Comfort Olayinka, Chukwuemeka Christian Ugwu, Omoibu Joseph Okhuoya, Adebayá Olusála Adetunmbi and Olugbemiga Solomon Popoála</i>	
Digital transformation in Nigeria: The prospects and challenges of the gig economy.....	594
<i>Kunle Olorundare, Adedeji Olowe and Adebimpe Olorundare</i>	
Development of a Low-Cost Wireless Environmental Monitoring System	599
<i>Abdulkarim Oloyede, Nasir Faruk, Abdulkarim Abubakar, Adetola Sogbesan, Salisu Garba and Lukman A. Olawoyin</i>	
International Standards and Development Mechanism, Architecture and Services for RSTT: Challenges and Future Research Direction	604
<i>Abdulkarim. A. Oloyede, Nasir Faruk, Abisola Rukayat Hassan, Salisu Garba, Rislan Kanya Abdulazeez and Olugbenga. A. Sowande</i>	
Descriptive and Diagnostic Analysis of NASA and NiMet Big Weather Data.....	609
<i>Opeyemi Oloyede, Simeon Ozuomba and Philip Asuquo</i>	
Development Of a Web-Based Platform For Heart Disease Prediction (Diagnosis) Using Machine Learning.....	614
<i>Oshin Oluwadamilola, Okokpujie Kennedy and Onaeko Iyinoluwa John</i>	
Location-based Distribution of Network Towers using Spatial Analysis.....	621
<i>Joshua Onolemhemen, Opeyemi Osanaiye, Bukola Babatunde Adetokun and Oje Abdul-Quadri</i>	
Smart Grid Reliability Computation- A Solution to Ageing Infrastructure in Nigerian Power Grid	626
<i>Rapheal Onoshakpor, K. C. Okafor and Modukpe Gabriel</i>	
Using Twitter Sentiment Analysis for Sustainable Improvement of Business Intelligence in Nigerian Small and Medium-Scale Enterprises	631
<i>Ugochukwu Orji, Modesta Ezema, Jideofor Ujah, Ponsak Bande and Jonathan Agbo</i>	
Machine Learning Models for Predicting Bank Loan Eligibility	636
<i>Ugochukwu Orji, Chikodili Ugwuishiwu, Joseph Nguemaleu and Peace Ugwuanyi</i>	

Applications, Challenges and Future Trends towards Enabling Internet of Things for Smart Energy Systems	641
<i>Efe Orumwense and Khaled Abo-Al-Ez</i>	
Comparative Analysis of Machine Learning Models for Network Intrusion Detection	648
<i>Edosa Osa and Oghenevbaire Efevberha Ogodo</i>	
Design and Implementation of Obstacle Detection System for An Unmanned Aerial Vehicle.....	653
<i>E.A Otsapa, S.M Sani and O. A Ayofe</i>	
Performance Assessment of 407kW Photovoltaic Power System	658
<i>Michael Paul Okpe, Bukola Babatunde Adetokun and Oghenewogaga Oghorada</i>	
Embedded Systems Application and Network in Water Utility Systems	663
<i>Martin Peter, Sadiq Thomas and James Agajo</i>	
An Iterative k-means++ and Ant Colony Clustering Scheme for Vehicular Networks.....	668
<i>Kayode Popoola, David Grace, Tim Clarke and Muheeb Ahmed</i>	
An Evolutionary Approach Towards Achieving Enhanced Intrusion Detection System.....	673
<i>Olugbemiga Solomon Popoola, Ikechukwu Ignatius Ayogu, Olamatanmi Josephine Mebawondu, Chukwuemeka Christian Ugwu and Adebayo Ohusola Adetunmbi</i>	
Design and Implementation of Obstacle Detection And Warning System For Visually Impaired People.....	678
<i>Yusuf Sahabi Lolo, Kelechi Lawrence Ohammah, Amina Alfa, Halima Ginsau, Ali Obadiyah and Sadiq Abubakar</i>	
Modern Methods For Solving Weighted Minimum Spanning Tree Problems	683
<i>Ahmed Tijani Salawudeen, Bashir Baba Abba, Issaku Ibrahim, Muhammad Mustapha Muhammad and Tajudeen Humble Sikiru</i>	
The Impact of Communication Technologies On The Smart Grid.....	688
<i>Jaafaru Sanusi, Oghorada Oghenewogaga, Bukola Babatunde Adetokun and Aminu Muhammad Abba</i>	
Machine Learning Approach to Improving Operating System Process Scheduling	693
<i>Nasir Shehu Malami, Fidelis Onah, Fatima Imam, Kelechi Ohammah, Habiba Nasir Mohammed and Halima Ginsau</i>	
Quantum-resistant University Credentials Verification System on Blockchain.....	698
<i>Mahendra Shrivias, Srujan Kachhwaha, Ashok Bhansali and Satya Singh</i>	
Short Circuit Analysis of Benin Sub-Region 132 kV Transmission Network for Distance Protection Scheme	704
<i>Igberaese Simon, Jacob Tsado, Jonathan Kolo and Umar Dauda</i>	
Design of a 3.8-GHz Microstrip Patch Antenna for Sub-6 GHz 5G Applications.....	709
<i>Olugbenga Sowande, Francis E. Idachaba, Sunday C. Ekpo, Nasir Faruk, Noushin Karimian, Olugbenga Ogunmodimu, Abdulkarim A. Oloyede, Lukman A. Olawoyin and Sulyman A. Abdulkareem</i>	
IoT-Based Home Automation System with Covid-19 Detector	714
<i>Mariam Sulleiman and Jacob Tsado</i>	

Performance Analysis of OFDM signal using Different Modulation Schemes with Least Square Channel Estimation Technique.....	719
<i>Michael Tarerefa, Ayibapreye Kelvin Benjamin and Waterway Deinmodei</i>	
Performance Analysis of a PMSM for Traction Applications in Electric Vehicles with Hairpin Winding Technology.....	723
<i>Omokhafa Tola, Edwin Umoh, Ambafi James and Olusegun Osinowo</i>	
An Embedded Fuzzy Logic Based Smart Street Lighting System	728
<i>Geofrey Twesigye, Alexander Ngenzi and Emmanuel Ndashimye</i>	
A Bi-Factor Biometric Authentication System for Secure Electronic Voting System	733
<i>Buhari Ugbede Umar, Olayemi Mikail Olaniyi, Abisoye Blessing Olatunde, Ademoh Agbogunde Isah, Arifa Khatoon Haq and Isaac Taiye Ajayi</i>	
Towards Determining the Effect of Age and Educational Level on Cyber-Hygiene.....	738
<i>Celestine Ugwu, Casmir Ani, Modesta Ezema, Caroline Asogwa, Uchenna Ome, Adaora Obayi, Deborah Ebem, Aminat Atanda and Elochukwu Ukwandu</i>	
Performance Analysis of a Ball-on-Sphere System using Linear Quadratic Regulator Controller.....	743
<i>Abubakar Umar and Zaharuddeen Haruna</i>	
A Topology for Fingerprint Image Encryption based on HDWT-SVD and Hyperchaos	748
<i>Edwin Umoh and Ogechukwu Iloanusi</i>	
Chaos Theory Applied to Cascading Disaster Dynamics, Modelling and Control	753
<i>Edwin Umoh, Musa Umar and Muhammed Umar</i>	
A Simplified Method for Extended Duration Measurements of Mobile Broadband Performance	757
<i>Vincent Umoh, Ubong Ukommi and Unwana Ekpe</i>	
LoRa Network Planning Using Empirical Path Loss Models	762
<i>Uyoata Uyoata</i>	
Performance Analysis of a Dynamic Voltage Restorer using two Compensation Strategies for Voltage Sag Mitigation.....	767
<i>Shayan Zafar, Fredrick Nkado and Franklin Nkado</i>	



Mohammed Abdulmalik Danlami <drmalik@futminna.edu.ng>

NIGERCON 2022 review response (submission 56)

1 message

NIGERCON 2022 <nigercon2022@easychair.org>

Mon, Apr 11, 2022 at 4:41 PM

To: Abdulmalik Danlami Mohammed <drmalik@futminna.edu.ng>

Dear Abdulmalik Danlami,

Thank you for your submission to NIGERCON 2022. Following your provisional Acceptance, the NIGERCON 2022 rebuttal period will be between 7th April 2022 and 20th, April 2022. This is part of IEEE best practices, and we crave your indulgence.

During this time, you will have access to the current state of your reviews and have the opportunity to submit a response of up to reviewers comments in your revised camera ready.

Please keep in mind the following during this process:

- * The response must focus on any factual errors in the reviews and any questions posed by the reviewers. It must not provide new research results or reformulate the presentation. Try to be as concise and to the point as possible.
- * The rebuttal period is an opportunity to react to the reviews but is not a requirement to do so. Thus, if you feel the reviews are accurate and the reviewers have not asked any questions, then you do not have to respond.
- * The program committee will read your responses carefully and take this information into account during the discussions. On the other hand, the program committee will not directly respond to your responses, either before the program committee meeting or in the final versions of the reviews.
- * Your response will be seen by all PC members who have access to the discussion of your paper, so please try to be polite and constructive.

The reviews on your paper are attached to this letter. To submit your response you should log on to the EasyChair Web page for NIGERCON 2022 and select your submission on the menu.

Those that have already submitted camera-ready should complete this rebuttal form to complete the Final assessment and issuance of Final Acceptance letter.

----- REVIEW 1 -----

SUBMISSION: 56

TITLE: A Three-Step One-Time Password, Textual and Recall-Based Graphical Password for an Online Authentication

AUTHORS: Haruna Adamu, Abdulmalik Danlami Mohammed, Solomon Adelowo Adepoju and Abisoye Opeyemi Aderiike

----- Overall evaluation -----

SCORE: 0 (borderline paper)

---- TEXT:

A Three-Step One-Time Password, Textual and Recall-Based Graphical Password for an Online Authentication

The authors proposed the use of graphical passwords in combination with other second-level authentication methods as alternative to text-based passwords.

Introduction

This line needs to be rephrased: "One explanation for the surge in popularity of graphical passwords is because visuals, as opposed to strings of characters, are thought to be more remembered." Should rather be easy to remember and the use of the word surge should be substantiated with evidence.

There are quite a lot missing in the proposed method:

The usability testing did not use any known Technology Acceptance Model.

There was no specifications on tools used specifically for the security testing and how long the test lasted under different conditions.

The use of text-based passwords have been attractive because of ease of use and convenience. How convenient is a graphical password?

How does the use of graphical passwords different from Captcha as MFA system?

Of what advantage is graphical password system over emerging passwordless use cases?

There has been some research aimed at this domain, but implementation remains a daunting task because of convenience, ease of use, management, responsible innovations and adaptation.

----- REVIEW 2 -----

SUBMISSION: 56

TITLE: A Three-Step One-Time Password, Textual and Recall-Based Graphical Password for an Online Authentication

AUTHORS: Haruna Adamu, Abdulmalik Danlami Mohammed, Solomon Adelowo Adepoju and Abisoye Opeyemi Aderiike

----- Overall evaluation -----

SCORE: 2 (accept)

---- TEXT:

The following were observed:

The entire login process is time-consuming

The concept seems nice but, it appears it is already in use, how is this different from the existing?

Minor grammatical errors that need attention within the text.

The references and their usage is good.

Nice effort.

----- REVIEW 3 -----

SUBMISSION: 56

TITLE: A Three-Step One-Time Password, Textual and Recall-Based Graphical Password for an Online Authentication

AUTHORS: Haruna Adamu, Abdulmalik Danlami Mohammed, Solomon Adelowo Adepoju and Abisoye Opeyemi Aderiike

----- Overall evaluation -----

SCORE: 0 (borderline paper)

---- TEXT:

In this work authors propose a novel 3-stage authentication scheme. However, the description remains at a very superficial level, being that few technical details on security are missing.

Authors have made a basic mistake of english language. The expression "prone to" means that something has chances of occurring. For example, saying YES to "Prone to hidden camera attacks" means that your solution is easily attackable via hidden cameras. So, in table I, you solution would be the worst option. Fix this by replacing "Prone to" with "Prevents".

Also, in table I, authors report a login time of 82 Seconds. This is a very high value and should be improved. Users are not so patient...

----- REVIEW 4 -----

SUBMISSION: 56

TITLE: A Three-Step One-Time Password, Textual and Recall-Based Graphical Password for an Online Authentication

AUTHORS: Haruna Adamu, Abdulmalik Danlami Mohammed, Solomon Adelowo Adepoju and Abisoye Opeyemi Aderiike

----- Overall evaluation -----

SCORE: 1 (weak accept)

----- TEXT:

The manuscript presented a 3 step PTG authentication approach to online users. It has more robust features when compared with the existing techniques.

The manuscript is well written with focused coherence. Still, the methodology section requires expansion with the details of the adopted/adapted model(s) for the processes 1-3, such as the password combination of characters, its length, storage approach, matching technique, RNG for the OTP image processing technique as well as the justification for its choice. The selection process of the volunteers: age, gender....

What is the outcome when there are only 2 processes, and then 3 processes? It'd be suitable to state the 3 process combination mechanism: in parallel or series? How is the authentication score achieved and accepted

----- REVIEW 5 -----

SUBMISSION: 56

TITLE: A Three-Step One-Time Password, Textual and Recall-Based Graphical Password for an Online Authentication

AUTHORS: Haruna Adamu, Abdulmalik Danlami Mohammed, Solomon Adelowo Adepoju and Abisoye Opeyemi Aderiike

----- Overall evaluation -----

SCORE: 2 (accept)

----- TEXT:

1. The paper proposes a hybrid method of authentication to address the shortcomings of conventional user password
2. Provide some comments on the limitations of the proposed user authentication technique.

----- REVIEW 6 -----

SUBMISSION: 56

TITLE: A Three-Step One-Time Password, Textual and Recall-Based Graphical Password for an Online Authentication

AUTHORS: Haruna Adamu, Abdulmalik Danlami Mohammed, Solomon Adelowo Adepoju and Abisoye Opeyemi Aderiike

----- Overall evaluation -----

SCORE: 1 (weak accept)

----- TEXT:

This paper looks good but can only be provisionally accepted for presentation at the Conference subject to the authors reducing the Similarity Index (SI).

The SI of this paper is 46%. This MUST be reduced to 30% or less to qualify for IEEE Xplore inclusion and Conference proceedings. Revise the camera-ready alongside other reviewers' comments.

Best wishes,

Kennedy Chinedu Okafor, Ph.D., Fellow ASI, SMIEEE
Technical Program Committee
IEEE Nigercon2022

A Three-Step One-Time Password, Textual and Recall-Based Graphical Password for an Online Authentication

Haruna Adamu
 Department of Computer Science
 Federal University of Technology,
 Minna
 Minna, Nigeria
 harunaadamu1909@gmail.com

Abdulmalik Danlami Mohammed
 Department of Computer Science
 Federal University of Technology,
 Minna
 Minna, Nigeria
 drmalik@futminna.edu.ng

Solomon Adelowo Adepoju
 Department of Computer Science
 Federal University of Technology,
 Minna
 Minna, Nigeria
 solomon.adepoju@futminna.edu.ng

Abisoye Opeyemi Aderiike
 Department of Computer Science
 Federal University of Technology,
 Minna
 Minna, Nigeria
 o.abisoye@futminna.edu.ng

Abstract—Text passwords are the most extensively used technique of computer authentication. This approach has been found to have several flaws. Users, for example, typically select passwords that are simple to guess. A difficult-to-guess password, on the other hand, is also difficult-to-remember. Textual passwords are vulnerable to brute-force and keylogger attacks. Graphic passwords have been proposed in the literature as a possible replacement for alphanumeric passwords, based on the assumption that people remember pictures better than text. Existing graphical passwords, on the other hand, are vulnerable to a shoulder surfing assault. To solve these security flaws, this paper proposes an authentication method for online applications that uses a combination of one-time passwords, textual, and graphical passwords. The efficacy of the recommended solution was confirmed by usability testing and security analysis procedures. A total of thirty participants took part in the system evaluation. The security assessment found that the proposed system meets all its primary security requirements. The proposed system was found to be simple to use, friendly, and secure throughout the usability test. When compared to traditional authentication solutions, this study exhibited greater usability and security.

Keywords—Textual Password, One-Time Password, Graphical Password, Shoulder Surfing, Key-logging

I. INTRODUCTION

User authentication is a method for a device to confirm the identity of a person connecting to network resources. Textual passwords are the most often used form of authentication for all websites and applications. Textual passwords are made up of a string of letters and numbers, with or without special characters or integers. Users can usually log into several accounts with just one username and password [1]. They are not, however, fully safe. As a result, strong passwords with numbers, uppercase, and lowercase letters should be used. These textual passwords are then considered strong enough to survive brute force attacks. On the other side, a strong textual password is difficult to memorize and recall. Password replay and keylogger attacks are also possible with textual passwords [2].

To address the struggle with alphanumeric authentication, a significant variety of graphical password schemes have been devised and tested [3]. The prevalence of graphical passwords can be explained by the fact that pictures, rather than strings of characters, are easier to recall [4]. Graphical passwords are passwords that are made up of pictures or drawings. Because people remember pictures better than text, graphical passwords are easier to remember. They are also more resistant to brute-force attacks because the search space is practically infinite. In conclusion, graphical passwords are a superior option for memorability and usability than text-based passwords [5].

One of the shortcomings of using a graphical password system is the likelihood of shoulder surfing [6]. A graphical passcode could be physically seen, particularly in public places, and if the adversary has a clear visual of the passcode being inserted numerous times, they can easily crack it, which is a severe flaw [7]. Another drawback of using a graphical password is that it is susceptible to guessing. Just like with a textual password, if the user simply registers a brief and predictable password, the chances of it being guessable grow [1]. Some researchers have proposed the use of passwordless use cases like fingerprint verification [8]. However, if one of the fingers is used as a password, for instance, and it is compromised, it cannot be used again since altering a fingerprint is nearly impossible, therefore it is irreversibly compromised. There are several ways to avoid keyloggers, shoulder surfing, and guessing attacks, but none of them are sufficient in and of themselves. A combination of strategies must be employed to effectively eliminate the problem [9]. This study uses a combination of one-time passwords, textual and graphical passwords to combat shoulder-surfing, replay, and key-logging assaults. As a result, the research's main contributions are as follows:

1. Development of a secure one-time password system.
2. Development of a secure textual password authentication system.
3. Development of a secure graphical password authentication system.

The remainder of the paper is organized as follows: A synopsis of recent password authentication research is presented in the second section. Section 3 explains the study's approach. The results of the experiment, as well as the conclusions obtained, are discussed in Section 4. Section 5 summarizes the findings and considers potential future projects.

II. RELATED WORKS

To prevent shoulder surfing attacks, [10] recommended using a graphical password authentication (GPA) system. The proposed system combined textual and graphical passwords, removing the requirement for complex textual passwords that may be difficult to remember. Instead, with the graphical password in place, users can use any textual password. The type of graphical password method used in this study, however, was not mentioned. Furthermore, the usability of the suggested solution was not assessed.

A GPA scheme was suggested by [11]. This scheme was based on the finest existing features, such as distorted images, hash index, and loci metrics, as well as visual encryption algorithms and additional naive features, to protect against well-known threats such as brute-force, guessing, sniffing, hidden camera, shoulder surfing, and phishing. The paper's weakness, however, is that no assessment metric was used to evaluate the system's performance.

E-commerce authentication issues was solved by [12] using GPA. This paper proposes a modified Inkblot authentication mechanism. In the Inkblot authentication system, images are employed as a trigger for text password entering. During password generation, users can choose from a sequence of inkblots and type in the first and last letter of the phrase that best represents the inkblot. These pairs of letters make up the user's password. Users can utilize the inkblot to construct their own login. The drawback of this inkblot authentication mechanism is that users are limited to a small number of password alternatives.

A three-layer recall GPA technique with three layers of verification was proposed by [13]. The proposed recall-based authentication method improved on the Pass-Go approach, which featured secret questions, responses, and backdrop images. The suggested solution, known as CRS, consists of three components that work together to assure password security. The secret question and the text-based answer are the focus of the first part of the authentication phase. The second half focuses on choosing a picture based on recognition, and the third piece focuses on creating a password using an easy-to-remember artwork. The problem of this method is that while using sketching to construct a password, it is possible for individuals to forget their stroke order.

III. METHODOLOGY

This section provides an overview of the methods utilized to conduct the research. Fig. 1 illustrates the proposed solution, which is explored in greater depth in this section. Textual, one-time password, and graphical password are the three authentication modalities used in the proposed system, in that sequence.

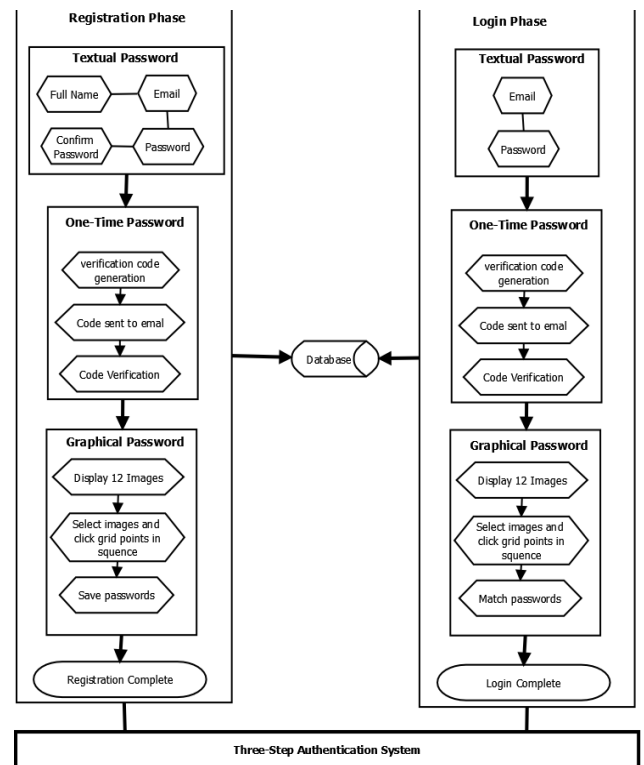


Fig. 1 Proposed System

The three-process combination mechanism was implemented serially to improve the password resistant given that a user or attacker cannot have access to the next password phase without been verified in the previous password phase.

A. Registration phase

The registration phase consists of three main processes: textual password, One-Time Password (OTP) and graphical password implementation.

- **Process 1: Textual Password Registration-** In this phase the user is asked to input their email, full name, password and confirm password.
- **Process 2: OTP Authentication-** The OTP authentication phase deals with the generation of OTP by the system. This generated OTP is sent the inputted email from the textual password registration phase. Then, the user is asked to input the OTP for verification. If the OTP is wrong user is denied access to the next phase, otherwise the user is granted access to the graphical password phase.
- **Process 3: Graphical Password implementation-** A 2×2 -image grid is now displayed to the user from which the user clicks on one point of the image. After that, the user must choose another image and click on the two-image grid that has been formed. After that, the user must choose another image and click on the 2×2 grid that has been formed.

B. Login Phase

After a user registers, the user can then login to gain access to the system. The steps involved the login phase is discussed below.

- **Process 1: Textual Password Authentication:** During the login phase, the user registered password

and email must be submitted which is compared with the email and password stored in the database. If email and password match, then the user is allowed to move to the next step.

- **Process 2: OTP Authentication:** in this step the user is asked to supply the OTP that was generated and sent to their registered email address. If a wrong OTP is supplied then, access is denied. However, if the OTP is correct the user is given access to the next authentication process.
- **Step 3: Graphical Password Authentication -** Twelve photos are displayed after the OTP dosage is authenticated. The user is asked to choose one of the photos on the screen. When a user clicks on a picture, a 2×2 grid containing sections of the selected image is presented. For successful authentication, the user is expected to click on the grid in the image. If the first attempt fails, the user is prompted to start over.

C. Textual Password Authentication

A textual password is a chunk of encrypted data that is used to validate a user's identity. It is commonly a string of alphabet, digits, or other symbols. Passwords used to be required to be recalled, but with the substantial number of password-protected services that the average individual uses, it's impossible to remember unique passwords for every site [1]. Shoulder-surfing, brute-force attacks, covert camera attacks, and malware attacks are all possible with textual passwords [2]. In this study, a minimum of 6 characters was required as textual passwords. These characters can be uppercase, lowercase, numbers, or special characters, but there was not restriction to their combinations. The user is allowed to use a single character type such as only numbers or combination of characters such as combining lowercase, numbers and uppercase. The user was allowed this flexibility given that the proposed system is protected by two additional layers of passwords (OTP and graphical passwords). For enhanced security the textual password was stored in the database in an encrypted form using the PHP password_hash function which is a strong one-way hashing algorithm. During the registration process to ensure that the entered password matches, the confirm password field was created.

D. One-Time Password (OTP)

An OTP is a one-time password that is automatically generated and utilized to authenticate users for a single transaction or login session. A fixed password is insecure compared to an OTP. To add an extra layer of security, OTPs can be used instead of or in addition to verification login credentials. OTP techniques frequently use pseudo-randomness and cryptographic hash functions to generate a shared key or seed, that can be utilized to extract a value but are hard to reverse, making it hard for an attacker to obtain the data used for the hash. The unexpected and unique nature of the pseudo-random value prevents password repeat attempts [14]. In this study the hash-based message authentication codes (HMAC) one-time password (HOTP) was used for OTP generation. The HOTP approach uses a growing counter value and a fixed symmetric key that is only known by the token and verification service [15]. The HMAC-SHA-1 technique is used to generate the HOTP value. Since the outcome of the HMAC-SHA-1 computation is 160 bits, the value was shortened to make it easier for the user to input using the formula in equation 1.

$$HOTP(K, C) = Truncate(HMAC - SHA - 1(K, C)) \quad (1)$$

The function Truncate transforms an HMAC-SHA-1 value to a HOTP value. The values of the Key (K), Counter (C), and Data are hashed high-order byte first. The HOTP method was selected because, unlike public key systems, the hash functions employed by HOTP are generated and verified quickly, and HMAC provides comparable security to digital signatures, despite the fact that digital signatures are bulkier than HMACs.

E. Recall-Based Graphical Password (Cued Click Point)

In this technique, the system gives users some pointers to help them precisely reproduce their passwords. These hints will display in the picture as hot spots [16]. To register as a passcode, the user must choose one of these regions, and then select the same region in the same sequence to log into the system. In this study, a recall-based technique called Cued Click Points (CCP) was used for user authentication. CCP users select a single point on each photo instead of many points on a single photo. It contains cued-recall and visual indicators that alert valid users if they input their most previous click-point incorrectly. It also complicates hotspot analysis assaults [17]. Cued recall of one point on each of the different photos appears to be simpler than memorizing an ordered series of different points on one image, which is a usability advantage of CCP.

F. Evaluation Metrics

1) *Usability testing:* The practice of evaluating software by putting it through its trials with real-world users is known as usability testing. Users are used to confirm that the system satisfies the stated requirements. As part of the usability metric, the login success rate, creation time, and login time were all assessed.

2) *Security Analysis:* The suggested system was evaluated based on its resistance to four common attacks: hidden camera, shoulder surfing, guessing, and key-logging.

IV. RESULTS AND DISCUSSION

This section details the proposed system's implementation, including registration and login procedure screenshots. It also details all of the tests carried out to assess the proposed system.

The first step of authentication, that is textual password is shown in Fig. 2 and 3. Fig. 2 is the signup page where the user registers their full name, email address and password. Fig. 3 is the first login page where the user inputs their registered email and password. On clicking on the login button, the supplied email and password is verified with the ones stored in the database.

Signup Form

It's quick and easy.

Full Name

Email Address

Password

Confirm password

Signup

Already a member? [Login here](#)

Fig. 2 Textual Password Registration Page

Login Form

Login with your email and password.

Email Address

Password

[Forgot password?](#)

Login

Not yet a member? [Signup now](#)

Fig. 3 Textual Password Login Page

The second step which is OTP authentication is presented in Fig. 4. The user is required to input the OTP code sent to their registered email. If the OTP code matches the sent OTP, then the user is allowed access to the last authentication phase displayed in Fig. 5. Fig. 5 is the graphical password authentication page, which displays 11 images for users to choose from. After selecting an image, that image is then divided into four parts as shown in Fig. 6.

Code Verification

We've sent a verification code to your email - haruna123@gmail.com

Enter verification code

Submit

Fig. 4 OTP Verification Page

Create New Account

Select the 1st image for the graphical password

Fig. 5 Graphical Password Page

Fig. 6 shows four sub-images of the selected image. The user is required to select one of these four sub-images. After clicking on one of the sub-images, the user is asked to select another image from the eleven initial images. The second selected image is then divided into four sub-images and the user is prompted to select from these sub-images

Create New Account

Following is the 1st image you chose.

Select one from below four parts.

Fig. 6 Grid of Selected Image

A. System Evaluation

In this study two types of evaluation (usability testing and security analysis) were conducted. The usability test was implemented using a questionnaire which was issued to the users after they used the system. The users were timed to get the login and creation time. For the security analysis, the hidden camera, shoulder surfing, and guessing attacks was

physically tested by researchers as they acted as intruders in these scenarios. The system was tested by 30 users. The users were within the age range of 18 to 35 years old. The users consist of 18 males and 12 females. Five users were master's degree students, while the remaining 25 users were undergraduate students. These volunteers were randomly selected to test the system. Two testing procedures was carried out. Firstly, the users were asked to use the system without been trained and secondly the users were asked to test the system after been trained on how to use the system.

1) *Usability Testing and Security Analysis*: The extent to which a product allows individual users to fulfill their specified goals efficiently, successfully, and satisfactorily in the particular context is referred to as usability. When developing a good graphical password strategy that meets the demands and requirements of its users, usability is a crucial thing to consider. This section defines and describes the primary usability aspects utilized in graphical passwords. These characteristics of usability are discussed in further depth farther down.

- **Easy to remember**: This implies that the system should provide passwords that are simple to remember.
- **Easy to Use**: This refers to the system's capacity to provide a good password-creation environment.
- **Easy to Create**: Means users can simply construct graphical passwords when the registration process is straightforward.
- **Easily Executed**: When the registration and login process is broken down into basic steps, people can easily perform the algorithm.
- **Nice and Simple Interface**: It emphasizes on the user's interactions in addition to making the interface pleasant. A nice and simple interface's purpose is to make user interactions as efficient and simple as possible.
- **Creation Time**: How long does it take an average user to finish the registration process?
- **Login Time**: How long does it take an average user to finish the login process?
- **Login Success Rate**: the percentage of users that completed the login job successfully.

The system's usability testing based on the eight defined features and security analysis based on four common attacks are presented in Table 1.

TABLE I. USABILITY TESTING AND SYSTEM ANALYSIS

	Attributes	[12]	[18]	Proposed System
Security Analysis	Prevents hidden camera attacks	Yes	No	Yes
	Prevents shoulder surfing attacks	Yes	No	Yes
	Prevents guessing attacks	No	No	Yes
	Prevents keylogger attacks	No	Yes	Yes
	Easy to remember	Yes	No	Yes
	Easy to Use	Yes	Yes	Yes

Usability features	Easy to Create	Yes	No	Yes
	Easily Executed	Yes	Yes	Yes
	Nice and Simple Interface	Yes	Yes	Yes
	Creation Time	-	94.08 Seconds	73 Seconds
	Login Time	-	57.40 seconds	46 Seconds
	Login Success rate	-	90.38%	90%

Table I shows that the suggested system is immune to assaults such as concealed cameras, shoulder surfing, guessing, and key-loggers. While [12] is prone to hidden camera, shoulder surfing and resistant to guessing, and keylogger attacks. [18] is resistant to hidden camera, shoulder surfing, guessing, but prone to keylogger attack. However, the proposed system is resistant to hidden camera, shoulder surfing, guessing, and keylogger attacks.

The registration and login were tested by trained and untrained users. It was noticed that as users were trained the creation and login time got reduced from 111 seconds for creation time to 73 seconds and from 82 seconds to 46 seconds for login time. The high value of login and creation time achieved by the proposed system is due to the time spent by users in accessing their emails to retrieve the OTP code. Before the users were trained the login success rate was about 85%. Nonetheless this value increased to 90% after they were trained. The high login success rate shows that the users of this proposed system are more likely to remember their passwords. Based on the usability features the proposed system takes shorter time to register and login than the system proposed by Mackie [18]. The proposed system is highly usable than previous systems. The proposed system is limited to the availability of users having access to emails and this can cause delay to the authentication process.

V. CONCLUSION AND FUTURE WORK

In this study, user authentication for online application access was accomplished using textual, OTP, and recall-based graphical password techniques. The user authentication procedure is made up of the registration and login phases. The registration procedure employs OTP to validate the user's email address, collects the user's text password, and captures the user's graphical password in a sequential order. The login step validates a user's identification by using the provided email, password, OTP, and graphical password sequence to enable access to an online application. Finally, to provide a solution for user authentication for online applications, a three-step authentication technique was adopted. Authentication employing these combined mechanisms provided a greater and more reliable level of security than conventional textual and graphical password systems, which are prone to shoulder surfing attacks.

The study made use of the cued click point recall-based graphical password technique for authentication. For future work other graphical password methods such as the recognition-based authentication can be used in combination with text, and OTP password.

REFERENCES

- [1] A. Fulkar, S. Sawla, Z. Khan, and S. Solanki, "a Study of Graphical Passwords and Various Graphical Password Authentication Schemes," *World Research Journal of Human-Computer Interaction ISSN: 2278-8476*, vol. 1, no. 1, pp. 4–8, 2012.
- [2] R. S. Yenape and A. Waghmare, "Three Way Graphical Password Authentication," *Iarjset*, vol. 4, no. 4, pp. 155–157, 2017, doi: 10.17148/iarjset/nciarcse.2017.45.
- [3] R. S. Jadhav, D. K. Chandole, M. D. Wani, S. R. Kuslkar, K. G. Shinde, and M. S. Dighe, "Graphical Password Authentication System," *International Journal of Latest Technology in Engineering, Management & Applied Science*, vol. 3, no. 3, pp. 64–68, 2014.
- [4] D. Kadu and S. Therese, "Different Graphical Password Authentication Techniques," no. March, pp. 56–58, 2017.
- [5] A. Vaddeti, D. Vidiyala, V. Puritipati, R. B. Ponnuru, J. S. Shin, and G. R. Alavalapati, "Graphical passwords: Behind the attainment of goals," *Security and Privacy*, vol. 3, no. 6, p. e125, Nov. 2020, doi: 10.1002/SPY2.125.
- [6] M. O. Kenneth and S. M. Olujuwon, "Web Application Authentication Using Visual Cryptography and Cued Clicked Point Recall-based Graphical Password," *Journal of Computer Science Research*, vol. 3, no. 3, Aug. 2021, doi: 10.30564/jcsr.v3i3.3535.
- [7] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, "Multi-factor authentication: A survey," *Cryptography*, vol. 2, no. 1, pp. 1–31, 2018, doi: 10.3390/cryptography2010001.
- [8] A. T. B. Jin, D. N. C. Ling, and A. Goh, "Biobhashing: two factor authentication featuring fingerprint data and tokenised random number.," *Pattern recognit.*, vol. 37, no. 11, pp. 2245–2255, Nov. 2004, doi: 10.1016/j.patcog.2004.04.011.
- [9] C. Santwana, "Hypervisor based Mitigation Technique for Keylogger Spyware Attacks," *International Journal of Computer Science and Information Technologies*, vol. 5, no. 2, pp. 1867–1870, 2014.
- [10] S. Abhijith, S. Sam, Sreelekshmi K U, and T. T. Samjeevan, "Web based Graphical Password Authentication System," *International Journal of Engineering Research & Technology*, vol. 9, no. 7, pp. 29–32, 2021, [Online]. Available: www.ijert.org
- [11] A. Vaddeti, D. Vidiyala, V. Puritipati, R. B. Ponnuru, J. S. Shin, and G. R. Alavalapati, "Graphical passwords: Behind the attainment of goals," *Security and Privacy*, vol. 3, no. 6, 2020, doi: 10.1002/spy2.125.
- [12] A. H. Shnain and S. H. Shaheed, "The use of graphical password to improve authentication problems in e-commerce," *AIP Conference Proceedings*, vol. 2016, no. September, 2018, doi: 10.1063/1.5055535.
- [13] B. Togookhuu and J. Zhang, "New Graphic Password Scheme Containing Questions-Background-Pattern and Implementation," in *Procedia Computer Science*, 2017, vol. 107, pp. 148–156. doi: 10.1016/j.procs.2017.03.071.
- [14] S. Ma *et al.*, "An empirical study of SMS one-time password authentication in android apps," in *PervasiveHealth: Pervasive Computing Technologies for Healthcare*, Dec. 2019, pp. 339–354. doi: 10.1145/3359789.3359828.
- [15] H. Parmar, N. Nainan, and S. Thaseen, "GENERATION OF SECURE ONE-TIME PASSWORD BASED ON IMAGE AUTHENTICATION," *Computer Science & Information Technology*, vol. 07, no. 1, pp. 195–206, 2012, doi: 10.5121/csit.2012.2417.
- [16] P. G. Panduranga Rao, "A Study of Various Graphical Passwords Authentication Schemes Using Ai Hans Peter Wickelgren Approach," *IOSR Journal of Computer Engineering*, vol. 10, no. 6, pp. 14–20, 2013, doi: 10.9790/0661-1061420.
- [17] V. Moraskar, S. Jaikalyani, M. Saiyyed, J. Gurnani, and K. Pendke, "Cued Click Point Technique for Graphical Password Authentication," vol. 3, no. 1, pp. 166–172, 2014.
- [18] I. Mackie and M. Yildirim, "A Novel Hybrid Password Authentication Scheme Based on Text and Image," in *32nd Annual IFIP WG 11.3 Conference, DBSec 2018*, 2018, pp. 1–16.