Research Article / Review Article FUPRE JOURNAL 8(1): 39-54(2024)

FUPRE Journal
of
Scientific and Industrial Research

ISSN: 2579-1184(Print) ISSN: 2578-1129 (Online)

http://fupre.edu.ng/journal

Deployment of a Virtual Key-Card Smart-Lock System: The Quest for Improved Client Security, Eased User Mobility and Privacy

OBRUCHE, C. O.[1,*], *ABERE, R. A.* [2], *AKO, R. E.*[3]

[1,2,3]*Department of Computer Science, College of Science, Federal University of Petroleum Resources Effurun, Delta State*

ARTICLE INFO

Received: 07/08/2023

Accepted: 19/10/2023

Keywords

Virtual key-card,
NodeMCU
Arduino
Raspberry Pi
Embedded systems

ABSTRACT

With an upsurge of data by global brands to interact/reach prospective clients, the birth of the Internet has today bridged the information gap. Virtualization techniques are today utilized as means to bridge the various lapses in our human processing endeavors. The adoption of tech to perform a variety of functions has since become imperative to ease our daily living as well as seamlessly allow transformations of various kinds to be impacted on our society. Study proposes a virtual key card access with cost-effective and cheap solution for managing access to areas within a facility. We have successfully integrated IoTs, virtual key card access, web-access control, solenoid lock integration, and ESP32-controller to create a comprehensive access control system. Its 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.

1. INTRODUCTION

The security of lives and property has since become a predominant challenge facing many individuals, businesses, organizations and nations in general (Guntur et al., 2018; Ojugo & Ekurume, 2021a). Security systems and protocols have since become necessary measure and technology to provide high-end user trust and assurances in the protection of lives and property. Today, the advancement in the adoption and use of technology in every facet of life's endeavour – has consequently, also made it imperative to employ tech in the advancement of security (Filippi et al., 2019; Kowalski et al., 2008; Ojugo, Eboka, et al., 2015; Yoro, Aghware, Akazue, et al., 2023).

Locks today are neatly and nicely placed on doors to help users access domain and spaces. Doors are designed to keep people out of public or private spaces. They are often used in homes, offices, hotels etc. they grant users access to restricted spaces and thus, it becomes imperative for managers of such facilities to ensure measures are in place to prevent unauthorized access by unauthorized users (Mazitelli, 2015; Sun et al., 2021).

The ability of administrators of such facilities through the exploration of experts to prevent unauthorized access to people from entering a space – has since become a crucial factor and component in the design of systems that houses users from time to time (Lin, 2018; Yoro, Aghware, Malasowe, et al., 2023).

Advances made generally to provision better living from inception, is poised

Corresponding author: *obruche65@gmail.com*
DIO

towards the use of imaginary locks to protect client privacy and personal property (Agrafiotis et al., 2015; Al-Qatf et al., 2018). 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. Oftentimes, many doors are left unlocked due to forgetfulness amongst many other reasons. While, these are common occurrence (Ojugo, Ugboh, et al., 2013; Ojugo & Otakore, 2020) – smart-locks are currently exploring and exploiting embedded systems technology with internet-capabilities through the use of key-codes, smart-phones, key-cards etc – as means to ensure safety and ease user-trust of lock systems, and this agrees with (Okuyama et al., 2014; Ometov et al., 2021).

Also, a majority of the employed devices for such lock-system – are rippled with flaws that adversaries and intruders, also exploit to gain unauthorized access to barred locations. In our effort to close these security gaps, our study employs the use of cryptographic virtual key-card system to provide improved security for the virtual key-card lock system.

1.1 Virtual(ization) Key-Cards

Virtual technology as currently today being 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/adjustment 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 (Ibor et al., 2023; Ojugo & Ekurume, 2021b).

Due to the fact that technology is becoming more advanced, the fact that such 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 (Al-Mhiqani et al., 2021; Alsowai & Al-Shehari, 2021).

Businesses today, that integrate the use of physical servers with onsite/off-site locations will often profit from the low-cost implementation, reduced maintenance cost, improved administration as well as the over-simplification that accompanies a virtualized server databanks and environment (Amalraj & Lourdusamy, 2022; Ileberi et al., 2022). Through such shared resources, virtualization enables the expansion of hardware (Anderson & Wood, 2021; Benchaji et al., 2021; Gao et al., 2021). 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. 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 (Kakhi et al., 2022; Nahavandi et al., 2022; Sasikala et al., 2022). We note that each evolution help also to evolve intelligent security systems, which are deployed to forestall illicit invasions of user privacy. The primary aim of this study is the provision of security protocols for the door lock key system with a single-key for one-lock phenomenon (Huang et al., 2021; Ojugo & Yoro, 2020c; Thorat et al., 2021).

Kim et al. (2020) designed an 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 PIC 16f877A (Kim et al., 2020). 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 functions. The embedded system was developed using Visual Basic 2010 Edition 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, fingerprint scanner, etc. 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 (Eboka & Ojugo, 2020; Kortum & Bangor, 2013; Ojugo, Akazue, Ejeh, Ashioba, et al., 2023).

Yuan et al., (2021) 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 (Yuan & Wu, 2021).

Joshi et al., (2018) as extended by Joshi et al. (2021) presented a part of a smart home technology using the Bluetooth of a mobile device. A system named door locks automation system using Bluetooth-based Android Smartphones was proposed and prototyped. 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 for/as its controller centre and data processing centre, and solenoid as door lock output (C. Joshi et al., 2021; R. Joshi & Vaghela, 2018).

Nasir et al., (2021) also presented and analyzed the design and implementation of a microcontroller-based home security system using the GSM technology. It employed two micro-controllers that were used to extend the functionalities in other peripherals such as the LED, LCD, Buzzer, and a GSM Module are responsible for the reliable operation of the proposed security system (Hosseini et al., 2016; Nasir et al., 2021).

Sun et al., (2021) in furtherance of the works by Nasir et al. (2021) 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 like lights, fans, television, etc; While, its second system incorporates some additional features like capturing and storage of an intruder's images unknown to the intruder (Sun et al., 2021).

Zawislak et al., (2022) investigated the automatic password-based door lock system by utilizing 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 (Aghware et al., 2023b; Ojugo, Akazue, Ejeh, Odiakaose, et al., 2023; Singh & Sharma, 2022; Zawislak et al., 2022).

Bhavani et al. (2023) extended the works of Kim et al. (2020) by designing an 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 PIC 16f877A (Bhavani & Mangla, 2023). They also extended the graphic user interface to yield greater and improved functionalities of the overall system such as display of live ID tag transactions, registering ID, deleting ID, recording attendance, and other functions. 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 (Bhavani & Mangla, 2023; Hakonen, 2022; Leira et al., 2021).

Zardi et al., (2023) designed a password-protected home automation system with an automatic door lock using the Arduino Uno board which is controlled by the ATmega-328. First, the user combination will be

compared with the pre-decided passwords stored in the system memory. If the user's combination matches the password, the door, light, and fan will be unlocked. The system was also built in a way that it could be locked by just pressing one key. In this system, the Arduino UNO microcontroller board is used for interfacing the various hardware 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 through a motor driver for operating the door (Gokarn & Choudhary, 2021; Malasowe et al., 2023; Zardi & Alrajhi, 2023).

The study is motivated as thus and seeks to (Aghware et al., 2023a; Akazue et al., 2022, 2023; Oyemade et al., 2016; Oyemade & Ojugo, 2020, 2021; Pearson et al., 2007; Peterson, 2006):

1. *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 endeavor, 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.
2. *Privacy Integration with IoTs:* A key challenge in the deployment of Internet of things (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.
3. Low Cost, Efficient Energy: Deploying for use, virtual keycard door lock system 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 .
4. 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.

Thus, the study seeks to achieve security, user data privacy, improved user-trust, energy efficiency and low-power computation via the development and deployment of a smart, virtual key-card door lock system using the IoT-enabled device(s).

2. MATERIALS AND METHODS

2.1 Technical Procedure

The study aims to design a smart virtual key-card for implementation via the mobile smartphones. The objectives thus, are to design and test the programming inside Arduino for receiving and sending the coordinated location and to design and test the assembly of all the hardware (electrical components) and software for the virtual key-card system. Emphasize on the embedded system here, involves both the hardware and software component parts (Chevalier et al., 2003; Ojugo, Aghware, et al., 2015; Ojugo & Eboka, 2014; Ojugo & Otakore, 2018; Okobah & Ojugo, 2018; Tarafdar & Zhang, 2005). The scope of this

study is as follows:

1. Microcontroller Arduino is used and loaded using Embedded 'C' language.
2. Using the smartphone to send SMS to GSM to receive the virtual keycard
3. Displaying the SMS received from the dedicated server.
4. Proteus software is used to simulate the operation of the microcontroller design before constructing a physical prototype.

2.2. Analysis of Existing System

The output design of the existing Smart NFC Door Access System primarily revolves around providing a seamless and efficient guest experience. When a guest successfully taps their NFC-enabled device (smartphone or smartcard) on the NFC reader located near the hotel room's door, the system triggers the NFC door lock to unlock the door as seen in figure 1a and figure 1b respectively.

Upon successful access, the door lock emits an audible signal to indicate the door's opening, providing immediate feedback to the guest. The output design ensures that the entire access process is swift and quite straightforward, allowing guests to access their rooms effortlessly and this agrees with (Ojugo et al., 2021a, 2021b; Ojugo & Eboka, 2019; Ojugo & Yoro, 2020a).

Also, the existing system was found to generates access logs in the backend server, recording details such as the timestamp of access, the unique identifier of the NFC device used, and the room number accessed. These logs are accessible through 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 behaviour and occupancy patterns.

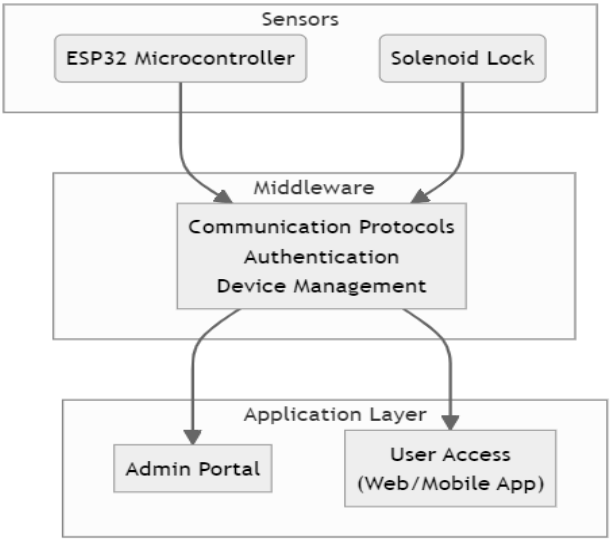

Figure 1a. Existing virtual IoT key-card schematics

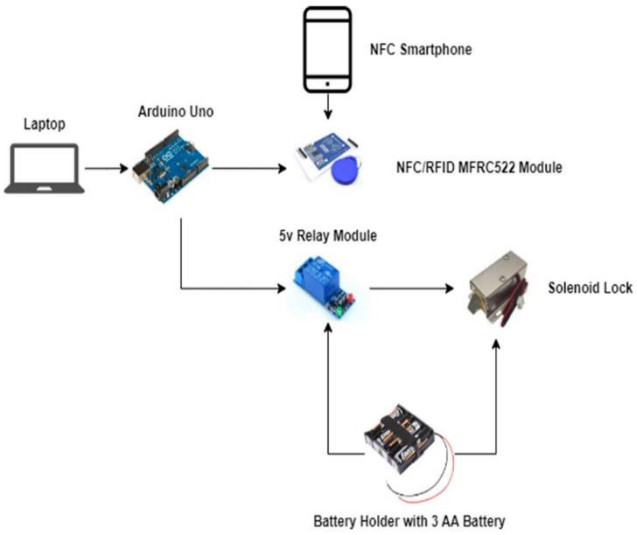

Figure 1b. Virtual key-card

2.3. Proposed Virtual Key-Card Model

The proposed system for the virtual key card system aims 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. Furthermore, it provisions a fail-safe protocol cum mechanism 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.

The proposed system's intuitive mobile app and administrative interface streamline the check-in process, empowering guests to manage their access effortlessly and enabling hotel staff to efficiently handle access permissions and monitor real-time access logs. Overall, the proposed virtual key card System promises an enhanced guest experience, heightened security, and improved operational efficiency for modern, tech-savvy hotels.

Some of the major benefits that the proposed system offers will include: (a) an enhanced device compatibility, supports a wide range of NFC-enabled devices for seamless access, (b) an 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 during 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 allows easy management of access permissions for hotel staff, (f) an improved guest experience with convenient room access using preferred NFC devices, and (g) the heightened security will instil in guests improved user-trust, confidence level and safeguards personal information.

Figure 2a shows the schematic diagram of the proposed virtual key-card system. The figure 2b represents the system flowchart and the flow of data from one component to another; while, the figure 2c represents the block circuitry diagram of the proposed system with its structural workings.

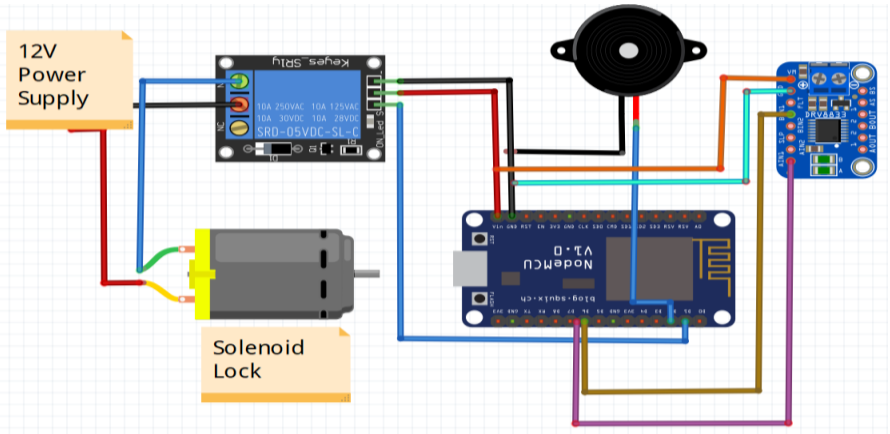

Figure 2a. Schematic diagram of the proposed virtual smart key-card door lock

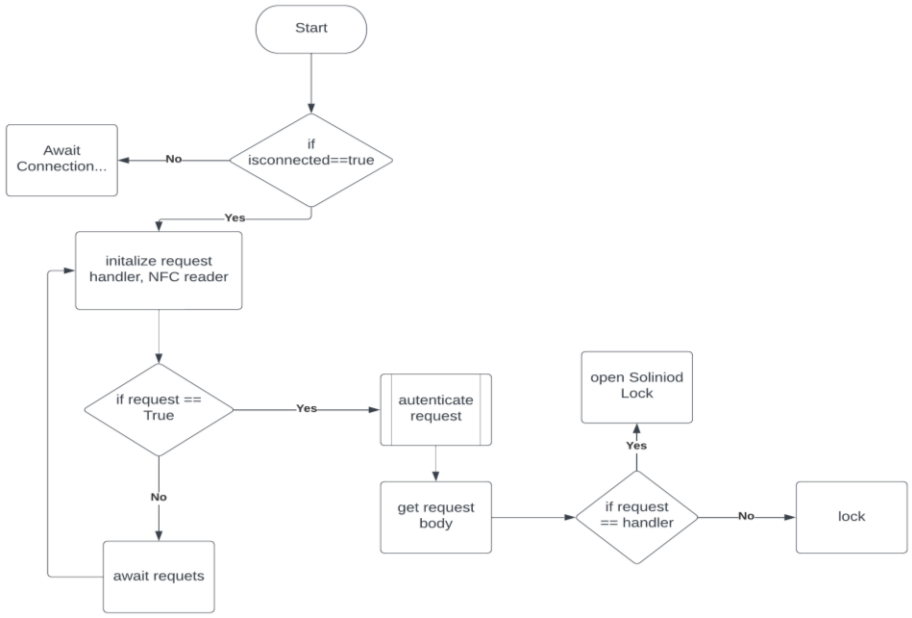

Figure 2b. System flowchart of the proposed virtual smart key-card door lock

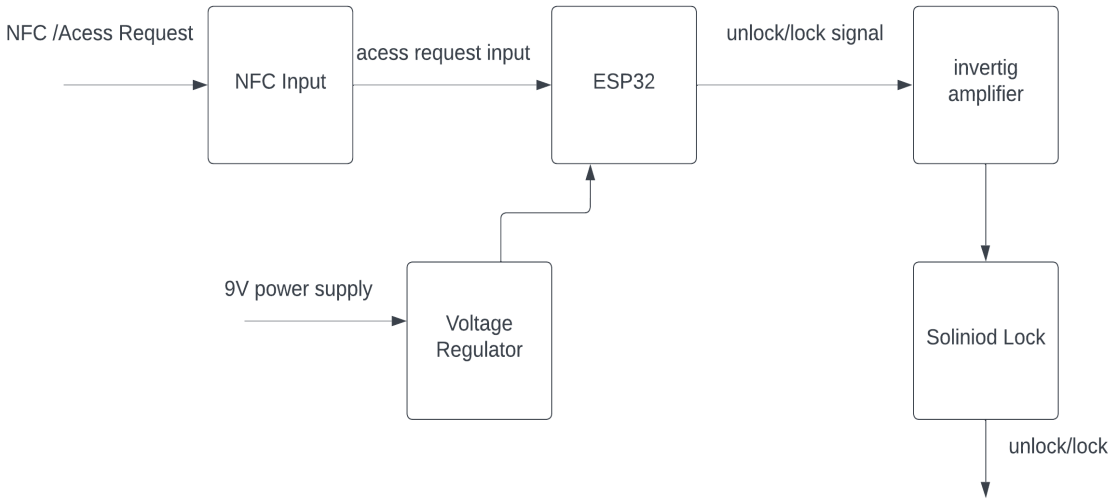

Figure 2c. Block circuitry flow diagram of proposed virtual key-card door lock

2.4. The Experimental Virtual Key-Card

The proposed virtual key card access system specifications sought to account for – amongst other important factors, the issues of security, privacy, robustness and flexibility. For this, 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. The system also incorporated a GSM module in the case of its usage in areas without the Internet access. Also, incorporated was the solenoid lock, which will be activated by the microcontroller in response to the appropriate input signals.

The system also 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 virtual key card access system should be designed to work with a cloud-based server, allowing for remote management and monitoring of the system.

For hardware, the system should include a card reader that can read RFID or NFC tags on the virtual key cards. The system also includes a display on the web application 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. RESULT FINDINGS AND DISCUSSION

3.1. Performance Evaluation

Table 1 shows the performance test result and indices from the system as generated.

Table 1. System Test Results

No	Test Description	Actual Results	Remark
1	Successful access using authorized NFC tags	The door unlocks upon presenting an authorized NFC tag	Pass
2	Failed access via unauthorized device access	Door remained lock upon presenting an unauthorized device	Pas
3	Failed access using invalid NFC tag	Door remains locked upon presenting invalid NFC tags	Pass
4	Error Handling for invalid NFC tag	System displays appropriate error message on the web application and serial monitor upon presenting an invalid NFC tag	Pass
5	Compatibility with the different types of NGFC tags	System is able to read and grant access to different types of NFC tags	Pass

Table 1 shows the 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. We also evaluated based on several key metrics to include access control speed, reliability, and user convenience respectively – as in agreement with (Ojugo, Allenotor, et al., 2015; Ojugo & Eboka, 2019; Yoro & Ojugo, 2019).

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 (Cerf, 2020; Charan et al., 2020; Manickam et al., 2022; Ojugo, Abere, et al., 2013; Ojugo, Yoro, et al., 2013).

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 application was also found to be user-friendly and intuitive, with a simple and straightforward interface. This is in agreement with (Ferrari et al., 2012; Hurt, 2019; Kakhi et al., 2022; Og & Ying, 2021; Ojugo, Odiakaose, Emordi, Ejeh, et al., 2023).

3.2. Result Findings

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

Table 2. System Test Results

Metrics	Description	Results
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 1.8seconds for access to be granted if the tag is used, and 1.1seconds 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 virtual key cards and control the locks based on the access rights defined in the web application	The system was found to have a 99.5% accuracy in reading the virtual key-card and in controlling the locks to either of the lock/unlock states based on access rights defined in the web application
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 stability and 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 etc	The system was found compatible with devices and technologies that incorporated the WIFI, Bluetooth and NFCs
Error Handling	The ability for a system to support a large number of users and access points, handle concurrent requests, invalid NFC tags and WiFi connectivity issues	The system was found to support large number of client and user access points with no performance degradation and security issues reported
Scalability	System's ability to support large number of users and access points, handle concurrent requests, invalid NFC tags and WiFi connectivity issues without compromising performance or security	The system was found to support large number of client and user access points with no performance degradation and security issues reported

Table 3 shows the system has an accuracy of 99.5percent accuracy in reading the virtual key-card and in controlling the locks to either of the lock/unlock states based on access rights defined in the web application. The system was found to have great fault-tolerance and was compatible with a major of the NFC tags and accompanying devices. This agrees with (Ojugo & Yoro, 2020b)

The study successfully implemented an ESP32 microcontroller, a solenoid lock, a web API, and a web app to manage the access of authorized personnel. We suggest persons of interest can convert from traditional key-access to a virtual key card access system has provided several benefits such as increased security, efficiency, and convenience. Some of the associated problems with traditional key can include

the risk of lost or stolen keys, the inconvenience of having to carry physical keys, and the lack of real-time access control and monitoring. Thus, the virtual key access system allows authorized personnel to access designated areas without the need for physical keys, reducing the risk of lost or stolen keys. The system provides real-time access control and monitoring, allowing administrators to track and manage access to the facility remotely.

The 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 virtual key card access system has demonstrated a practical, cost-effective and cheap solution for managing access to areas within a facility. We have successfully also integrated IoTs, virtual key card access, web-access control, solenoid lock integration, and ESP32-controller 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.

Conflict of Interest

The authors declare that there is no conflict of interest.

References

Aghware, F. O., Yoro, R. E., Ejeh, P. O., Odiakaose, C. C., Emordi, F. U., & Ojugo, A. A. (2023a). DeLClustE: Protecting Users from Credit-Card Fraud Transaction via the Deep-Learning Cluster Ensemble. *International Journal of Advanced Computer Science and Applications*, *14*(6), 94–100. https://doi.org/10.14569/IJACSA.2023.0140610

Aghware, F. O., Yoro, R. E., Ejeh, P. O., Odiakaose, C. C., Emordi, F. U., & Ojugo, A. A. (2023b). Sentiment analysis in detecting sophistication and degradation cues in malicious web contents. *Kongzhi Yu Juece/Control and Decision*, *38*(01), 653.

Agrafiotis, I., Nurse, J. R., Buckley, O., Legg, P., Creese, S., & Goldsmith, M. (2015). Identifying attack patterns for insider threat detection. *Computer Fraud and Security*, *2015*(7), 9–17. https://doi.org/10.1016/S1361-3723(15)30066-X

Akazue, M. I., Ojugo, A. A., Yoro, R. E., Malasowe, B. O., & Nwankwo, O. (2022). Empirical evidence of phishing menace among undergraduate smartphone users in selected universities in Nigeria. *Indonesian Journal of Electrical Engineering and Computer Science*, *28*(3), 1756–1765. https://doi.org/10.11591/ijeecs.v28.i3.pp1756-1765

Akazue, M. I., Yoro, R. E., Malasowe, B. O., Nwankwo, O., & Ojugo, A. A. (2023). 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*, *29*(3), 1623–1633. https://doi.org/10.11591/ijeecs.v29.i3.pp1623-1633

Al-Mhiqani, M. N., Isnin, S. N., Ahmed, R., & Abidi, Z. Z. (2021). An Integrated Imbalanced Learning and Deep Neural Network Model for Insider Threat Detection. *International Journal of Advanced Computer Science and Applications*, *12*(1), 1–5.

Al-Qatf, M., Lasheng, Y., Al-Habib, M., & Al-Sabahi, K. (2018). Deep Learning

Approach Combining Sparse Autoencoder With SVM for Network Intrusion Detection. *IEEE Access*, *6*, 52843–52856. https://doi.org/10.1109/ACCESS.2018.2869577

Alsowai, R. A., & Al-Shehari, T. (2021). A multi-tiered framework for insider threat prevention. *Electronics (Switzerland)*, *10*(9). https://doi.org/10.3390/electronics10091005

Amalraj, J. R., & Lourdusamy, R. (2022). A Novel distributed token-based algorithm using secret sharing scheme for secure data access control. *International Journal of Computer Networks and Applications*, *9*(4), 374. https://doi.org/10.22247/ijcna/2022/214501

Anderson, I. A., & Wood, W. (2021). Habits and the electronic herd: The psychology behind social media's successes and failures. *Consumer Psychology Review*, *4*(1), 83–99. https://doi.org/10.1002/arcp.1063

Benchaji, I., Douzi, S., El Ouahidi, B., & Jaafari, J. (2021). Enhanced credit card fraud detection based on attention mechanism and LSTM deep model. *Journal of Big Data*, *8*(1), 151. https://doi.org/10.1186/s40537-021-00541-8

Bhavani, A. D., & Mangla, N. (2023). A Novel Network Intrusion Detection System Based on Semi-Supervised Approach for IoT. *International Journal of Advanced Computer Science and Applications*, *14*(4), 207–216. https://doi.org/10.14569/IJACSA.2023.0140424

Cerf, V. G. (2020). On the internet of medical things. *Communications of the ACM*, *63*(8), 5. https://doi.org/10.1145/3406779

Charan, D. S., Nadipineni, H., Sahayam, S., & Jayaraman, U. (2020). *Method to Classify Skin Lesions using Dermoscopic images*. http://arxiv.org/abs/2008.09418

Chevalier, K., Bothorel, C., & Corruble, V. (2003). Discovering Rich Navigation Patterns on a Web Site. In *Webometrics* (Vol. 5, Issue 6, pp. 62–75). https://doi.org/10.1007/978-3-540-39644-4_7

Eboka, A. O., & Ojugo, A. A. (2020). Mitigating technical challenges via redesigning campus network for greater efficiency, scalability and robustness: A logical view. *International Journal of Modern Education and Computer Science*, *12*(6), 29–45. https://doi.org/10.5815/ijmecs.2020.06.03

Ferrari, A., Schoolnet, E., Punie, Y., Commission, E., Redecker, C., & Commission, E. (2012). *21st Century Learning for 21st Century Skills* (A. Ravenscroft, S. Lindstaedt, C. D. Kloos, & D. Hernández-Leo (eds.); Vol. 7563, Issue July 2015). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-33263-0

Filippi, P., Jones, E. J., Wimalathunge, N. S., Somarathna, P. D. S. N., Pozza, L. E., Ugbaje, S. U., Jephcott, T. G., Paterson, S. E., Whelan, B. M., & Bishop, T. F. A. (2019). An approach to forecast grain crop yield using multi-layered, multi-farm data sets and machine learning. *Precision Agriculture*, *20*(5), 1015–1029. https://doi.org/10.1007/s11119-018-09628-4

Gao, Y., Zhang, S., Lu, J., Gao, Y., Zhang, S., & Lu, J. (2021). Machine Learning for Credit Card Fraud Detection. *Proceedings of the 2021 International Conference on Control and Intelligent Robotics*, 213–219. https://doi.org/10.1145/3473714.3473749

Gokarn, S., & Choudhary, A. (2021). Modeling the key factors influencing the reduction of food loss and waste in fresh produce supply chains. *Journal of*

Environmental Management, *294*, 113063. https://doi.org/10.1016/j.jenvman.2021.113063

Guntur, S. R., Gorrepati, R. R., & Dirisala, V. R. (2018). Internet of Medical Things. In *Medical Big Data and Internet of Medical Things* (Issue October 2018, pp. 271–297). CRC Press. https://doi.org/10.1201/9781351030380-11

Hakonen, P. (2022). Detecting Insider Threats Using User and Entity Behavior Analytics. *International Journal of Electrical and Computer Engineering*, *21*(October), 5765–5783. https://www.theseus.fi/handle/10024/786079

Hosseini, S. A., Abyaneh, H. A., Sadeghi, S. H. H., Razavi, F., & Nasiri, A. (2016). An overview of microgrid protection methods and the factors involved. *Renewable and Sustainable Energy Reviews*, *64*, 174–186. https://doi.org/10.1016/j.rser.2016.05.089

Huang, D., Lin, Y., Weng, Z., & Xiong, J. (2021). Decision Analysis and Prediction Based on Credit Card Fraud Data. *The 2nd European Symposium on Computer and Communications*, 20–26. https://doi.org/10.1145/3478301.3478305

Hurt, A. (2019). "Internet of Medical Things" emerges. *Dermatology Times*, *40*(10), 52–58. http://ezproxy.uct.ac.za/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=cin20&AN=138944526&site=ehost-live

Ibor, A. E., Edim, E. B., & Ojugo, A. A. (2023). Secure Health Information System with Blockchain Technology. *Journal of the Nigerian Society of Physical Sciences*, *5*(992), 1–8. https://doi.org/10.46481/jnsps.2022.992

Ileberi, E., Sun, Y., & Wang, Z. (2022). A machine learning based credit card fraud detection using GA algorithm for feature selection. *Journal of Big Data*, *9*(1), 24. https://doi.org/10.1186/s40537-022-00573-8

Joshi, C., Aliaga, J. R., & Insua, D. R. (2021). Insider Threat Modeling: An Adversarial Risk Analysis Approach. *IEEE Transactions on Information Forensics and Security*, *16*, 1131–1142. https://doi.org/10.1109/TIFS.2020.3029898

Joshi, R., & Vaghela, P. S. (2018). Online buying habit: an empirical study of Surat City. *International Journal of Market Trends*, *21*(2), 1–15.

Kakhi, K., Alizadehsani, R., Kabir, H. M. D., Khosravi, A., Nahavandi, S., & Acharya, U. R. (2022). The internet of medical things and artificial intelligence: trends, challenges, and opportunities. *Biocybernetics and Biomedical Engineering*, *42*(3), 749–771. https://doi.org/10.1016/j.bbe.2022.05.008

Kim, A., Oh, J., Ryu, J., & Lee, K. (2020). A review of insider threat detection approaches with IoT perspective. *IEEE Access*, *8*, 78847–78867. https://doi.org/10.1109/ACCESS.2020.2990195

Kortum, P. T., & Bangor, A. (2013). Usability Ratings for Everyday Products Measured With the System Usability Scale. *International Journal of Human-Computer Interaction*, *29*(2), 67–76. https://doi.org/10.1080/10447318.2012.681221

Kowalski, E., Keverline, S., Ph, D., Williams, M., & Moore, A. (2008). Insider Threat Study: Illicit Cyber Activity in the Government Sector. *Carnegie Melon Software Engineering Institute*, *12*(1).

Leira, F. S., Helgesen, H. H., Johansen, T. A., & Fossen, T. I. (2021). Object

detection, recognition, and tracking from UAVs using a thermal camera. *Journal of Field Robotics*, *38*(2), 242–267. https://doi.org/10.1002/rob.21985

Lin, D. (2018). Insider threat detection: Where and how data science applies. *Cyber Security: A Peer-Reviewed Journal*, *2*, 1–8. https://www.ingentaconnect.com/content/hsp/jcs/2018/00000002/00000003/art00003

Malasowe, B. O., Akazue, M. I., Okpako, E. A., Aghware, F. O., Ojie, D. V., & Ojugo, A. A. (2023). Adaptive Learner-CBT with Secured Fault-Tolerant and Resumption Capability for Nigerian Universities. *International Journal of Advanced Computer Science and Applications*, *14*(8), 135–142. https://doi.org/10.14569/IJACSA.2023.0140816

Manickam, P., Mariappan, S. A., Murugesan, S. M., Hansda, S., Kaushik, A., Shinde, R., & Thipperudraswamy, S. P. (2022). Artificial Intelligence (AI) and Internet of Medical Things (IoMT) Assisted Biomedical Systems for Intelligent Healthcare. *Biosensors*, *12*(8). https://doi.org/10.3390/bios12080562

Mazitelli, N. (2015). Insider threats. *Engineering & Technology Reference*. https://doi.org/10.1049/etr.2015.0045

Nahavandi, D., Alizadehsani, R., Khosravi, A., & Acharya, U. R. (2022). Application of artificial intelligence in wearable devices: Opportunities and challenges. *Computer Methods and Programs in Biomedicine*, *213*(December), 106541. https://doi.org/10.1016/j.cmpb.2021.106541

Nasir, R., Afzal, M., Latif, R., & Iqbal, W. (2021). Behavioral Based Insider Threat Detection Using Deep Learning. *IEEE Access*, *9*, 143266–143274. https://doi.org/10.1109/ACCESS.2021.3118297

Og, S., & Ying, L. (2021). The Internet of Medical Things. *ICMLCA 2021 - 2nd International Conference on Machine Learning and Computer Application*, 273–276.

Ojugo, A. A., Abere, R. A., Orhionkpaiyo, B. C., Yoro, R. E., & Eboka, A. O. (2013). Technical Issues for IP-Based Telephony in Nigeria. *International Journal of Wireless Communications and Mobile Computing*, *1*(2), 58. https://doi.org/10.11648/j.wcmc.20130102.11

Ojugo, A. A., Aghware, F. O., Yoro, R. E., Yerokun, M. O., Eboka, A. O., Anujeonye, C. N., & Efozia, F. N. (2015). Dependable Community-Cloud Framework for Smartphones. *American Journal of Networks and Communications*, *4*(4), 95. https://doi.org/10.11648/j.ajnc.20150404.13

Ojugo, A. A., Akazue, M. I., Ejeh, P. O., Ashioba, N. C., Odiakaose, C. C., Ako, R. E., & Emordi, F. U. (2023). Forging a User-Trust Memetic Modular Neural Network Card Fraud Detection Ensemble: A Pilot Study. *Journal of Computing Theories and Applications*, *1*(2), 1–11. https://doi.org/10.33633/jcta.v1i2.9259

Ojugo, A. A., Akazue, M. I., Ejeh, P. O., Odiakaose, C., & Emordi, F. U. (2023). DeGATraMoNN : Deep Learning Memetic Ensemble to Detect Spam Threats via a Content-Based Processing. *Kongzhi Yu Juece/Control and Decision*, *38*(01), 667–678.

Ojugo, A. A., Allenotor, D., Oyemade, D. A., Yoro, R. E., & Anujeonye, C. N. (2015). Immunization Model for Ebola Virus in Rural Sierra-Leone. *African Journal of Computing & ICT*, *8*(1), 1–10. www.ajocict.net

Ojugo, A. A., & Eboka, A. O. (2014). A Social Engineering Detection Model for the Mobile Smartphone Clients. *African Journal of Computing & ICT*, *7*(3). www.ajocict.net

Ojugo, A. A., & Eboka, A. O. (2019).

Inventory prediction and management in Nigeria using market basket analysis associative rule mining: memetic algorithm based approach. *International Journal of Informatics and Communication Technology (IJ-ICT)*, *8*(3), 128. https://doi.org/10.11591/ijict.v8i3.pp128-138

Ojugo, A. A., Eboka, A. O., Yoro, R. E., Yerokun, M. O., & Efozia, F. N. (2015). Framework design for statistical fraud detection. *Mathematics and Computers in Science and Engineering Series*, *50*, 176–182.

Ojugo, A. A., & Ekurume, E. O. (2021a). Deep Learning Network Anomaly-Based Intrusion Detection Ensemble For Predictive Intelligence To Curb Malicious Connections: An Empirical Evidence. *International Journal of Advanced Trends in Computer Science and Engineering*, *10*(3), 2090–2102. https://doi.org/10.30534/ijatcse/2021/851032021

Ojugo, A. A., & Ekurume, E. O. (2021b). Predictive Intelligent Decision Support Model in Forecasting of the Diabetes Pandemic Using a Reinforcement Deep Learning Approach. *International Journal of Education and Management Engineering*, *11*(2), 40–48. https://doi.org/10.5815/ijeme.2021.02.05

Ojugo, A. A., Obruche, C. O., & Eboka, A. O. (2021a). Empirical Evaluation for Intelligent Predictive Models in Prediction of Potential Cancer Problematic Cases In Nigeria. *ARRUS Journal of Mathematics and Applied Science*, *1*(2), 110–120. https://doi.org/10.35877/mathscience614

Ojugo, A. A., Obruche, C. O., & Eboka, A. O. (2021b). Quest For Convergence Solution Using Hybrid Genetic Algorithm Trained Neural Network Model For Metamorphic Malware Detection. *ARRUS Journal of Engineering and Technology*, *2*(1), 12–23. https://doi.org/10.35877/jetech613

Ojugo, A. A., Odiakaose, C. C., Emordi, F. U., Ejeh, P. O., Adigwe, W., Anazia, K. E., & Nwozor, B. (2023). Forging a learner-centric blended-learning framework via an adaptive content-based architecture. *Science in Information Technology Letters*, *4*(1), 40–53. https://doi.org/10.31763/sitech.v4i1.1186

Ojugo, A. A., & Otakore, D. O. (2018). Redesigning Academic Website for Better Visibility and Footprint: A Case of the Federal University of Petroleum Resources Effurun Website. *Network and Communication Technologies*, *3*(1), 33. https://doi.org/10.5539/nct.v3n1p33

Ojugo, A. A., & Otakore, O. D. (2020). Computational solution of networks versus cluster grouping for social network contact recommender system. *International Journal of Informatics and Communication Technology (IJ-ICT)*, *9*(3), 185. https://doi.org/10.11591/ijict.v9i3.pp185-194

Ojugo, A. A., Ugboh, E., Onochie, C. C., Eboka, A. O., Yerokun, M. O., & Iyawa, I. J. B. (2013). Effects of Formative Test and Attitudinal Types on Students' Achievement in Mathematics in Nigeria. *African Educational Research Journal*, *1*(2), 113–117. http://search.ebscohost.com/login.aspx?direct=true&db=eric&AN=EJ1216962&site=ehost-live

Ojugo, A. A., & Yoro, R. E. (2020a). Empirical Solution For An Optimized Machine Learning Framework For Anomaly-Based Network Intrusion Detection. *Technology Report of Kansai University*, *62*(08), 6353–6364.

Ojugo, A. A., & Yoro, R. E. (2020b). Forging A Smart Dependable Data Integrity And Protection System

Through Hybrid-Integration Honeypot In Web and Database Server. *Technology Report of Kansai University*, *62*(08), 5933–5947.

Ojugo, A. A., & Yoro, R. E. (2020c). Predicting Futures Price And Contract Portfolios Using The ARIMA Model: A Case of Nigeria's Bonny Light and Forcados. *Quantitative Economics and Management Studies*, *1*(4), 237–248. https://doi.org/10.35877/454ri.qems139

Ojugo, A. A., Yoro, R. E., Oyemade, D. A., Eboka, A. O., Ugboh, E., & Aghware, F. O. (2013). Robust Cellular Network for Rural Telephony in Southern Nigeria. *American Journal of Networks and Communications*, *2*(5), 125. https://doi.org/10.11648/j.ajnc.20130205.12

Okobah, I. P., & Ojugo, A. A. (2018). Evolutionary Memetic Models for Malware Intrusion Detection: A Comparative Quest for Computational Solution and Convergence. *International Journal of Computer Applications*, *179*(39), 34–43. https://doi.org/10.5120/ijca2018916586

Okuyama, S., Tsuruoka, S., Kawanaka, H., & Takase, H. (2014). Interactive Learning Support User Interface for Lecture Scenes Indexed with Extracted Keyword from Blackboard. *Australian Journal of Basic and Applied Sciences*, *8*(4), 319–324.

Ometov, A., Shubina, V., Klus, L., Skibińska, J., Saafi, S., Pascacio, P., Flueratoru, L., Gaibor, D. Q., Chukhno, N., Chukhno, O., Ali, A., Channa, A., Svertoka, E., Qaim, W. Bin, Casanova-Marqués, R., Holcer, S., Torres-Sospedra, J., Casteleyn, S., Ruggeri, G., … Lohan, E. S. (2021). A Survey on Wearable Technology: History, State-of-the-Art and Current Challenges. *Computer Networks*, *193*, 108074. https://doi.org/10.1016/j.comnet.2021.108074

Oyemade, D. A., & Ojugo, A. A. (2020). A Property Oriented Pandemic Surviving Trading Model. *International Journal of Advanced Trends in Computer Science and Engineering*, *9*(5), 7397–7404. https://doi.org/10.30534/ijatcse/2020/71952020

Oyemade, D. A., & Ojugo, A. A. (2021). An Optimized Input Genetic Algorithm Model for the Financial Market. *International Journal of Innovative Science, Engineering and Technology, 8*(2), 408–419. https://ijiset.com/vol8/v8s2/IJISET_V8_I02_41.pdf

Oyemade, D. A., Ureigho, R. J., Imouokhome, F. ., Omoregbee, E. U., Akpojaro, J., & Ojugo, A. A. (2016). A Three Tier Learning Model for Universities in Nigeria. *Journal of Technologies in Society*, *12*(2), 9–20. https://doi.org/10.18848/2381-9251/CGP/v12i02/9-20

Pearson, J. M., Pearson, A., & Green, D. (2007). Determining the importance of key criteria in web usability. *Management Research News*, *30*(11), 816–828. https://doi.org/10.1108/01409170710832250

Peterson, K. (2006). Academic Web Site Design and Academic Templates: Where Does the Library Fit In? *Information Technology and Libraries*, *25*(4), 217. https://doi.org/10.6017/ital.v25i4.3354

Sasikala, G., Laavanya, M., Sathyasri, B., Supraja, C., Mahalakshmi, V., Mole, S. S. S., Mulerikkal, J., Chidambaranathan, S., Arvind, C., Srihari, K., & Dejene, M. (2022). An Innovative Sensing Machine Learning Technique to Detect Credit Card Frauds in Wireless Communications. *Wireless Communications and Mobile Computing*, *2022*, 1–12. https://doi.org/10.1155/2022/2439205

Singh, A. P., & Sharma, A. (2022). *A systematic literature review on insider*

threats. http://arxiv.org/abs/2212.05347

Sun, D., Liu, M., Li, M., Shi, Z., Liu, P., & Wang, X. (2021). DeepMIT: A Novel Malicious Insider Threat Detection Framework based on Recurrent Neural Network. *2021 IEEE 24th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, 335–341. https://doi.org/10.1109/CSCWD49262.2021.9437887

Tarafdar, M., & Zhang, J. (2005). Analyzing the influence of Web site design parameters on Web site usability. *Information Resources Management Journal*, *18*(4), 62–80. https://doi.org/10.4018/irmj.2005100104

Thorat, O., Parekh, N., & Mangrulkar, R. (2021). TaxoDaCML: Taxonomy based Divide and Conquer using machine learning approach for DDoS attack classification. *International Journal of Information Management Data Insights*, *1*(2), 100048. https://doi.org/10.1016/j.jjimei.2021.100048

Yoro, R. E., Aghware, F. O., Akazue, M. I., Ibor, A. E., & Ojugo, A. A. (2023). Evidence of personality traits on phishing attack menace among selected university undergraduates in Nigerian. *International Journal of Electrical and Computer Engineering (IJECE)*, *13*(2), 1943. https://doi.org/10.11591/ijece.v13i2.pp1943-1953

Yoro, R. E., Aghware, F. O., Malasowe, B. O., Nwankwo, O., & Ojugo, A. A. (2023). Assessing contributor features to phishing susceptibility amongst students of petroleum resources varsity in Nigeria. *International Journal of Electrical and Computer Engineering (IJECE)*, *13*(2), 1922. https://doi.org/10.11591/ijece.v13i2.pp1922-1931

Yoro, R. E., & Ojugo, A. A. (2019). An Intelligent Model Using Relationship in Weather Conditions to Predict Livestock-Fish Farming Yield and Production in Nigeria. *American Journal of Modeling and Optimization*, *7*(2), 35–41. https://doi.org/10.12691/ajmo-7-2-1

Yuan, S., & Wu, X. (2021). Deep learning for insider threat detection: Review, challenges and opportunities. *Computers and Security*, *104*. https://doi.org/10.1016/j.cose.2021.102221

Zardi, H., & Alrajhi, H. (2023). Anomaly Discover: A New Community-based Approach for Detecting Anomalies in Social Networks. *International Journal of Advanced Computer Science and Applications*, *14*(4), 912–920. https://doi.org/10.14569/IJACSA.2023.01404101

Zawislak, P. A., Reichert, F. M., Barbieux, D., Avila, A. M. S., & Pufal, N. (2022). The dynamic chain of innovation: bounded capabilities and complementarity in agribusiness. *Journal of Agribusiness in Developing and Emerging Economies*, *23*.