

Pilot study on deploying a wireless sensor-based virtual-key access and lock system for home and industrial frontiers

Andrew Okonji Eboka¹, Fidelis Obukohwo Aghware², Margaret Dumebi Okpor³,
Christopher Chukufunaya Odiakaose⁴, Ejaita Abugor Okpako², Arnold Adimabua Ojugo⁵,
Rita Erhovwo Ako⁵, Amaka Patience Binitie¹, Innocent Sunny Onyemenem¹,
Patrick Ogholuwaremi Ejeh⁵, Victor Ochuko Geteloma⁵

¹Department of Computer Science, Federal College of Education (Technical), Asaba, Nigeria

²Department of Computer Science, University of Delta Agbor, Agbor, Nigeria

³Department of Cybersecurity, Faculty of Info Technology, Delta State University of Science and Technology, Ozoro, Nigeria

⁴Department of Computer Science, Faculty of Computing, Dennis Osadebay University, Asaba, Nigeria

⁵Department of Computer Science, Federal University of Petroleum Resources Effurun, Warri, Nigeria

Article Info

Article history:

Received May 28, 2024

Revised Nov 21, 2024

Accepted Dec 3, 2024

Keywords:

Door access automation

Home security

Internet of things

Virtual key lock

Wireless sensor network

ABSTRACT

The rise in data processing activities vis-à-vis the consequent rise in adoption and adaptation of information and communication tech related approaches to resolve societal challenges has become both critical and imperative. Virtualization have become the order of the day to bridge various lapses of human mundane tasks and endeavors. Its positive impacts on society cannot be underestimated. This study advances a virtual wireless sensor-based key-card access system with cost-effective solution to manage access to restricted areas within a facility. We seek to integrate virtual key card access, web-access control, solenoid lock integration, and ESP32-controller to create a dependable internet of things (IoT)-enabled access control system. Results show system benefit includes improved security, improved convenience, privacy, efficiency with real-time control capabilities that will allows building administrators to track and manage access to the facility remotely.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Andrew Okonji Eboka

Department of Computer Science, Federal College of Education (Technical)

Asaba, Delta State, Nigeria

Email: eboka.andrew@fcetasaba.edu.ng, ebokaandrew@gmail.com

1. INTRODUCTION

Today, doors are designed to keep intruders out of both public and private infrastructures with locks neatly installed as security measures to help achieve this [1], [2]. Doors are installed and used in both hotel, homes, and office – to mention a few, as its mundane function is to either grant access to authorized persons, or keep out intruders cum strangers from restricted areas. Thus, facility managers utilize doors as security measure that prevents unauthorized access to unauthorized users [3], [4]. A predominant challenge facing many individuals and businesses today – is the security of both infrastructure, properties and lives [5], [6] as secure platforms require secure protocols as necessary measures to yield high-end user trust and requisite protection canvassed for [7]. Advances in informatics technology has made it imperative to adopt and adapt such emergent techs in almost every facet of life's endeavor; whilst, ensuring a consequent adaptation of the requisite imperative security measures [8]–[10] therein such facilities.

Administrators of such facilities and infrastructure today – have commenced the exploration and adoption of new technology targeted at advancing security protocols and measures that both dissuades

unauthorized access as well as ensure that legitimate users are not prevented access to such workspaces. This has become a crucial design component in modern homes over time [11], [12]. Advances made generally to provision better living from inception, is targeted at utilization of imaginary locks that protects user privacy as well as user's personal property [13], [14]. Its consequent improvement has continued to ensure greater protection overtime. So many of such door security protocols currently in place have also successfully, proven to be somewhat insecure, unreliable and are easily bypassed by adversaries.

With many doors often left unlocked from forgetfulness and other reasons – it is become imperative and critical to provide smart-locks [15], [16] which seeks to explore and exploit the use of embedded systems with internet-capabilities [17] via the use of key-codes, smart-phones, and key-cards – as means to ensure safety and ease user-trust of lock systems, and this agrees with [18], [19]. Also, a majority of devices used in such lock-system [20] are riddled with flaws that adversaries and intruders, also exploit to gain unauthorized access to barred locations [21]. In our effort to close these security gaps, our study employs the use of cryptographic [22] to provide extra layers and improved security for the virtual key-card lock system.

2. LITERATURE REVIEW

2.1. Review of related literature

Kong *et al.* [23] designed an radio frequency identification (RFID)-based automatic access control system that employed its universal serial bus (USB) as an effective means to communicate/interface with a host computer machine using the peripheral interface controller (PIC) 16f877A [24]. Its graphic user interface program provides functionalities of the overall system such as display of live ID tag transactions, registering ID, deleting ID, recording attendance, and other functionalities. It was deployed using Visual Basic 2010 with feature for registering and deleting ID makes the system more flexible but the system lacks facilities for true user identification such as a camera, and fingerprint scanner [25]. An improvement that can be made to this system is the use of an RFID fingerprint scanner instead of a tag to rule out the possibility of unauthorized access [26], [27]. Yuan and Xu [28] presented an Android-based control system to maintain the security of the home's main entrance and also the car door lock. The system can also control the overall appliances in a room. The mobile-to-security system or home automation system interface is established through Bluetooth. The hardware part is designed with the PIC microcontroller.

Joshi *et al.* [29] extended Joshi and Vaghela [30] for smart home technology using bluetooth in a mobile device. This Bluetooth-based Android smartphones was prototyped, and the hardware design for its door-lock system is the combination of an android smartphone features such as the taskmaster, Bluetooth module as command agent, Arduino microcontroller was used as its controller and data processing center, and solenoid as door lock output. Nasir *et al.* [31] also presented and analyzed the design and implementation of a microcontroller-based home security system using the global system for mobile communications (GSM). It used 3-microcontrollers to extend/expand the functionalities in other peripherals such as light emitting diode (LED), LCD, Buzzer, and a GSM module are responsible for the reliable operation of the proposed security system [31], [32]. Sun *et al.* [3] extended Nasir *et al.* [31] developed two remote monitoring systems using a cell phone with a focus on wider utilization. The first system is designed with an ARM LPC 2148 microcontroller based on commands received from the user's cell phone and presents sensor conditions to the LPC 2148 microcontroller system to sends signals via its ports to switch appliances on/off; While, its second system incorporates some additional features like capturing and store of an intruder's images unknown to him/her [33]. Zawislak *et al.* [34] investigated the automatic password-based door lock using electronic technology to build an integrated, fully customized home security system at a reasonable cost. The project is useful in keeping thieves and other sorts of dangers at bay [34], [35].

Kim *et al.* [24] extended Bhavani and Mangla [36] via RFID-based automatic access control system that used a USB as an effective means to communicate/interface with a host computer machine using the PIC 16f877A. They extended its user interface to yield greater functionalities of the overall system such as display of live ID tag transactions, registering ID, deleting ID, recording attendance, and other functions [37]. The embedded system features registration and deletion of IDs makes the system more flexible but the system lacks facilities for true user identification via Computer Vision model view to rule out the possibility of unauthorized access [38], [39]. Designed a password-protected home automation system with an automatic door lock using the Arduino board as controlled by ATmega-328. First, the user combination will be compared with the pre-decided passwords stored in the system memory [40]. If the user's combination matches the password, the door, light, and fan will be unlocked [41]. The system was built to be locked by just pressing a key. It used the Arduino board to interface various peripherals. If the password is matched with a pre-decided password, then the Arduino simply operates the relay to open the lights and fan. The Arduino simultaneously operates a DC motor via a motor driver for operating the door [42]–[44].

2.2. Wireless sensor networks

Wireless sensor networks (WSN) are fastidious in their adoption and extension of virtual technology. Virtual techs today, are used by many systems globally to include a variety of automation ranging from virtual remote-based light controllers, smart interfaces and many more. At its core is the embedded system that can adjusted with little modification to actualize virtual assistive techs. These can also be retrofitted to fully utilize our mobile devices capabilities. In all, they raise the quality of life for individuals who use these systems [45], [46]. Due to fast-paced advances in technology, smart key-cards are providing users with a variety of options to creating cost-effective, robust, flexible and low-maintenance virtualization solutions, there has since become a rise in the trend in the adoption and adaptation of such virtualization solution due to their dynamism and high-evolution [47]–[49].

Businesses and homes today, that integrate the use of physical servers with onsite/off-site locations will often profit from low-cost implementation, reduced maintenance cost, improved administration and over-simplification that accompanies a virtualized server databanks and environment [50], [51]. Through such shared resources, virtualization enables the expansion of hardware [52]–[54]. A plethora of restrictions often accompany such virtual systems – one critical component being the dearth of possibilities that can be brought together in one location [55], [56]. Furthermore, there is also the lack of high-security choices. To resolve such problem, we wish to combine all the current (security features, safety features, and monitoring functions) into a single, virtual smart-lock. This will thus, yield a highly-secured system that seeks to bridge the gaps in frontier door security options without conflict – to make our homes safer than before [57]–[59]. Thus, intelligent security systems evolve and are deployed to forestall illicit invasions of user privacy. Study aims to provide security protocols for adoption in a door lock system with a single-key for one-lock phenomenon [60], [61].

2.3. Study motivation

The study is motivated as listed below, and seeks to achieve the following:

- a) **Security:** to ensure that virtual keycard door lock system(s) are secured from unauthorized access, adversary hacking, and tampering – security has become a critical component and challenge facing the development and deployment of the smart virtual keycard door lock system. While, it can be applied to other aspects of our daily endeavour, the secured smart keycard door lock system must aim at provisioning secure protection for user sensitive and personal user information as well as prevent unauthorized access to such secure buildings and facilities [62], [63].
- b) **Privacy integration with internet of things (IoTs):** a key challenge in the deployment of IoT-based and enabled systems is that of privacy from adversarial attacks, threat cum unauthorized-to-compromised access. To enhance user-trust and privacy, such IoT-based lock mechanisms are linked and connected to the internet via smart mobile devices. This is aimed at ensuring the generated system is robust, productive and innovative [64], [65].
- c) **Low-cost energy solutions:** deploying for use, virtual keycard lock often makes it energy-efficient, it reduces its implementation cost, and ensures it is at a cheaper cost of maintenance. While, cheaper maintenance is not a panacea for improved system reliability – its use is very restrictive so that only a few clients, individuals or organizations can afford it. Biometric systems often have been found to violate users' privacy as some users often consider them to be personally invasive due to loss of anonymity [66].
- d) A key challenge that is faced in this project is the security and privacy of the IoT systems. Therefore, the paper will present an extensive investigation of the security and privacy of IoT systems seeking to enhance the lock mechanism by connecting it to the internet, making it more robust, productive, and innovative.

The study achieves improved security, user data privacy, improved user-trust, energy efficiency and low-power computation via the deployment of a smart, virtual keycard door lock using the IoT-enabled device(s).

2.4. The experimental virtual key-card wireless sensor model

The existing output design for the smart virtual door access primarily revolves around a seamless and efficient user experience. A user successfully taps their near field communication (NFC)-enabled device (smartphone or smartcard) on the NFC reader located near a door, which triggers the system door either lock to unlock as seen in Figure 1. Upon successful access, the door lock emits an audible signal to indicate an unlock state, with immediate feedback to the user. This design ensures the entire access is swift and easy to allow users access their rooms effortlessly [67], [68]. The system generates a backend server access log with these feats: (a) timestamp of access, (b) the used NFC device unique identifier, and (c) the room number accessed. These logs are accessible via the administrative interface, allowing hotel staff to monitor and review access activities in real-time. The output design of the access logs facilitates data analysis, enabling hotel management to gain valuable insights into guest behaviours and occupancy patterns.

The experimental scheme seeks to enhance hotel room access control via the integration of advanced secure, access tokens technology with user-friendly features. With the existing system, the proposed system addresses many of its identified weaknesses with the advent of new functionalities. All of which seeks to improve user experiences and operational efficiency. With a focus on device compatibility, the system allows guests to access their rooms using a wide range of NFC-enabled devices, including smartphones, smartwatches, and smartcards. It uses an advanced two-factor authentication and data encryption as security measures to ensure the utmost protection of user data alongside access to user credentials. Also, it provides a fail-safe that seamlessly integrates these features on to the hotel infrastructure; and thus, guarantees the continuous access control even in the event of system failures or connectivity issues.

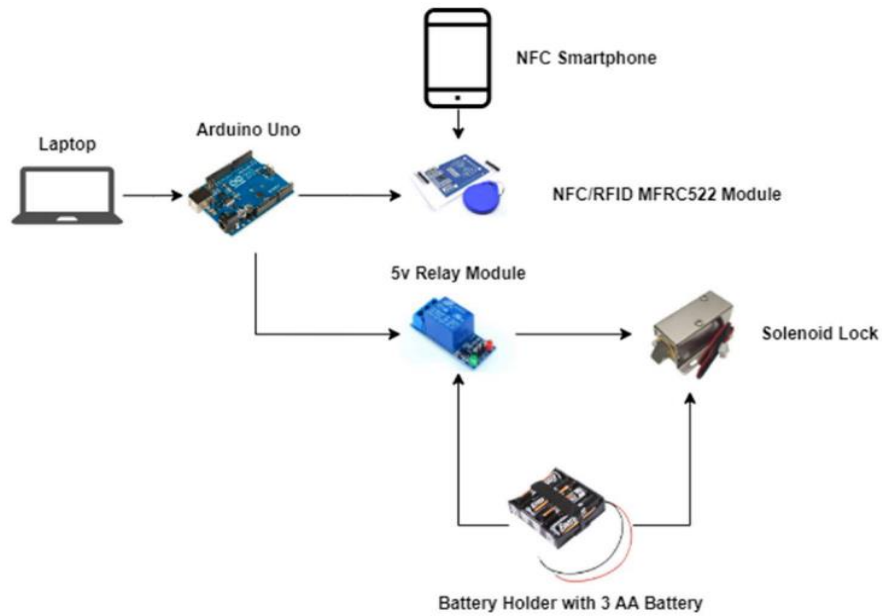


Figure 1. Schematics of the virtual wireless sensor key-card model

The proposed system's intuitive app as in Figure 2, and its administrative interface streamlines the check-in process, and empowers guests to manage their access effortlessly and enabling hotel staff to efficiently handle access permissions and monitor real-time access logs. The proposed virtual key card system promises an enhanced guest experience, heightened security, and improved operational efficiency for modern, tech-savvy hotels as in Figure 2. Which shows circuitry diagram of the proposed system with its structural workings and the schematic diagram of the proposed virtual key-card system as in Figure 3.

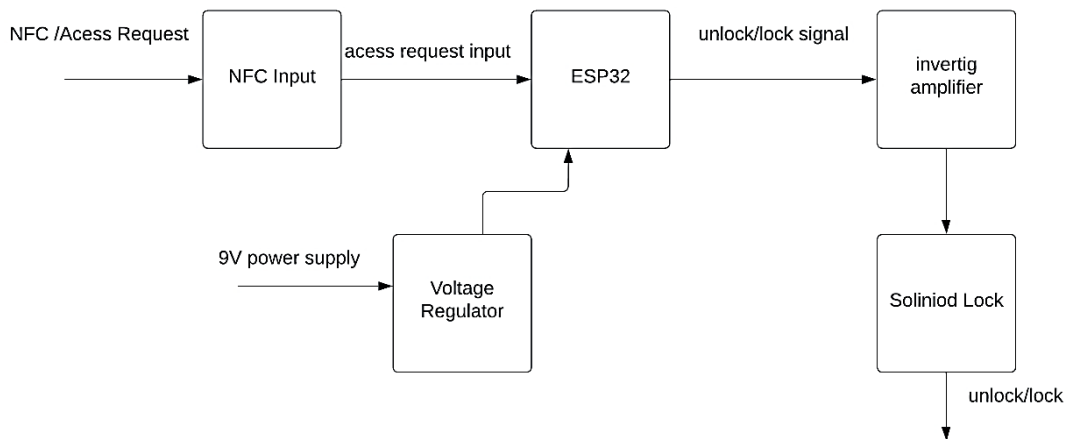


Figure 2. Circuitry diagram of the experimental system

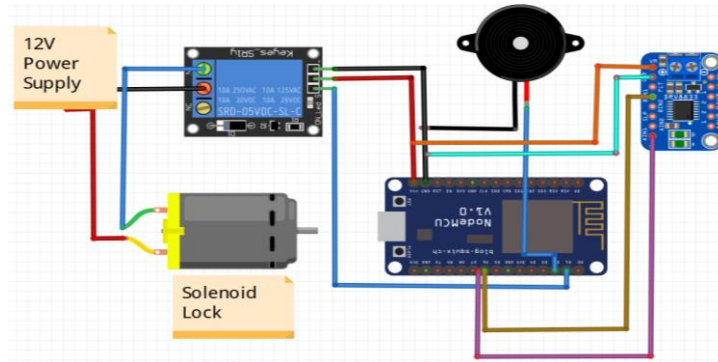


Figure 3. Schematic diagram of the experimental system

Major benefits the proposed system offers will include: (a) an enhanced device compatibility, supports a wide range of NFC-enabled devices for seamless access, (b) advanced security measures, including two-factor authentication and data encryption, ensure robust protection against unauthorized access and data breaches, (c) a fail-safe mechanism that provides continuous access control, even with system failure or network connectivity issues, (d) an equally streamlined integration with existing hotel infrastructure facilitates efficient data synchronization and operations, (e) an intuitive user interface simplifies guest check-ins and eases management of access permissions for both hotel staff and ancillary personnel, (f) improved guest experience with convenient room access using preferred NFC devices, and (g) improved security will improve user-trust, confidence level and safeguards personal information as in Figure 3 which shows the circuit construction of the proposed system architecture.

The proposed system specifications accounted for flexibility, security, robustness and privacy. We used the ESP32 microcontroller due to its powerful capabilities with built-in WiFi and Bluetooth connectivity – both of which are essential for IoT applications. We also integrated a GSM module for usage in areas without internet access. Also, incorporated was the solenoid lock, which will be activated by the microcontroller in response to the appropriate input signals. The system integrated a web-based user-friendly interface that allows users to register and manage their virtual key cards. The system also has robust security features to prevent unauthorized access, including encrypted communication between the microcontroller and the server. The system used a cloud-based server to allow remote management. It uses a card reader for the RFID or NFC tags on the virtual key cards. It yields a display on the web app to provide feedback to users, indicating whether access has been granted or denied. The solenoid lock is designed to withstand tampering, and the entire system is housed in a secure enclosure to prevent unauthorized access.

3. FINDINGS AND RESULT DISCUSSION

3.1. Experimental system performance and evaluation

Table 1 shows the performance test result and indices from the system as generated. Table 1 shows performance result of integrating the virtual key-card with IoT and embedded system as used to control a door lock. Results showed system's efficiency and effectiveness as compared to [69], [70]. We also evaluated several key metrics to include access control speed, reliability, and user convenience respectively – as in agreement with [71]. The access control speed was evaluated by measuring the time it took for the system to either grant or deny access to the door lock. The proposed system was found to be fast and responsive, with both granting of and the denial of access to unlock features in less than a second. This quick response time allowed for smooth and efficient access management. This is in agreement with [72]–[74].

Table 1. Performance evaluation for the experimental system

| Test description | Actual results | Remark |
|---|---|--------|
| Successful access using authorized NFC tags | The door unlocks upon presenting an authorized NFC tag | Pass |
| Failed access via unauthorized device access | Door remained lock upon presenting an unauthorized device | Pas |
| Failed access using invalid NFC tag | Door remains locked upon presenting invalid NFC tags | Pass |
| Error handling for invalid NFC tag | Displays correct error message on the web application and serial monitor upon presenting an invalid NFC tag | Pass |
| Compatibility with the different types of NGFC tags | System is able to read and grant access to different types of NFC tags | Pass |

Furthermore, we tested for reliability by testing the system's ability to accurately read the virtual key cards and control the locks based on the access rights defined in the web application. The system was found to be reliable, with no instances of incorrect access granted or denied. The locks were also found to be secure and reliable, able to withstand physical stress and external tampering. User convenience was evaluated by assessing the ease of use of the virtual key cards and the web application. The virtual key cards were found to be easy to use, with no special skills or knowledge required. The web app is user-friendly and intuitive, with a simple and straightforward interface, which agrees with [75]–[77].

3.2. Discussion of findings

Table 2 shows findings using a variety of the indices from the system. We evaluated using these features to include the following: (a) access control [78], (b) scalability [79], (c) reliability [80], (d) error handling [49], (e) users' usability convenience and satisfaction [81], (f) compatibility with several NFC devices [82], and (g) fault tolerance [83].

Table 2. System test results

| Test metrics | Description | Result |
|--------------------------------|--|---|
| Access control speed | The time it takes for the system to grant or deny access to the door to any user | It takes an average of 1.8 seconds for access to be granted if the tag is used, and 1.1 secs if the web-request is used |
| Physical security | The system's ability to withstand physical stress and external tampering | Resistant to external tampering and physical stress, with no reported incidents of unauthorized access or damage |
| Reliability | System's ability to accurately read the virtual key-card and control the locks based on the access rights defined in the web-application | System had 99.5% accuracy in reading key-card, controlling the locks to lock/unlock states based on access rights defined in the web app |
| User convenience | The ease with which a user uses the virtual key-card and web application | Users found the virtual key cards and web apps quite easy to use and convenient, with no major use issues or complaints |
| System fault tolerance | The system's ability to operate reliably over a prolonged period of time | The system operated reliably over a prolonged period of time, with no reported incidences of downtime and failure to access the network |
| System compatibility with NFCs | It describes how compatible system is with the plethora of other devices with NFC capabilities such as laptops, smartphones | System is compatible with devices and techs that incorporated WIFI, Bluetooth and NFCs |
| Error handling | System's ability to support a large number of users and access points, handle concurrent requests, invalid NFC tags and WiFi connectivity issues | The system supports a large number of client and user access points with no performance degradation and security issues reported |
| Scalability | Ability to support large number of users and access points, handle concurrent requests, invalid NFC tags and WiFi connectivity issues and not compromise performance and/or security | System was found to support large number of client and user-access points without any form of performance degradation and/or security issues reported |

The system yields a 99.5% accuracy in reading the virtual key-card and in controlling the lock/unlock states based on defined access-rights in the web app. The system yields fault-tolerance and is compatible with many NFC tags and accompanying devices, to agree with [84], [85]. We successfully used an ESP32, a solenoid lock, a web API, and a web app to manage the access of authorized personnel [86]–[88]. It yields several benefits like increased security, efficiency, and convenience, which agrees with [89]. It also eliminates the challenges associated with traditional key like risk of lost or stolen keys, the inconvenience of having to carry physical keys, and the lack of real-time access control and monitoring. It allows authorized personnel to access designated areas without the need for physical keys, reducing the risk of lost or stolen keys [90], [91].

The system provides real-time access control and monitoring, allowing administrators to track and manage access to the facility remotely [92]–[94]. This study can be advanced to include additional features, such as facial recognition and voice recognition, to enhance the security of the system. The study has also contributed by demonstrating the inherent potentials in the use of IoTs/embedded systems to provide innovative solutions to complex problems in various industries.

4. CONCLUSION

The system yields a cost-effective solution to manage user access integrating IoTs to create a comprehensive access control system. Its many benefits over traditional key includes better security, user data privacy, system efficiency, and user convenience. The system also provides real-time monitor and control capabilities that will allow administrators to track and manage access to the facility remotely. And in turn, enhancing system's security and efficiency.

REFERENCES

- [1] R. Sreevas, R. Shanmugasundaram, and V. S. Vadali, "Development of an iot based air quality monitoring system," *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 10 Special Issue, pp. 23–28, Sep. 2019, doi: 10.35940/ijtee.J1004.08810S19.
- [2] E. U. Omede, A. E. Edje, M. I. Akazue, H. Utomwen, and A. A. Ojugo, "IMANoBAS: an improved multi-mode alert notification iot-based anti-burglar defense system," *Journal of Computing Theories and Applications*, vol. 1, no. 3, pp. 273–283, Feb. 2024, doi: 10.62411/jcta.9541.
- [3] D. Sun, M. Liu, M. Li, Z. Shi, P. Liu, and X. Wang, "DeepMIT: a novel malicious insider threat detection framework based on recurrent neural network," in *Proceedings of the 2021 IEEE 24th International Conference on Computer Supported Cooperative Work in Design, CSCWD 2021*, May 2021, pp. 335–341, doi: 10.1109/CSCWD49262.2021.9437887.
- [4] N. Mazitelli, "Insider threats," *Engineering & Technology Reference*, 2015, doi: 10.1049/etr.2015.0045.
- [5] S. R. Guntur, R. R. Gorrepati, and V. R. Dirisala, "Internet of medical things," *Medical Big Data and Internet of Medical Things*, no. February, pp. 271–297, Oct. 2018, doi: 10.1201/9781351030380-11.
- [6] A. O. Eboka and A. A. Ojugo, "Mitigating technical challenges via redesigning campus network for greater efficiency, scalability and robustness: A logical view," *International Journal of Modern Education and Computer Science*, vol. 12, no. 6, pp. 29–45, 2020, doi: 10.5815/ijmecs.2020.06.03.
- [7] A. Jadon, M. Omama, A. Varshney, M. S. Ansari, and R. Sharma, "FireNet: a specialized lightweight fire and smoke detection model for real-time IoT applications," May 2019, [Online]. Available: <http://arxiv.org/abs/1905.11922>.
- [8] P. Filippi *et al.*, "An approach to forecast grain crop yield using multi-layered, multi-farm data sets and machine learning," *Precision Agriculture*, vol. 20, no. 5, pp. 1015–1029, Oct. 2019, doi: 10.1007/s11119-018-09628-4.
- [9] A. A. Ojugo and D. O. Otakore, "Intelligent cluster connectionist recommender system using implicit graph friendship algorithm for social networks," *IAES International Journal of Artificial Intelligence*, vol. 9, no. 3, pp. 497–506, 2020, doi: 10.11591/ijai.v9.i3.pp497-506.
- [10] R. E. Yoro, F. O. Aghware, M. I. Akazue, A. E. Ibor, and A. A. Ojugo, "Evidence of personality traits on phishing attack menace among selected university undergraduates in Nigerian," *International Journal of Electrical and Computer Engineering*, vol. 13, no. 2, pp. 1943–1953, Apr. 2023, doi: 10.11591/ijece.v13i2.pp1943-1953.
- [11] D. Lin, "Insider threat detection: Where and how data science applies," *Cyber Security: A Peer-Reviewed Journal*, vol. 2, no. 3, p. 211, 2018, doi: 10.69554/qyap6773.
- [12] R. E. Yoro, F. O. Aghware, B. O. Malasowe, O. Nwankwo, and A. A. Ojugo, "Assessing contributor features to phishing susceptibility amongst students of petroleum resources varsity in Nigeria," *International Journal of Electrical and Computer Engineering*, vol. 13, no. 2, pp. 1922–1931, Apr. 2023, doi: 10.11591/ijece.v13i2.pp1922-1931.
- [13] I. Agraftiotis, J. R. Nurse, O. Buckley, P. Legg, S. Creese, and M. Goldsmith, "Identifying attack patterns for insider threat detection," *Computer Fraud and Security*, vol. 2015, no. 7, pp. 9–17, 2015, doi: 10.1016/S1361-3723(15)30066-X.
- [14] M. Al-Qatf, Y. Lasheng, M. Al-Habib, and K. Al-Sabahi, "Deep learning approach combining sparse autoencoder with SVM for network intrusion detection," *IEEE Access*, vol. 6, pp. 52843–52856, 2018, doi: 10.1109/ACCESS.2018.2869577.
- [15] A. A. Ojugo and A. O. Eboka, "Empirical Bayesian network to improve service delivery and performance dependability on a campus network," *IAES International Journal of Artificial Intelligence*, vol. 10, no. 3, pp. 623–635, Sep. 2021, doi: 10.11591/ijai.v10.i3.pp623-635.
- [16] P. K. Nandi, T. Tabassum, and M. Ahmad, "Development of an IoT-based automatic remote health monitoring system," *Journal of Engineering Science*, vol. 14, no. 2, pp. 21–30, 2024, doi: 10.3329/jes.v14i2.71212.
- [17] J. K. Oladele *et al.*, "BEHeDaS: a blockchain electronic health data system for secure medical records exchange," *Journal of Computing Theories and Applications*, vol. 1, no. 3, pp. 231–242, 2024, doi: 10.62411/jcta.9509.
- [18] S. Okuyama, S. Tsuruoka, H. Kawanaka, and H. Takase, "Interactive learning support user interface for lecture scenes indexed with extracted keyword from blackboard," *Australian Journal of Basic and Applied Sciences*, vol. 8, no. 4, pp. 319–324, 2014.
- [19] A. Ometov *et al.*, "A survey on wearable technology: history, state-of-the-art and current challenges," *Computer Networks*, vol. 193, p. 108074, Jul. 2021, doi: 10.1016/j.comnet.2021.108074.
- [20] A. A. Ojugo, P. O. Ejeh, O. C. Christopher, A. O. Eboka, and F. U. Emordi, "Improved distribution and food safety for beef processing and management using a blockchain-tracer support framework," *International Journal of Informatics and Communication Technology*, vol. 12, no. 3, pp. 205–213, Dec. 2023, doi: 10.11591/ijict.v12i3.pp205-213.
- [21] A. N. Safriandono, D. R. I. M. Setiadi, A. Dahlan, F. Z. Rahmanti, I. S. Wibisono, and A. A. Ojugo, "Analyzing quantum feature engineering and balancing strategies effect on liver disease classification," *Journal of Future Artificial Intelligence and Technologies*, vol. 1, no. 1, pp. 51–63, Jun. 2024, doi: 10.62411/faith.2024-12.
- [22] D. R. I. M. Setiadi, A. Susanto, K. Nugroho, A. R. Muslikh, A. A. Ojugo, and H. S. Gan, "Rice yield forecasting using hybrid quantum deep learning model," *Computers*, vol. 13, no. 8, pp. 1–18, 2024, doi: 10.3390/computers13080191.
- [23] S. G. Kong, D. Jin, S. Li, and H. Kim, "Fast fire flame detection in surveillance video using logistic regression and temporal smoothing," *Fire Safety Journal*, vol. 79, pp. 37–43, Jan. 2016, doi: 10.1016/j.firesaf.2015.11.015.
- [24] A. Kim, J. Oh, J. Ryu, and K. Lee, "A review of insider threat detection approaches with IoT perspective," *IEEE Access*, vol. 8, pp. 78847–78867, 2020, doi: 10.1109/ACCESS.2020.2990195.
- [25] S. E. Brizimor *et al.*, "WiSeCart: sensor-based smart-cart with self-payment mode to improve shopping experience and inventory management," *Advances in Multidisciplinary & Scientific Research Journal Publications*, vol. 10, no. 1, pp. 53–74, Mar. 2024, doi: 10.22624/aims/sij/v10n1p7.
- [26] P. T. Kortum and A. Bangor, "Usability ratings for everyday products measured with the system usability scale," *International Journal of Human-Computer Interaction*, vol. 29, no. 2, pp. 67–76, 2013, doi: 10.1080/10447318.2012.681221.
- [27] A. A. Ojugo *et al.*, "Forging a user-trust memetic modular neural network card fraud detection ensemble: a pilot study," *Journal of Computing Theories and Applications*, vol. 1, no. 2, pp. 50–60, Oct. 2023, doi: 10.33633/jcta.v1i2.9259.
- [28] S. Yuan and X. Wu, "Deep learning for insider threat detection: review, challenges and opportunities," *Computers and Security*, vol. 104, 2021, doi: 10.1016/j.cose.2021.102221.
- [29] C. Joshi, J. R. Aliaga, and D. R. Insua, "Insider threat modeling: an adversarial risk analysis approach," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 1131–1142, 2021, doi: 10.1109/TIFS.2020.3029898.
- [30] R. Joshi and P. S. Vaghela, "Online buying habit: an empirical study of Surat City," *International Journal of Market Trends*, vol. 21, no. 2, pp. 1–15, 2018.
- [31] R. Nasir, M. Afzal, R. Latif, and W. Iqbal, "Behavioral based insider threat detection using deep learning," *IEEE Access*, vol. 9, pp. 143266–143274, 2021, doi: 10.1109/ACCESS.2021.3118297.
- [32] S. A. Hosseini, H. A. Abyaneh, S. H. H. Sadeghi, F. Razavi, and A. Nasiri, "An overview of microgrid protection methods and the factors involved," *Renewable and Sustainable Energy Reviews*, vol. 64, pp. 174–186, Oct. 2016, doi: 10.1016/j.rser.2016.05.089.




- [33] R. R. Atuduhor *et al.*, "StreamBoostE: a hybrid boosting-collaborative filter scheme for adaptive user-item recommender for streaming services," *Advances in Multidisciplinary & Scientific Research Journal Publications*, vol. 10, no. 2, pp. 89–106, Jun. 2024, doi: 10.22624/aims/v10n2p8.
- [34] P. A. Zawislak, F. M. Reichert, D. Barbieux, A. M. S. Avila, and N. Pufal, "The dynamic chain of innovation: bounded capabilities and complementarity in agribusiness," *Journal of Agribusiness in Developing and Emerging Economies*, vol. 13, no. 5, pp. 657–670, Apr. 2023, doi: 10.1108/JADEE-04-2021-0096.
- [35] A. A. Azzuhriyyah, Indrawati, and G. Ramantoko, "A systematic literature review on metaverse," pp. 118–125, Dec. 2023, doi: 10.2991/978-94-6463-340-5_11.
- [36] A. D. Bhavani and N. Mangla, "A novel network intrusion detection system based on semi-supervised approach for IoT," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 4, pp. 207–216, 2023, doi: 10.14569/IJACSA.2023.0140424.
- [37] A. M. Ifioko *et al.*, "CoDuBoTeSS: a pilot study to eradicate counterfeit drugs via a blockchain tracer support system on the nigerian frontier," *Advances in Multidisciplinary & Scientific Research Journal Publications*, vol. 10, no. 2, pp. 53–74, 2024, doi: 10.22624/aims/bij/v10n1p6.
- [38] F. S. Leira, H. H. Helgesen, T. A. Johansen, and T. I. Fossen, "Object detection, recognition, and tracking from UAVs using a thermal camera," *Journal of Field Robotics*, vol. 38, no. 2, pp. 242–267, 2021, doi: 10.1002/rob.21985.
- [39] P. Hakonen, "Detecting insider threats using user and entity behavior analytics," *International Journal of Electrical and Computer Engineering*, vol. 21, no. October, pp. 5765–5783, 2022.
- [40] E. A. Otorokpo *et al.*, "DaBO-BoostE: enhanced data balancing via oversampling technique for a boosting ensemble in card-fraud detection," *Advances in Multidisciplinary & Scientific Research Journal Publications*, vol. 12, no. 2, pp. 45–66, 2024, doi: 10.22624/aims/math/v12n2p4.
- [41] P. O. Ejeh *et al.*, "Counterfeit drugs detection in the nigeria pharma-chain via enhanced blockchain-based mobile authentication service," *Advances in Multidisciplinary & Scientific Research Journal Publications*, vol. 12, no. 2, pp. 25–44, 2024, doi: 10.22624/aims/math/v12n2p3.
- [42] H. Zardi and H. Alrajhi, "Anomaly discover: a new community-based approach for detecting anomalies in social networks," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 4, pp. 912–920, 2023, doi: 10.14569/IJACSA.2023.01404101.
- [43] S. Gokarn and A. Choudhary, "Modeling the key factors influencing the reduction of food loss and waste in fresh produce supply chains," *Journal of Environmental Management*, vol. 294, p. 113063, Sep. 2021, doi: 10.1016/j.jenvman.2021.113063.
- [44] B. O. Malasowe, M. I. Akazue, E. A. Okpako, F. O. Aghware, A. A. Ojugo, and D. V. Ojie, "Adaptive learner-CBT with secured fault-tolerant and resumption capability for Nigerian Universities," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 8, pp. 135–142, 2023, doi: 10.14569/IJACSA.2023.0140816.
- [45] A. E. Ibor, E. B. Edim, and A. A. Ojugo, "Secure health information system with blockchain technology," *Journal of the Nigerian Society of Physical Sciences*, vol. 5, no. 2, p. 992, Apr. 2023, doi: 10.46481/jnsps.2023.992.
- [46] A. A. Ojugo, P. O. Ejeh, C. C. Odiakaose, A. O. Eboka, and F. U. Emordi, "Predicting rainfall runoff in Southern Nigeria using a fused hybrid deep learning ensemble," *International Journal of Informatics and Communication Technology*, vol. 13, no. 1, pp. 108–115, Apr. 2024, doi: 10.11591/ijict.v13i1.pp108-115.
- [47] M. N. Al-Mhigani, R. Ahmed, Z. A. Z. Abidin, and S. N. Isnin, "An integrated imbalanced learning and deep neural network model for insider threat detection," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 1, pp. 573–577, 2021, doi: 10.14569/IJACSA.2021.0120166.
- [48] R. A. Alsowai and T. Al-Shehari, "A multi-tiered framework for insider threat prevention," *Electronics (Switzerland)*, vol. 10, no. 9, 2021, doi: 10.3390/electronics10091005.
- [49] T. Sutikno, M. H. Ar-Rasyid, T. Wahono, and W. Arsadiando, "Internet of things with NodeMCU ESP8266 for MPX-5700AP sensor-based LPG pressure monitoring," *International Journal of Advances in Applied Sciences*, vol. 12, no. 3, pp. 257–264, Sep. 2023, doi: 10.11591/ijaas.v12.i3.pp257-264.
- [50] J. R. Amalraj and R. Lourdasamy, "A novel distributed token-based access control algorithm using a secret sharing scheme for secure data access control," *International Journal of Computer Networks and Applications*, vol. 9, no. 4, pp. 374–384, Aug. 2022, doi: 10.22247/ijcna/2022/214501.
- [51] E. Ileberi, Y. Sun, and Z. Wang, "A machine learning based credit card fraud detection using the GA algorithm for feature selection," *Journal of Big Data*, vol. 9, no. 1, p. 24, Dec. 2022, doi: 10.1186/s40537-022-00573-8.
- [52] I. A. Anderson and W. Wood, "Habits and the electronic herd: The psychology behind social media's successes and failures," *Consumer Psychology Review*, vol. 4, no. 1, pp. 83–99, Jan. 2021, doi: 10.1002/arc.1063.
- [53] I. Benchaji, S. Douzi, B. El Ouahidi, and J. Jaafari, "Enhanced credit card fraud detection based on attention mechanism and LSTM deep model," *Journal of Big Data*, vol. 8, no. 1, p. 151, Dec. 2021, doi: 10.1186/s40537-021-00541-8.
- [54] Y. Gao, S. Zhang, J. Lu, Y. Gao, S. Zhang, and J. Lu, "Machine learning for credit card fraud detection," in *ACM International Conference Proceeding Series*, Jun. 2021, pp. 213–219, doi: 10.1145/3473714.3473749.
- [55] M. I. Akazue *et al.*, "FiMoDeAL: pilot study on shortest path heuristics in wireless sensor network for fire detection and alert ensemble," *Bulletin of Electrical Engineering and Informatics*, vol. 13, no. 5, pp. 3534–3543, Oct. 2024, doi: 10.11591/eei.v13i5.8084.
- [56] F. O. Aghware *et al.*, "BloFoPASS: a blockchain food palliatives tracer support system for resolving welfare distribution crisis in Nigeria," *International Journal of Informatics and Communication Technology*, vol. 13, no. 2, pp. 178–187, Aug. 2024, doi: 10.11591/ijict.v13i2.pp178-187.
- [57] D. Nahavandi, R. Alizadehsani, A. Khosravi, and U. R. Acharya, "Application of artificial intelligence in wearable devices: opportunities and challenges," *Computer Methods and Programs in Biomedicine*, vol. 213, no. December, 2022, doi: 10.1016/j.cmpb.2021.106541.
- [58] K. Kakhi, R. Alizadehsani, H. M. D. Kabir, A. Khosravi, S. Nahavandi, and U. R. Acharya, "The internet of medical things and artificial intelligence: trends, challenges, and opportunities," *Biocybernetics and Biomedical Engineering*, vol. 42, no. 3, pp. 749–771, 2022, doi: 10.1016/j.bbe.2022.05.008.
- [59] G. Sasikala *et al.*, "An innovative sensing machine learning technique to detect credit card frauds in wireless communications," *Wireless Communications and Mobile Computing*, vol. 2022, pp. 1–12, Jun. 2022, doi: 10.1155/2022/2439205.
- [60] D. Huang, Y. Lin, Z. Weng, and J. Xiong, "Decision analysis and prediction based on credit card fraud data," in *ACM International Conference Proceeding Series*, Apr. 2021, pp. 20–26, doi: 10.1145/3478301.3478305.
- [61] O. Thorat, N. Parekh, and R. Mangrulkar, "TaxoDaCML: taxonomy based divide and conquer using machine learning approach for DDoS attack classification," *International Journal of Information Management Data Insights*, vol. 1, no. 2, p. 100048, Nov. 2021, doi: 10.1016/j.jjime.2021.100048.

- [62] J. M. Pearson, A. Pearson, and D. Green, "Determining the importance of key criteria in web usability," *Management Research News*, vol. 30, no. 11, pp. 816–828, Oct. 2007, doi: 10.1108/01409170710832250.
- [63] K. Peterson, "Academic Web site design and academic templates: where does the library fit in?," *Information Technology and Libraries*, vol. 25, no. 4, pp. 217–221, Dec. 2006, doi: 10.6017/ital.v25i4.3354.
- [64] F. O. Aghware, R. E. Yoro, P. O. Ejeh, C. C. Odiakaose, F. U. Emordi, and A. A. Ojugo, "DeLClustE: protecting users from credit-card fraud transaction via the deep-learning cluster ensemble," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 6, pp. 94–100, 2023, doi: 10.14569/IJACSA.2023.0140610.
- [65] M. I. Akazue, A. A. Ojugo, R. E. Yoro, B. O. Malasowe, and O. Nwankwo, "Empirical evidence of phishing menace among undergraduate smartphone users in selected universities in Nigeria," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 28, no. 3, pp. 1756–1765, Dec. 2022, doi: 10.11591/ijeecs.v28.i3.pp1756-1765.
- [66] M. I. Akazue, R. E. Yoro, B. O. Malasowe, O. Nwankwo, and A. A. Ojugo, "Improved services traceability and management of a food value chain using block-chain network: a case of Nigeria," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 29, no. 3, pp. 1623–1633, 2023, doi: 10.11591/ijeecs.v29.i3.pp1623-1633.
- [67] S. N. Okofu *et al.*, "Pilot study on consumer preference, intentions and trust on purchasing-pattern for online virtual shops," *International Journal of Advanced Computer Science and Applications*, vol. 15, no. 7, pp. 804–811, 2024, doi: 10.14569/IJACSA.2024.0150780.
- [68] M. I. Akazue *et al.*, "Handling transactional data features via associative rule mining for mobile online shopping platforms," *International Journal of Advanced Computer Science and Applications*, vol. 15, no. 3, pp. 530–538, 2024, doi: 10.14569/IJACSA.2024.0150354.
- [69] C. O. Obruché, R. A. Abere, and R. E. Ako, "Deployment of a virtual key-card smart-lock system: the quest for improved security, eased user mobility and privacy," *FUPRE Journal of Scientific and Industrial Research*, vol. 8, no. 1, pp. 80–94, 2024.
- [70] W. L. Hsu, J. Y. Jhuang, C. S. Huang, C. K. Liang, and Y. C. Shiau, "Application of internet of things in a kitchen fire prevention system," *Applied Sciences (Switzerland)*, vol. 9, no. 17, p. 3520, Aug. 2019, doi: 10.3390/app9173520.
- [71] A. A. Ojugo and R. E. Yoro, "Forging a deep learning neural network intrusion detection framework to curb the distributed denial of service attack," *International Journal of Electrical and Computer Engineering*, vol. 11, no. 2, pp. 1498–1509, 2021, doi: 10.11591/ijece.v11i2.pp1498-1509.
- [72] A. A. Ojugo, A. O. Eboka, R. E. Yoro, M. O. Yerokun, and F. N. Efozia, "Hybrid model for early diabetes diagnosis," in *Proceedings - 2015 2nd International Conference on Mathematics and Computers in Sciences and in Industry, MCSI 2015*, Aug. 2016, pp. 55–65, doi: 10.1109/MCSI.2015.35.
- [73] V. G. Cerf, "On the internet of medical things," *Communications of the ACM*, vol. 63, no. 8, p. 5, Jul. 2020, doi: 10.1145/3406779.
- [74] P. Manickam *et al.*, "Artificial intelligence (AI) and internet of medical things (IoMT) assisted biomedical systems for intelligent healthcare," *Biosensors*, vol. 12, no. 8, 2022, doi: 10.3390/bios12080562.
- [75] T. Söderholm, "Examining the internet of medical things," *New Electronics*, vol. 57, no. 4, pp. 30–31, 2024.
- [76] A. Hurt, "Internet of medical things emerges," *Dermatology Times*, vol. 40, no. 10, pp. 52–58, 2019, [Online]. Available: <http://ezproxy.uct.ac.za/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=cin20&AN=138944526&site=ehost-live>.
- [77] A. Ravenscroft, S. Lindstaedt, C. Delgado Kloos, and D. Hernández-Leo, *21st century learning for 21st century skills*, vol. 7563, no. July 2015. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012.
- [78] I. E.I., A. M.I., O. Edith, and O. Deborah, "A framework for smart city model enabled by internet of things (IoT)," *International Journal of Computer Applications*, vol. 185, no. 6, pp. 6–11, 2023, doi: 10.5120/ijca2023922685.
- [79] A. Shahzad, K. Zhang, and A. Gherbi, "Intuitive development to examine collaborative iot supply chain system underlying privacy and security levels and perspective powering through proactive blockchain," *Sensors (Switzerland)*, vol. 20, no. 13, pp. 1–27, 2020, doi: 10.3390/s20133760.
- [80] I. Ehsan *et al.*, "Internet of things-based fire alarm navigation system: a fire-rescue department perspective," *Mobile Information Systems*, vol. 2022, pp. 1–15, Sep. 2022, doi: 10.1155/2022/3830372.
- [81] D. A. Sungheetha and D. R. Sharma R, "Real time monitoring and fire detection using internet of things and cloud based drones," *Journal of Soft Computing Paradigm*, vol. 2, no. 3, pp. 168–174, Jul. 2020, doi: 10.36548/jscp.2020.3.004.
- [82] A. Roehrs, C. A. Da Costa, R. D. R. Righi, S. J. Rigo, and M. H. Wichman, "Toward a model for personal health record interoperability," *IEEE Journal of Biomedical and Health Informatics*, vol. 23, no. 2, pp. 867–873, Mar. 2019, doi: 10.1109/JBHI.2018.2836138.
- [83] D. A. Obasuyi *et al.*, "NiCuSBlockIoT: sensor-based cargo assets management and traceability blockchain support for Nigerian custom services," *Advances in Multidisciplinary & Scientific Research Journal Publications*, vol. 15, no. 2, pp. 45–64, Jun. 2024, doi: 10.22624/aims/cisdi/v15n2p4.
- [84] A. A. Ojugo and R. E. Yoro, "Extending the three-tier constructivist learning model for alternative delivery: Ahead the COVID-19 pandemic in Nigeria," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 21, no. 3, pp. 1673–1682, Mar. 2021, doi: 10.11591/ijeecs.v21.i3.pp1673-1682.
- [85] V. O. Geteloma *et al.*, "AQuaMoAS: unmasking a wireless sensor-based ensemble for air quality monitor and alert system," *Applied Engineering and Technology*, vol. 3, no. 2, pp. 86–101, 2024, doi: 10.31763/aet.v3i2.1536.
- [86] A. A. Ojugo and D. A. Oyemade, "Boyer moore string-match framework for a hybrid short message service spam filtering technique," *IAES International Journal of Artificial Intelligence*, vol. 10, no. 3, pp. 519–527, 2021, doi: 10.11591/ijai.v10.i3.pp519-527.
- [87] R. F. R. Suleiman and F. Q. M. I. Reza, "Gas station fuel storage tank monitoring system using internet of things," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 8, no. 1.6 Special Issue, pp. 531–535, Dec. 2019, doi: 10.30534/ijatcse/2019/7881.62019.
- [88] K. Pradeepa and M. Praveen, "A survey on routing protocols with security in internet of things," *Solid State Technology*, vol. 63, no. 4, pp. 38–111, 2020.
- [89] S. Sendra, L. García, J. Lloret, I. Bosch, and R. Vega-Rodríguez, "LoRaWAN network for fire monitoring in rural environments," *Electronics (Switzerland)*, vol. 9, no. 3, p. 531, Mar. 2020, doi: 10.3390/electronics9030531.
- [90] P. Ratazzi, Y. Aafer, A. Ahlawat, H. Hao, Y. Wang, and W. Du, "A systematic security evaluation of android 's multi-user framework," *MoST*, no. December 2020, 2014.
- [91] E. Aworonye, R. A. Abere, R. E. Ako, B. Nwozor, and V. O. Geteloma, "IoT-motion electric eye ensemble for reduced power consumption in automated homes," *FUPRE Journal of Scientific and Industrial Research*, vol. 8, no. 2, pp. 128–142, 2024.
- [92] V. V. Krishna, Y. Rupa, G. Koushik, T. Varun, B. V. Kiranmayee, and K. Akhil, "A comparative study on authentication vulnerabilities and security issues in wearable devices," *Proceedings of the Fourth International Conference on Advances in Computer Engineering and Communication Systems (ICACECS 2023)*, Atlantis Highlights in Computer Sciences 18, vol. 18, no. Icacces, pp. 106–116, 2023, doi: 10.2991/978-94-6463-314-6_11.




- [93] B. P. L. Lau *et al.*, "A survey of data fusion in smart city applications," *Information Fusion*, vol. 52, no. January, pp. 357–374, 2019, doi: 10.1016/j.inffus.2019.05.004.
- [94] J. M. Kapadia and P. Vaghela, "An application of technology acceptance model in understanding students' behavioural intention for use of internet banking in Surat City," *International Conference on Governance in E-commerce: Contemporary Issues and Challenges*, no. 1, pp. 1–11, 2016, [Online]. Available: <https://www.researchgate.net/publication/307639141>.

BIOGRAPHIES OF AUTHORS






Andrew Okonji Eboka    received his HND in Computer Science in 1998 from the Akanu Ibiam Federal Polytechnic in Ebonyi State; His PGD from the Ebonyi State University in 2013, B.Sc./Ed in Computer Science Education from the Enugu State University of Science and Technology, Enugu in 2013. He received his M.Sc. in Network Computing from Coventry University, United Kingdom. He is a Chief Lecturer at the Department of Computer Education at the Federal College of Education Technical Asaba, Nigeria. His research interests include: cybersecurity, ubiquitous computing, and forensics. He is a member of: The British Computer Society, Association of Computer Machinery, Computer Professionals of Nigeria and International Association of Engineers (IAENG). He can be contacted at email: andrew.eboka@fctetasaba.edu.ng.






Fidelis Obukohwo Aghware    received B.Sc. in Computer Science from The University of Lagos in 1998; M.Sc. in 2005 from the Nnamdi Azikiwe University Awka, and also Ph.D. in Computer Science in 2015 from the Ebonyi State University, Abakiliki. He is currently a Associate Professor with the Department of Computer Science, University of Delta in Agbor, Delta State of Nigeria. His research interests include (but not limited to): cybersecurity, data science, and information security. He is a member of Nigerian Computer Society (NCS), the Council for Registration of Computer Professionals of Nigeria (CPN), and the International Association of Engineers (IAENG). He can be contacted at: fidelis.aghware@unidel.edu.ng.






Margaret Dumebi Okpor    received her B.Sc. and M.Sc. in Computer Science in 1997 and 2014 respectively from the University of Benin in Edo State of Nigeria; and her Ph.D. in 2023 also in Computer Science from the Ignatius Ajuru University of Education in Port-Harcourt, Rivers State in Nigeria. She currently lectures with the Department of Computer Science at the Faculty of Computing, Delta State University of Science and Technology Ozoro in Delta State of Nigeria. Her research interests are in machine learning, AI-driven identity management and access control, cybersecurity, and insider threat intelligence. She is also a member of the Nigerian Computer Society (NCS) and the Council for Registration of Computer Professionals of Nigeria. She can be contacted at email: okpormd@dsust.edu.ng.






Christopher Chukwufunaya Odiakaose    received his BSc from Enugu State University of Science and Technology, Enugu and is M.Sc. from the Federal University of Petroleum Resources Effurun in Delta State. He is currently a research assistant and undergoing his doctoral studies with the Department of Computer Science at the Federal University of Petroleum Resources Effurun in Delta State, Nigeria. He currently lectures at the Department of Data Science of the Dennis Osadebay University Asaba. He has several publications to his credit and his interest is in big-data, machine learning approaches, and user trust modeling. He can be contacted at email: osegalaxy@gmail.com.






Ejaita Abugor Okpako    received BSc, MSc and PhD (all in Computer Science) from the University of Port-Harcourt in Rivers State, Nigeria. He is presently the Acting Dean of the Faculty of Computing at the University of Delta, Agbor in Nigeria. His areas of interest include artificial intelligence, data science, cybersecurity, big data and software engineering. He served previously as the Director of ICT at the Edwin Clark University Kiangbodo in Delta State, Nigeria. He has published over 49 articles comprising of journals and proceedings. He is presently the PRO of the Nigeria Computer Society, Delta State Chapter. He can be contacted at email: ejaita.okpako@unidel.edu.ng.






Prof. Arnold Adimabua Ojugo    received his B.Sc., M.Sc. and Ph.D. in Computer Science from Imo State University Owerri, NnamdiAzikiwe University Awka, and Ebonyi State University Abakiliki in 2000, 2005 and 2013 respectively. He is a professor with the Department of Computer Science at The Federal University of Petroleum Resources Effurun with research interest(s) in: intelligent systems computing, data science, cybersecurity, and graphs. He has many scholarly publications, and a member of various editorial/reviewers boards (to include): Frontiers in Big Data, The International Journal of Modern Education in Computer Science IJMECS, and Progress for Intelligent Computation and Application. He is a member of the Nigerian Computer Society, Council of Computer Professionals of Nigeria, and International Association of Engineers. He can be contacted at email: ojugo.arnold@fupre.edu.ng.






Rita Erhovwo Ako    received her B.Sc. Industrial Mathematics in 2000 from the Delta State University Abraka in Delta State, Nigeria; M.Sc. Computer Science in 2005 from the University of Ibadan in Oyo State; M.Sc. Internet-Computer and System Security in 2006, and Ph.D. Computer Science in 2013 respectively from the University of Bradford, Bradford, United Kingdom. She is currently a senior lecturer with the Department of Computer Science at The Federal University of Petroleum Resources Effurun. She has several publications to her credit with research interests in: artificial intelligence, cybersecurity, e-commerce, embedded systems, and risk management. She is a member of the Nigerian Computer Society. She can be contacted at email: ako.rita@fupre.edu.ng.






Amaka Patience Binitie    obtained her B.Sc. degree in Computer Science from Nnamdi Azikiwe University Awka, Nigeria, in 2007. She obtained her M.Sc. degree in Computer science from Adamawa State University, Nigeria in 2015 and her Ph.D. in Computer from the University of Benin, Nigeria in 2023. She is currently a lecturer at the Federal College of Education Technical Asaba. She has lots of publications to her name. Her research interests are in the areas of cyber security, information technology, and artificial intelligence. She can be contacted at email: amaka.binitie@fctetasaba.edu.ng.






Innocent Sunny Onyemenem    received his B.Sc. Computer Science from the University of Nigeria Nsukka in 20026; MSc in Info Technology from the University of Aberdeen in 2022. He currently lectures with the Department of Computer Science at The Federal College of Education (Technical) Asaba in Nigeria. He has several publications to his credit with research interests in: information technology, cybersecurity, e-commerce, and risk management. He is a member of the Nigerian Computer Society and the Council for the Registration of Computer Professionals in Nigeria. He can be contacted at email: innocentsunnyonyemenem@gmail.com.



Patrick Ogholuwaremi Ejeh    received his HND in Computer Science from the Federal Polytechnic Auchi, Edo State in 2006; M.Sc. in Computer Science from Northumbria University, Newcastle, United Kingdom in 2010; and, his Ph.D. in Computer Science from Sunderland University, Sunderland, United Kingdom in 2017. He is currently a lecturer with the Department of Computer Science at the Dennis Osadebey University, Asaba, Delta State. His research interests includes; artificial intelligence, knowledge management, data science, and IoT. He is also a member Nigerian Computer Society and Higher Education Academic; United Kingdom. He can be contacted at email: patrick.ejeh@dou.edu.ng.



Victor Ochuko Geteloma    received his B.Sc. in Computer Science from the Federal University of Petroleum Resources Effurun, Delta State, Nigeria in 2015; M.Sc. in Computer Science in 2019 from the Covenant University, Ogun State. He currently lectures with the Department of Computer Science at the Federal University of Petroleum Resources Effurun. He has several publications to his credit. His research interests and specialization includes cyber security, cloud computing, e-government, technology adoption, and digital inclusion. He is a member of the Nigerian Computer Society. He can be contacted at email: geteloma.victor@fupre.edu.ng.