CHAPTER ONE

1.1 BACKGROUND TO THE STUDY

Globally, the novel coronavirus (Covid-19) has undoubtedly made the e-learning revolution more prominent. The advent of the World Wide Web (www) has created many opportunities. One such opportunity is electronic learning (e-learning). According to (Ajadi et al., 2008), e-learning is the use of electronic technology to deliver education and training applications, monitor learners' performance, and report learners' progress. A reimagined education can also include remote learning, which may include digital learning. By offering a variety of remedial programs, remote learning offers various ways to reduce the learning losses that children may experience during school closures brought on by crises, including those related to climate change. Nevertheless, with the declaration of global pandemic status for COVID-19 by the World Health Organization (WHO), numerous educational establishments were compelled to transition entirely from in-person teaching and learning approaches to electronic learning alternatives.

Krönke (2020) reported that UNESCO puts 1.2 billion students and the youth worldwide at a disadvantage as a result of closure of schools and universities due to Covid-19 pandemic; and in Africa, approaches to adaptations to changes in technology-enhanced learning keep improving, but at a snail's pace. One may assume that this phenomenon would have affected only under-developed and/or developing countries (Daniel et al., 2022). However, Allah (2013) stated that it is a global challenge for higher education institutions to effectively implement e-learning solutions.

In spite of this, Nigeria, categorized as a developing country, experienced significant impacts when the government declared the extensive shutdown of all educational establishments in response to the emergence of Covid-19 in March 2020. This made it abundantly clear to key education stakeholders in Nigeria that, regrettably, covid-19 had emerged to disrupt traditional methods, particularly in the area of education.

E-learning refers to any method of education involving electronic devices like smartphones or personal computers connected to the internet. It also encompasses audio/video lessons created by educators for learners, eliminating the need for in-person teaching. Given the substantial transformation caused by COVID-19, traditional practices were disrupted, compelling higher educational institutions to adopt innovative approaches in order to sustain academic activities. This is because almost all academic institutions had to completely move from face-to-face modes of teaching and learning to other modes (Daniel et al., 2022). (Crawford et al, 2020) concluded that inasmuch as some schools responded and keep responding proactively through the introduction of

innovative ways of teaching and learning during the period of the pandemic, other similar academic institutions are lagging.

In Nigeria, Adanikin et al. (2020) discovered that the effectiveness of e-learning implementation in educational institutions is hindered by factors such as expensive Internet expenses, inadequate Internet availability, unreliable electrical power supply, and the absence of access to electronic devices like smartphones and computers.

Cybersecurity involves safeguarding computers, servers, mobile devices, electronic systems, networks, and data against malicious attacks. However, the efficacy of cybersecurity relies heavily on the level of awareness a cyber-user possesses. As a result, being well-informed and educated serves as the primary shield against cybercrimes. Insufficient security knowledge among users is a significant driver behind the global surge in internet-related crimes and cybersecurity breaches. Cybercriminals take advantage of the ignorance of cyber users to perpetuate their malicious activities and this has been a major challenge to curbing cybercrimes (Kaspersky Lab 2023).

With Nigeria's burgeoning population of cyber users (Nigerian Bureau of Statistics, 2020), it is expected that a lot more information will be gathered, shared and added to the cyberspace which is open for exploitation Preserving this data has turned exceptionally crucial for both the security of cyber users and the stability of the economy. Hence, a cyber-user's awareness regarding cybersecurity will serve as a pivotal factor in deterring cyber-attacks initiated by online threats and maintaining the cybersecurity of our educational systems.

The COVID-19 pandemic brought to light both the strengths and weaknesses of the global education landscape, spanning developed and developing nations. Consequently, this ongoing research delved into the repercussions of the COVID-19 crisis on Nigeria's educational system, thereby proposing a unique solution to the challenges impeding the continuity of education in the country. The closure of schools for an extended period due to the initial impact of the COVID-19 outbreak, coupled with the incapacity of educational institutions to effectively involve students in remote learning during this period, further exposed the inadequacies of the education system within the nation. This revelation led to the identification of the absence of distance online education, webbased learning systems, and ICT infrastructure within Nigeria's educational framework. The incidence of COVID-19 disrupted the academic calendar, resulted in teacher attrition, amplified student dropout rates, and fostered disinterest in digital education. Consequently, this study explored the attitudes and readiness of students to embrace distance online education, utilizing online data to examine the various factors influencing these attitudes and willingness to participate in online learning.

1.2 STATEMENT OF THE PROBLEM

The rapid adoption of disruptive technologies in the educational sector in Nigeria, particularly in response to the COVID-19 pandemic, has brought about significant changes in teaching and learning. While these technologies offer numerous benefits, they also present cybersecurity implications that need to be addressed. Therefore, the problem statement for this study is as follows:

1. How do disruptive technologies, such as online learning platforms, artificial intelligence (AI), virtual and augmented reality (VR/AR), and Internet of Things (IoT), impact the educational sector in Nigeria during the post-COVID-19 pandemic period?
2. What are the specific cybersecurity implications that arise from the adoption of disruptive technologies in the educational sector in Nigeria?
3. What are the potential risks and challenges related to data privacy and protection, phishing and social engineering, network security, device security, and secure remote learning platforms in the Nigerian educational sector?
4. How does the cybersecurity landscape in the Nigerian educational sector contribute to the overall risk and vulnerability of educational institutions?
5. What policy and regulatory considerations should be taken into account to address the cybersecurity challenges and ensure a secure and resilient educational ecosystem in Nigeria?
6. What are the lessons learned and best practices from the post COVID-19 pandemic period that can guide the development of effective strategies for cybersecurity in the educational sector in Nigeria?

1.3 MOTIVATION FOR THE STUDY

The motivation for conducting this study stems from the following factors:

1. Rapid Technological Transformation: The COVID-19 pandemic accelerated the adoption of disruptive technologies in the educational sector, leading to a paradigm shift in teaching and learning. It is crucial to understand the impact of these technologies on education in Nigeria and examine their implications for cybersecurity.
2. Emerging Cybersecurity Challenges: The increased reliance on digital platforms and online learning exposed educational institutions to new cybersecurity risks and vulnerabilities. It is

essential to identify and understand these challenges to develop effective strategies and safeguard student and staff data.

3. Protection of Sensitive Information: Educational institutions handle a vast amount of sensitive information, including student records, academic data, and personal details. It is imperative to examine the cybersecurity implications to ensure the privacy, integrity, and confidentiality of this information.
4. Vulnerability of the Educational Sector: Educational institutions, particularly in developing countries like Nigeria, may face resource constraints and limited cybersecurity awareness. Investigating the cybersecurity landscape can shed light on the vulnerabilities present in the sector and help identify areas that require attention.
5. Policy and Regulatory Considerations: The study can provide insights into the policy and regulatory frameworks needed to address cybersecurity challenges in the educational sector. It can inform policymakers in Nigeria on the necessary measures to protect educational institutions from cyber threats and promote a secure learning environment.
6. Resilient and Inclusive Education: By understanding the implications of disruptive technologies and cybersecurity in education, stakeholders can develop strategies to ensure a resilient and inclusive educational ecosystem in Nigeria. This includes bridging the digital divide and providing equitable access to quality education while maintaining data security.
7. Lessons for Future Preparedness: The post COVID-19 pandemic period provides an opportunity to reflect on the challenges faced and lessons learned. This study can contribute to the knowledge base for future preparedness and resilience, enabling educational institutions to navigate future disruptions effectively.

1.4 AIM AND OBJECTIVES OF THE STUDY

AIM:

To assess the impact of disruptive technologies and the associated cybersecurity implications in the educational sector in Nigeria, with a focus on the post COVID-19 pandemic period.

OBJECTIVES:

1. To examine the adoption and utilization of disruptive technologies, such as online learning platforms, AI, VR/AR, and IoT, in the Nigerian educational sector during and after the COVID19 pandemic.

2. To identify and analyze the specific cybersecurity implications arising from the adoption of disruptive technologies in the educational sector in Nigeria.
3. To evaluate the current cybersecurity landscape in the Nigerian educational sector, including vulnerabilities and threats faced by educational institutions.
4. To propose policy and regulatory considerations for addressing cybersecurity challenges and ensuring a secure and resilient educational ecosystem in Nigeria.
5. To provide recommendations for policymakers, educators, and stakeholders in Nigeria to mitigate cybersecurity risks, protect sensitive data, and promote a secure and resilient educational environment in the face of disruptive technologies.

1.5 SIGNIFICANCE OF THE STUDY

This study holds significant importance for various stakeholders. The significance of this study can be outlined as follows:

1. Policy Development: The study provides valuable insights into the impact of disruptive technologies and cybersecurity challenges in the educational sector. Policymakers can use this information to develop and update policies and regulations that address the unique needs and risks associated with technology adoption in education. It can help shape policies that promote secure and resilient educational ecosystems in Nigeria.
2. Enhanced Cybersecurity: By identifying the specific cybersecurity implications in the educational sector, the study raises awareness among educational institutions, administrators, and educators. It helps them understand the potential risks and vulnerabilities associated with disruptive technologies, enabling them to implement effective cybersecurity measures and protect sensitive data. This can lead to improved data privacy, enhanced network security, and better overall cybersecurity practices in the educational sector.
3. Student and Staff Protection: The study's findings and recommendations contribute to the protection of students and staff members within the educational sector. By addressing cybersecurity challenges, educational institutions can ensure the privacy and security of student records, personal information, and academic data. This fosters trust and confidence among students, parents, and stakeholders, creating a safe and secure learning environment.
4. Digital Transformation: The study explores the impact of disruptive technologies in education, such as online learning platforms, AI, VR/AR, and the social media. Understanding these technologies' implications allows educational institutions to harness their benefits effectively, thereby promoting digital transformation in teaching and learning. This can lead to improved

educational outcomes, expanded access to quality education, and increased engagement among students.

5. Resilience in Crisis Situations: The COVID-19 pandemic highlighted the need for educational institutions to be resilient and adaptable to sudden disruptions. By assessing the post-pandemic period, the study provides insights into lessons learned and best practices for future crisis situations. It equips educational institutions with the knowledge and strategies to navigate similar challenges effectively, ensuring uninterrupted education and continuity of learning.
6. International Perspective: The findings of this study can contribute to the global discourse on disruptive technologies and cybersecurity implications in education. As the world becomes increasingly interconnected, understanding the experiences and challenges faced by the Nigerian educational sector can offer valuable insights to educational institutions and policymakers globally, promoting international cooperation and collaboration in addressing cybersecurity in education.

1.6 DEFINITION OF TERMS

1. Artificial Intelligence (AI): Artificial Intelligence refers to the development of computer systems capable of performing tasks that would typically require human intelligence. In the context of education, AI technologies can be used for various purposes, such as personalized learning, intelligent tutoring systems, automated grading, and data analysis for educational insights.
2. Cybersecurity: Cybersecurity refers to the practice of protecting computer systems, networks, and data from unauthorized access, cyber threats, and attacks. It encompasses measures and strategies designed to ensure the confidentiality, integrity, and availability of information in the digital realm.
3. Data Privacy and Protection: Data privacy and protection refer to the measures and practices put in place to safeguard the confidentiality, integrity, and availability of personal and sensitive information. It involves ensuring that data is collected, stored, and processed securely, and that individuals' privacy rights are respected.
4. Device Security: Device security refers to the protection of computers, smartphones, tablets, and other devices used for educational purposes against unauthorized access, malware, and data breaches. It involves implementing security measures such as password protection, antivirus software, device encryption, and regular software updates.
5. Disruptive Technologies: Disruptive technologies refer to innovations that significantly alter existing markets, industries, or systems by introducing new approaches, products, or services.

In the context of this study, disruptive technologies include online learning platforms, artificial intelligence (AI), virtual and augmented reality (VR/AR), and the Internet of Things (IoT) as they pertain to the educational sector.

6. Educational Sector: The educational sector refers to the collective institutions, organizations, and systems involved in providing education and learning opportunities. This includes schools, colleges, universities, educational authorities, regulatory bodies, and stakeholders associated with the delivery and management of education.
7. Internet of Things (IoT): The Internet of Things refers to a network of interconnected physical devices, objects, and sensors embedded with software, sensors, and connectivity capabilities. In the educational context, IoT devices can be used to enhance learning experiences, monitor environmental conditions, track assets, and enable smart campus solutions.
8. Network Security: Network security focuses on protecting computer networks and the data transmitted within them from unauthorized access, misuse, and attacks. It involves implementing security measures such as firewalls, intrusion detection systems, encryption, and network monitoring to ensure network integrity and confidentiality.
9. Online Learning Platforms: Online learning platforms are digital platforms that facilitate the delivery of educational content and interactions between educators and learners in a virtual environment. These platforms typically include features such as video lectures, discussion forums, assignments, and assessments, enabling remote learning and collaboration.
10. Phishing and Social Engineering: Phishing and social engineering involve deceptive techniques used by malicious actors to trick individuals into revealing sensitive information or performing actions that may compromise their cybersecurity. Phishing typically occurs through fraudulent emails or websites, while social engineering exploits human psychology to manipulate individuals into providing access to confidential data or systems.
11. Post COVID-19 Pandemic: Post COVID-19 pandemic refers to the period following the global outbreak of the COVID-19 virus. It signifies the time when the initial impact of the pandemic has subsided, and societies are transitioning to a new normal, with adjustments made in response to the challenges posed by the pandemic.
12. Secure Remote Learning Platforms: Secure remote learning platforms are online learning platforms that prioritize data privacy and protection. These platforms employ encryption, secure authentication mechanisms, and other security measures to ensure the confidentiality and integrity of student and educator data during remote learning activities.
13. Virtual and Augmented Reality (VR/AR): Virtual Reality (VR) is a technology that creates a simulated environment, immersing users in a computer-generated three-dimensional world.

Augmented Reality (AR) overlays digital information onto the real world, enhancing the user's perception and interaction with the environment. VR and AR have applications in education for immersive experiences, virtual field trips, and interactive learning.

CHAPTER TWO LITERATURE REVIEW

2.1 INTRODUCTION TO DISRUPTIVE TECHNOLOGIES IN EDUCATION

Any technological advancement that displaces an established technology by creating an entirely new industry is deemed disruptive. Such disruptive technology not only forges fresh markets but also reshapes existing ones, thus offering customers and end users the utmost access, authority, convenience, variety, and value. The central essence of disruptive technology revolves around its capacity to challenge established business models and drastically reshape the landscape of products and services. Coined by Joseph Bower, a Harvard Professor, and Clayton Christensen, a businessman, in 1995, the term "disruptive technology" characterizes technologies that substantially deviate from existing ones, often through simplification, greater accessibility, and reduced costs (Uwa, 2017).

Disruptive technologies creates an entirely new industry or product by displacing conventional technology. According to Dawsey (2022), five (5) disruptive technologies in education are online learning (o-Learning), Artificial Intelligence (AI) Guided learning, Chat-Based collaboration, Virtual and Augmented Reality (VR and AR). E-learning is disrupting conventional classroom learning (U-EENI, 2022). Hence, disruptive technology is conceptualized in this study as that technological innovation that majorly changes the processes, procedures or methods enterprises, institutions, industries operate their affairs.

E-Learning According to Hedge et al (2004) cited in Gunga (2010) e-learning is an innovative methodology for conveying electronically facilitated, learner-centered, well-designed, and interactive learning environment to anybody at any time and at any place through the utilization of the internet and digital technology. Osuji et al (2019) defined e-learning as the method of accessing online teaching, learning and research materials with the application of ICT facilities.

In this study, e-learning encompasses the utilization of digital technologies or ICTs, which include but are not limited to the Internet, the Web, mobile phones, tablets, computers, and social media. This integration aims to facilitate education both within the traditional classroom environment and beyond its boundaries, regardless of whether the approach is asynchronous, synchronous, or a combination of both.

However, e-learning manifests itself in a multitude of forms, applications, and platforms. Examples encompass diverse options such as phone-in radio programs, interactive television shows, satellite broadcasts, Internet or Web-based methods, ethernet, intranets, extranets, CDs, DVDs, digital textbooks (e-textbooks), cloud computing, instant messaging, video conferences, podcasts, and various mobile technologies. Additionally, it encompasses an array of platforms that support multimedia sharing, including Skype, audio/video conferencing tools, WhatsApp, Adobe Connect,

webinars, blogs, video blogging (vlogging), wikis, YouTube, Flicker, Twitter, ScoopIt, and Facebook. These applications, platforms, and tools facilitate various modes of teaching and learning, ranging from traditional face-to-face interactions with a teacher's presence (synchronous learning) to blended synchronous learning involving both online and offline presentations with or without a teacher's presence, and asynchronous learning, where teacher presence may be absent.

2.1.1 Disruptive technologies in educational sector:

i. When we contemplate the influence of disruptive technologies on education, one of the foremost aspects that comes to thought is the impact of online learning. This transformative technology has fundamentally altered the manner in which educational institutions offer their services. Internet-based education presents novel prospects for both learners and instructors. It can address the educational needs of individuals who, for various reasons, lack access to conventional learning methods. Given its convenient accessibility, individuals such as parents, those who are employed full-time, and people with disabilities can exploit this avenue to pursue education without the need to physically attend educational facilities. It serves as a useful tool for improving quality teaching and learning by increasing the teachers' motivation to teach and students' motivation to learn and by playing the crucial role of preparing a new crop of teachers, and up-skilling existing teachers to meet twenty-first century pedagogical expectations (Oye et al, 2011).

   E-learning promotes dynamic engagement in learning, providing learners with the autonomy to progress through material at their preferred speed. Additionally, it facilitates group-based and cooperative learning undertakings among students. These aspects collectively enhance the development of advanced cognitive skills among students, leading to an eventual enhancement in the absorption and retention of knowledge. Furthermore, this approach yields improved academic success rates and overall learning outcomes. For example, Obuekwe et al (2017) noted that e-learning environments enrich and deepen skills, promote individualized learning, strengthen teaching by drawing the world closer to the classroom, and relating learning experiences to the real world of work, as well as creating economic viability for workers of the future.

ii. Collaboration platforms equipped with chat features enable global participation in the educational journey. Moreover, educators can engage experts from their respective domains to partake in online discussions, engaging directly with students. The progress in online learning tools is contributing to elevating the influence and reach of higher education, rendering it more influential and attainable for a broader demographic. iii. Competency-driven education (CDE) encompasses the notion that students embark on their educational journey with distinct skills and varying learning paces. The core objective revolves around evaluating these disparities and shaping adaptable learning schemes. The aim is to amplify students' participation in education while averting scenarios where students are compelled to revisit familiar knowledge. CDE strives to personalize the learning experience, resulting in more effective knowledge acquisition. If a learner necessitates more time to grasp a specific subject, CDE systems precisely gauge this requirement. This transformative educational technology accommodates the learning needs of students who deviate from the conventional archetype of a typical learner.

iv. Virtual Reality (VR) extends beyond gaming and entertainment, converging the advantages of both traditional in-person and online education within an immersive encounter. This technology offers an exceedingly authentic and cost-effective means of exploring otherwise unfeasible situations. VR permits the creation of affordable yet authentic scenarios that hold educational value for disciplines like medicine, archaeology, physics, and various other subjects.

v. Artificial Intelligence (AI) possesses the potential to utilize algorithms that tailor the learning encounter. AI systems can discern how a specific learner engages with information and assess the requirements of an individual student or an entire class. Given the present state of technological advancement, AI systems within transformative education have the capability to provide personalized guidance and facilitate discussions.

vi. In education, the utilization of case-based or project-based instruction proves efficacious by bridging the divide between theoretical concepts and practical application. Additionally, students express heightened involvement in their studies when case studies form a part of the curriculum. Despite their effectiveness, these approaches are not as commonly employed in the classroom as the more conventional lecture-centered teaching methods.

vii. In the realm of education, the integration of Augmented Reality (AR) presents learners with the opportunity to enhance their comprehension of concepts through the utilization of threedimensional models. AR permits the addition of supplementary information onto the physical reality by means of smartphones or tablets. By employing this transformative

technology, educators can deliver engaging presentations capable of capturing students' interest, even when the subject matter may initially appear less captivating.

viii. The advent of the Internet of Things has unfurled a realm of fresh possibilities within higher education. Enhanced interconnection among devices and commonplace items translates to improved data tracking, analytics, and enhanced communication among students, educators, and institutions, often without requiring verbal interaction. IoT simplifies learning for students, allowing them to choose when, where, and how they learn, while offering professors the means to cultivate a more adaptable and interconnected learning milieu. With the integration of IoT technologies, predictive analytics gain the capacity to furnish additional insights into student performance both in the classroom and on campus. Given the appropriate infrastructure, universities stand poised to respond to early cues of students who might be at risk academically, intervening at that pivotal juncture before their performance wanes. The potential that IoT offers higher education is seemingly only restricted by the creativity of those implementing it (Gejendhiran et al 2020).

2.2 THE BENEFITS AND CHALLENGES ASSOCIATED WITH THE ADOPTION OF DISRUPTIVE TECHNOLOGIES IN EDUCATION

BENEFITS:

1. **Enhanced Accessibility and Flexibility**: Disruptive technologies in education enable learners to access educational resources and opportunities remotely, breaking down barriers of time, location, and physical limitations. Online learning platforms and mobile applications allow learners to engage in self-paced learning, access course materials at their convenience, and participate in collaborative activities regardless of their geographical location. With the integration of e-learning into academic institutions, governments, institutions, and individual learners will be saving a lot of cost. Irrespective of race, creed, and gender, education through technology gives people the opportunity to stand out in their lives and in their communities (Isaac 2021). The need for physical infrastructure by way of classroom facilities will be reduced. Likewise, students do not need to travel to far away places to enroll in programmes and courses of their choice if they are available online (Gordon et al 2021).

2. **Personalized and Adaptive Learning**: Disruptive technologies leverage data analytics, artificial intelligence, and learning algorithms to provide personalized learning experiences tailored to individual student needs and preferences. By providing support to differently abled persons, engaging learners who do not respond well to conventional educational settings, providing opportunities to enhance learning by the gifted and talented learner, and by developing independent

learning skills through professional learning experiences (Malale, et al, 2019). Most especially, by enabling self-study at one's own pace and personalized learning, e-learning helps older learners overcome the learning challenges posed by physical disabilities and coping with one's numerous roles as an adult. It also enhances face-to-face interactions during teaching and administration, and creates room for integration into the work place. Adaptive learning platforms can adjust the pace, content, and delivery of instruction based on the learner's progress and learning style, promoting more effective and engaging learning experiences.

3. **Engagement and Interactivity**: Disruptive technologies offer interactive and engaging learning experiences that go beyond traditional classroom settings. It offers greater access to information; better communication; increased cooperation and collaboration; synchronous learning; Virtual reality (VR) and augmented reality (AR) applications provide immersive and improved pedagogy through simulations and virtual laboratories/experiences, and impacting academic goal achievement, and by helping to meet the needs of the knowledge based economy.

Enabling hands-on exploration and enhancing understanding and retention of complex concepts (Wu H.K et al 2013.

4. **Collaboration and Communication**: Disruptive technologies facilitate collaborative learning environments where students can interact with peers and educators, fostering communication, teamwork, and knowledge sharing. Online discussion forums, video conferencing tools, and collaborative platforms enable learners to engage in meaningful discussions, collaborate on projects, and receive feedback from peers and instructors. Digital environments offered far greater independence regarding choice of learning, a faster rate of information transfer, reduced costs, and increased access to education (Meskhi et al, 2019). As noted by Deb (2011) in the earlier literature this provided students with the opportunity for self-learning or study. Thus, the usefulness of digital technology and the promise that it held, as can be seen in its wide applications in teaching, management and administration, and research (Ouma et al, 2013), warranted its current integration into institutions of learning, especially at the tertiary level.

CHALLENGES:

1. **Infrastructure and Access Disparities**: The adoption of disruptive technologies in education requires reliable internet connectivity, adequate hardware, and access to digital devices. However, disparities in infrastructure and access can limit the equitable implementation of these technologies, particularly in underserved areas or among marginalized populations.

Several factors including inadequate study routines, a sense of isolation among learners, limited interaction and collaboration among peers, delayed instructor responses to queries, particularly in

asynchronous settings, and standardized instructional content that may hinder the potential for revision or creative adaptation.

2. **Technological Readiness and Digital Skills**: An evident digital disparity is apparent not only between nations but also within institutions and learners in developing countries such as Nigeria. The availability of high-speed Internet broadband is unevenly distributed across numerous regions in the developing world, Nigeria included. Furthermore, considering the reliance of ICTs on a consistent power supply, the precarious state of electricity in Nigeria presents a considerable obstacle to the seamless implementation of e-learning platforms. Despite the proliferation of ICTs, a significant number of individuals still struggle to afford the premium instructional materials necessary for contemporary online learning encounters. Individual differences with respect to ereadiness are also prevalent as many still lack basic computing skills to undertake e-learning modes of study. Educators and learners need adequate technological readiness and digital literacy skills to effectively utilize disruptive technologies. Lack of training and support for teachers in integrating these technologies into their pedagogical practices can hinder successful implementation and impact on learning outcomes.

3. **Privacy and Security Concerns**: Employing transformative technologies entails the compilation and safekeeping of student information, giving rise to apprehensions about privacy and protection. Educational establishments must establish robust security protocols to shield student records from potential breaches.

2.3 THE IMPACT OF DISRUPTIVE TECHNOLOGY ON EDUCATION IN NIGERIA:

In the contemporary era, addressing severe poverty effectively necessitates equipping individuals in impoverished communities with digital skills and resources. This is imperative due to our engagement in the most significant communication transformation of the past five centuries. This revolution is of such magnitude that it is causing disruption across all industries.

Therefore, to survive and thrive, even the poor need access to digital resources so that they can use it to add value to themselves, their communities, and the world at large (Isaac 2021).

The use of digital technologies has become an intrinsic aspect of the lives of digital natives, who have grown up in a digital era surrounded by technology. These digital natives are comfortable and fluent in using digital tools, and as a result, the integration of digital technologies has become a natural and inseparable part of their educational experiences.

In the digital classroom, students interact with digital technologies in various ways, such as using laptops, tablets, or smartphones for accessing educational resources, participating in online discussions, conducting research, creating multimedia presentations, and submitting assignments

electronically. Digital technologies enable them to access vast amounts of information, collaborate with peers, and engage in interactive and multimedia-rich learning experiences.

Moreover, digital natives actively engage with digital course work. They are accustomed to using online learning management systems, educational apps, and digital content platforms to access course materials, submit assignments, take quizzes, and engage in virtual discussions or collaborative activities. They leverage digital tools to organize their coursework, manage their time, and communicate with their peers and instructors.

The integration of digital technologies in education offers several advantages for digital natives. It enhances their digital literacy skills, as they learn to navigate and evaluate digital information effectively. Digital tools provide opportunities for active and hands-on learning experiences, promoting student engagement and participation. They also facilitate personalized learning, allowing students to learn at their own pace and explore topics of interest.

However, it is essential to recognize that not all students are digital natives, and there can be a digital divide in terms of access to technology and digital literacy skills. It is crucial for educators to be mindful of these differences and provide necessary support and resources to ensure equitable access and opportunities for all students.

The use of digital technologies has become an intrinsic part of the educational experiences of digital natives. These technologies empower students to actively engage in the digital classroom and interact with course work, offering new possibilities for learning, collaboration, and personalization.

The research findings indicate that the current generation of digital students in the study are not only familiar with but also motivated by various digital technologies, such as digital mobile computing, e-Learning education functionalities, multimedia tools, and ICT gadgets. This suggests that educators, including teachers and lecturers, should leverage these students' digital potentials, teaching abilities, and learning opportunities to create a more effective and engaging learning environment for the next generation of digitally driven learners. It also highlight the positive impact of multimedia technologies on students' cognitive processes and learning experiences. The continuous exposure to multimedia tools as part of their digitally rich lives has been observed to influence the structure of their brains and impact the way they think, learn, and respond to digital scenarios. This emphasizes the transformative potential of multimedia technologies in shaping students' learning behaviors and outcomes.

Given the availability of multimedia tools, ICT resources, and e-learning education functionalities, the research findings suggest a hopeful outlook for educational growth and survival. By effectively

integrating these tools into teaching and learning practices, educators can tap into the students' digital stimulation and create a more dynamic and interactive educational environment. This can lead to improved educational outcomes and better preparedness for the digital age.

Overall, the research findings support the idea that embracing multimedia technologies and leveraging their potential in education can contribute to a positive learning experience for students and enhance their educational journey in the digital era.

2.4 CHALLENGES FACED BY EDUCATIONAL INSTITUTIONS, EDUCATORS, AND STUDENTS IN INTEGRATING DISRUPTIVE TECHNOLOGIES INTO THE NIGERIAN EDUCATION SYSTEM.

Nigeria's education sector faces many challenges that have contributed to keeping more than 10.5 million children out of school in Africa's most populous nation (OCHA, 2023).

Before COVID-19, about 10.5 million Nigerian children aged between 5 and 14 were not in school. Today in Nigeria, more than 9.7 million children are at risk of never returning to school, their learning left behind (Catherine, 2023)

1. **Digital Divide**: The digital divide refers to the gap in access to technology and internet connectivity between different regions, institutions, and individuals. In developing countries like Nigeria, there can be disparities in access to high-speed internet broadband, with rural areas often having limited or no connectivity. This hampers the ability of learners in those areas to fully participate in online learning activities. However, as over fifty percent of Nigeria's populace lacks internet connectivity, a significant portion of these initiatives remain inaccessible to numerous Nigerian learners. This is predominantly attributed to the comparatively elevated expenses associated with technology and internet entry for individuals residing in impoverished circumstances. This has created a huge digital divide — inequalities in access to and use of new media technologies — in which children from rural areas and vulnerable communities in urban centers are unable to continue learning, while those from more affluent backgrounds or whose parents can afford remote learning leave them behind. Both the digital divide and COVID-19 have shown us that we must innovate to help Nigerian children fulfil their right to an education.

2. **Power Infrastructure:** Reliable and uninterrupted electricity supply is crucial for the effective implementation of ICT-based systems, including e-learning. However, Nigeria, like many other developing countries, faces challenges with power infrastructure. Frequent power outages or

unreliable electricity supply can disrupt e-learning sessions and create barriers to accessing online materials.

3. **Affordability of Instructional Media**: While ICTs are becoming more common, the cost of quality instructional media, such as computers, tablets, and internet access, can still be a significant barrier for many individuals, especially those from low-income backgrounds. Affordability issues can limit the access and participation of students in e-learning programs
4. **E-Readiness and Digital Skills:** Individual differences in e-readiness, including basic computing skills and digital literacy, pose challenges for effective e-learning implementation. Not all students may have the necessary computer skills or familiarity with digital tools and platforms, hindering their ability to navigate and engage in online learning experiences. By addressing these challenges and taking proactive measures, the implementation of e-learning in Nigeria can become more inclusive and effective, ensuring that all learners have equal opportunities to benefit from digital education initiatives.

2.5 CYBER SECURITY IMPLICATIONS IN THE EDUCATIONAL SECTOR

Universities are highly dependent on the Internet and cyberspaces within it to actualize their statutory responsibilities. Cyberspace refers to an interconnected and interdependent information technology (IT) based networks that include the Internet, telecommunication networks, computer systems, and social systems. Cyberspaces have evolved tremendously over the years, providing a variety of digital platforms universities need to manage teaching, learning, research, community development and administration. Cyberspaces have helped universities to manage admission processes, students' life issues, finance, examinations and records, and to facilitate academic processes. Consequently, each modern university undertakes its mandated duties and provides services to various stakeholders including faculty, students, parents, guardians, funding entities, governmental bodies, accreditation agencies, and more, utilizing virtual domains. Despite the considerable advantages that these virtual spaces bring to universities, they concurrently present noteworthy risks and challenges to their functionality and operations. This is primarily due to the evolution of cybercrimes and their proliferation in recent times. Existing literature highlights that within the virtual realms employed by universities to fulfill their obligations, a variety of perpetrators have arisen, proving particularly elusive to identify and apprehend. Instances of cybercrimes in academic institutions have led cybersecurity experts to acknowledge that cybercrime is not confined solely to financial institutions and related sectors.

2.6 CYBERCRIME IMPLICATIONS IN THE EDUCATIONAL SECTOR

Cybercrime has become the world's second-largest man-made risk. It encompasses all illegal activities perpetrated by scammers, hackers, and internet fraudsters. The illegal activities may include human activities carried out to gain illegal access to data and information or sending spam, malware, worms into devices, networks, or even organizational information systems and global connection to make them malfunction. Cybercrimes have had debilitating effects on individuals, governments, organizations, and universities. It has cost billions of dollars' worth of damages, data loss, and website defacement. It has sent many governments, organizations, and individuals into bankruptcy and global shock (De Paoli et al., 2020). Cybercrime has remained a major threat to universities, particularly as it touches that core mandates of teaching, learning, research, community services, and administration and management of staff and student records (Bukhari et al, 2018). There are indications in the extant literature that the COVID-19 era is likely to result in a surge in the number of cybercrimes perpetrated against universities. The COVID-19 has forced an increase in the dependence on cyberspace for both individuals and organizations and that this is likely to result in cybersecurity threats and risks. Morgan (2020) also observed that more than four thousand malicious COVID-19 related websites appeared on the internet within months of the first COVID19 pandemic in 2020. He argued that the occurrence of cybercrime in 2021 would be in every eleven seconds; a fit that is almost four times the average in 2020 (every nineteen seconds) and almost twice the pace in 2019 (every forty seconds) (Morgan, 2020). Meanwhile, cybercrime is projected to cost the global economy $6 trillion yearly from 2021, up from $3 trillion in 2015. While from 2025, cybercrime will cost $10.5 trillion annually. Besides the United States and China, cybercrime would eventually be the world's third-largest economy (WEF, 2020). Losses to ransomware are projected to cost the world $20 billion by 2021, which is 57 times what they were in 2015 ($325 million) (Chapman, 2019; Morgan, 2020). Consequently, ransomware stands as the swiftest expanding type of cyber misconduct, even within the university context. Moreover, spear-phishing emails constitute the approach employed in 91 percent of cyber assaults, infiltrating both institutions and educational establishments. There's no denying that existing literature underscores the necessity for a sturdy framework for managing cybersecurity. Such a framework would supply practical insights to organizations and universities, addressing the escalating demands of this domain.

This further emphasizes the importance of a robust cybersecurity management framework for organizations and universities in Nigeria. It acknowledges the need for actionable knowledge to

address cybercrime and related incidents. The Office of the National Security Adviser (NSA) and the National Information and Technology Development Agency (NITDA) in Nigeria, along with Microsoft and the National Institutes of Standards and Technology, recognize the threats and advocate for the implementation of a consolidated cybersecurity framework. While the existing frameworks primarily target sectors like finance, oil and gas, and conglomerates, the statement highlights the significance of developing a specific cybersecurity framework tailored for Nigerian universities. This endeavor is seen as valuable and worthwhile to ensure effective cybersecurity measures within the higher education sector (Osho & Onoja 2015).

2.7 CYBERSECURITY CHALLENGES AND RISKS FACED BY EDUCATIONAL INSTITUTIONS IN NIGERIA

Cybersecurity is derived from two words: cyber and security. According to Valeriano and Maness (2015), cyber is related to the technology which contains systems, network and programs or data (Valeriano & Maness, 2015). On the other hand, Schneier (2009) argued that security relates to protection of systems, network, application, and information. Sanoo (2018) further described cybersecurity as the protection of interconnected systems, including hardware, software, and data from cyber-attacks. One important factor that Valeriano and Maness (2015), Sanoo (2018) and Schneier (2009) did not include in their definitions is the social: values, norms and cultures conjectured by organizations as suitable and logical ways of behaving and relating with others. Cybersecurity finds diverse applications within universities, with each institution tailoring its usage based on specific needs. Across the globe, the majority of universities have implemented cybersecurity measures to safeguard their networks and digital information. Renowned institutions like the University of Arizona, University of Edinburgh, University of Bristol, University of Sheffield, Princeton University, University of Illinois, University of Leicester, Carnegie Mellon University, and University of Pittsburgh, especially those in developed nations, employ various cybersecurity frameworks to effectively address risks associated with cybersecurity.

The framework deployed helps to facilitate the strategic vision of the universities and facilitate the protection of information systems against compromise of its confidentiality, integrity, and availability (Webb et al, 2018). In the process, this acknowledges the potential to uncover, cultivate, and exchange knowledge among staff members. Numerous research endeavors were undertaken to investigate matters related to cyber security vulnerabilities in Nigerian higher education institutions. A study conducted by Ekpoh et al. (2020) in which factors that served as cybersecurity threats to universities were examined at University of Lagos, it was found in the study that there existed a strong positive relationship between location, culture, facilities and personnel security of universities, while a weak, positive correlation existed between school climate and personnel

security. The research findings deduced that lack of discipline, insufficient awareness regarding safety and security among both staff and students, inadequate training for security personnel, insufficient funding for institutions, and outdated security protocols were the primary factors contributing to security deficiencies within Nigerian universities. A study was conducted by Dagogo et al (2005) on the role of security agents in curbing cybercrimes in Universities in the North-East Nigeria using seven tertiary institutions. The research findings unveiled that the training and ongoing education of security personnel and cybersecurity experts have a substantial impact on their performance and service quality. Statistically, Nigerian universities ranked 43 in Europe, the Middle East and Africa and ranked third among the nations that commit cybercrime in the world (Makeri, 2017).

The Nigerian academic and educational sector faced heightened susceptibility to cyberattacks due to the presence of numerous valuable materials within this domain that attracted the interest of malicious actors. Consequently, the education sector must take immediate action and establish partnerships with security agencies as the threat is indeed substantial.

The education sector is based on critical data and this critical data we cannot afford to expose them to malicious or opportunistic attackers (Ishaq, 2021). Abubakar (2021) executive secretary of the National Universities Commission (NUC) said, cybercrime had continued to pose serious threats to educational data as well as other materials, the commission was fully aware of the danger posed by the activities of cyber-criminals.

2.8 EXAMINATION OF COMMON CYBERSECURITY THREATS IN THE EDUCATIONAL SECTOR

In the aftermath of the pandemic, cybersecurity stands as a substantial worry for colleges and universities. Even prior to the pandemic's impact, higher education institutions had been amassing significant volumes of data from both students and faculty. This concern has become even more pronounced now, with numerous universities adopting hybrid or entirely remote teaching approaches.

Because colleges and universities store such massive amounts of data, they are often a target of hackers and other cyber criminals. To be precise, there were 1,851 instances of data breaches occurring in educational establishments from 2005 to 2021. Moreover, numerous universities possess obsolete or inadequately designed cybersecurity infrastructures, thereby rendering them even more susceptible. Given the multitude of impending cybersecurity risks, tertiary education institutions must proactively implement measures to avert these threats. Gaining insight into the specific categories of security threats pertinent to colleges and universities can facilitate the

formulation of a robust cybersecurity plan. In this research, we'll take a look at the top five cybersecurity threats facing universities today and how to address them.

1. **Phishing**: Phishing stands as a prevalent issue within the realm of colleges and universities. In a phishing assault, hackers assume the guise of a trusted source and exploit this perception to deceive users into divulging sensitive information such as passwords or even social security numbers. Phishing generally transpires through email or messages on social media platforms. Hackers typically employ various tactics to target colleges and universities through phishing. One approach involves masquerading as the educational institution to acquire student or faculty login credentials. Once acquired, hackers can utilize this data to breach the university's digital systems and gain access to an array of valuable information.

Another strategy entails focusing on university presidents or specific faculty members. These individuals might possess particular datasets that hackers seek, or they could be high-value targets. Hackers meticulously analyze the behavior of these targets to devise the most effective means of gaining their trust. This strategy is often referred to as spear phishing or whaling. Phishing schemes are among the most potent forms of cyber-attacks due to their capacity to evade detection and countermeasures. This modus operandi has transcended email communication and has even surged amidst the Covid-19 era. Attackers have expanded their techniques to include SMS and phone calls to illicitly obtain confidential information such as login credentials. Additionally, the acquisition of users' confidential or sensitive data becomes facile when users inadvertently access counterfeit websites or download files from insecure sources.

Educating both students and staff on how to discern phishing messages can be remarkably effective in thwarting successful attacks. This is particularly crucial since many students and faculty utilize personal electronic devices on campus, which may lack adequate security measures. Implementing two-factor authentication also proves highly efficacious in preventing phishing attacks. With this approach, students and faculty are mandated to input a code received via email or phone, along with their password, to gain access to the university's system. Applications like Google Authenticator make implementing this security protocol relatively straightforward.

2. **Ransomware**: Ransomware poses another significant obstacle confronting today's colleges and universities. Ransomware, a form of malicious software, locates valuable data within a targeted system and seizes it, demanding a ransom in return. Given that educational institutions house substantial amounts of crucial student information and engage in valuable high-level research, it's unsurprising that ransomware has become a preferred tactic for many hackers seeking to exploit them. The aftermath of a ransomware attack can be catastrophic for any university. The

demanded ransoms in such attacks can be exorbitant, often leading to severe financial strain. Moreover, these attacks jeopardize critical data and can even paralyze systems for extended durations, significantly hampering regular operations. Furthermore, the repercussions of a ransomware attack can cast a shadow over a university's reputation for years to follow.

To avert ransomware incidents, universities should establish a robust firewall spanning their entire system and ensure its constant updates. Furthermore, maintaining regular backups of crucial data can mitigate the impact of a ransomware assault should it occur. Collaborating with a reputable IT service provider can aid in staying vigilant about cybersecurity maintenance and thwarting potential ransomware attacks.

3. SQL Injections: Many hackers use SQL injections when attacking higher learning institutions. In an SQL injection, the hacker will enter a piece of malicious code into a query box on your website. The most common query boxes are login pages and contact forms, but there are many others. The malicious code enables the hacker to access protected data. They can even alter this data by adding new information or deleting it altogether.

Colleges and universities are often particularly vulnerable to SQL injections because of the number of query boxes on their website. There are ways to prevent SQL injections when designing your website by using parameterized statements. Working with an IT company through the web design process and updating your website to address these security threats can make a huge difference.

5. Identity theft: it is the deliberate use of someone else's identity, usually for a financial gain or to obtain credit and other benefits in the victim's name to the victims‟ disadvantage or loss (Okereafor K, et al, 2020). Numerous instances have arisen where social media accounts are compromised, leading to hackers dispatching messages and malware to all those connected with the account. Often, individuals inadvertently become targets by clicking on links that promise free services, oblivious to the fact that this action could result in their personal information being pilfered.

6. Data Breaches: There are many other types of data breaches that colleges and universities are vulnerable to. For example, there are many different types of malware that hackers have used over the years. As technology evolves, cybercriminals have gotten increasingly sophisticated and developed new strategies to gain access to valuable pieces of data. Human error can also increase the chances of a data breach.

7. **Outdated Technology**: Numerous higher education institutions rely on obsolete technology, thereby increasing their susceptibility to cyber threats. Even the oversight of a single software update can heighten your organization's exposure to risk. Given the perpetual advancement of educational technology, universities should frequently appraise the devices and software applications they employ to ensure their ongoing security. Additionally, it's very important to schedule time for regular software updates. While upgrading to the latest technology can be pricey, think of it as an investment in the safety of your organization, your staff, and your students.

2.9 CYBER SECURITY FRAMEWORK

A cybersecurity management framework is designed to mitigate cybersecurity risks and is becoming an essential component of overall risk management in organizations, including universities. Cybersecurity risks can arise from various sources, including natural events, human errors, third-party contractors, financial disruptions, and security breaches. By implementing a cybersecurity management framework, organizations can proactively identify, assess, and manage cybersecurity risks to protect their critical assets, systems, and data. The framework provides a systematic approach to develop strategies, policies, procedures, and controls to prevent, detect, respond to, and recover from cyber threats.

Universities, like other organizations, hold valuable and sensitive information, such as student and employee data, research data, intellectual property, and financial records. They also rely on digital systems and networks for day-to-day operations and educational activities. This makes them potential targets for cyberattacks and highlights the importance of having a robust cybersecurity management framework in place.

Risk is an unpredictable occurrence of an incident or situation in organizations or universities that has negative impact, such as time, cost, or quality (Mikkola et al., 2020). A risk may have one or more triggers or causes, and if it happens, it may have diverse effects. Every facet of universities' information systems and technical and social environments can face diverse risks which are likely to be caused by poor preparation and management procedures, and lack of centralized management systems (Hollis, 2015). Consequently, risk management (RM) has become an important and integral part of cybersecurity management in organizations over the last few decades (Whitehead, 2020). It encompasses the mechanisms involved in hazard preparation, assessment, interpretation, reactions, and threat management and regulation (Purohit et al., 2018), which is further described as a role that enables and adds value to organizations while increasing the likelihood of achieving strategic

objectives. In the meantime, any organization aspiring for excellence should cultivate robust competencies to manage intricate risks. Modern organizations must establish an enabling environment that mitigates the adverse impacts of risk. The notion that universities should possess cybersecurity frameworks is derived from perspectives advocated within the realm of Risk Management. This is given the relationship between critical aspects of RM and those of cybersecurity frameworks namely, techniques, processes, and resources used to define and manage risks (Aven et al.., 2010). There are several cybersecurity frameworks in use across the world, depending on person or organizational preference and adaptation (Pattinson et al., 2018). The unique characteristics of universities situated in developing countries also give rise to concerns that are not directly covered by current international frameworks. To effectively manage cybersecurity threats, universities must possess a comprehensive comprehension of their sociotechnical environments, operations, catalysts, and security challenges. As the threats, objectives, and processes of each university are distinct, the strategies and methods employed to attain the objectives inherent in cybersecurity frameworks typically diverge.

Consequently, this study encourages Nigerian universities and those in analogous developing country contexts to gain a lucid understanding of their sociotechnical landscapes, operations, motivating factors, and security challenges. To achieve this clarity of purpose, Nigerian universities must respond to the inquiries posed in this study, such as the cybersecurity issues confronting Nigerian universities and the anticipated challenges in the future. They must also ascertain the envisioned objectives of cybersecurity initiatives within Nigerian universities, determine how suitable cybersecurity programs can be devised and executed, establish procedures to assess the relevance and sufficiency of cybersecurity initiatives, and explore avenues to communicate these programs to pertinent stakeholders. Diligently and systematically deriving answers to these queries will lay the foundation for a distinctive cybersecurity framework.

2.9.1 A COMPREHENSIVE CYBERSECURITY MANAGEMENT FRAMEWORK TYPICALLY INCLUDES THE FOLLOWING KEY COMPONENTS:

1. **Risk Assessment**: Identifying and assessing potential cybersecurity risks specific to the organization, including internal and external threats.
2. **Security Policies and Procedures**: Developing and implementing policies, procedures, and guidelines to govern cybersecurity practices, including data protection, access control, incident response, and employee training.

3. **Security Controls**: Implementing technical and organizational measures to safeguard information systems, such as firewalls, intrusion detection systems, encryption, secure configurations, and vulnerability management.

4. **Incident Response and Recovery**: Establishing plans and procedures to detect, respond to, and recover from cybersecurity incidents effectively, including incident reporting, incident handling, and business continuity.

5. **Employee Awareness and Training**: Providing ongoing education and training programs to raise awareness about cybersecurity risks, best practices, and responsibilities among staff, faculty, and students.

6. **Continuous Monitoring and Improvement**: Regularly monitoring and assessing the effectiveness of security controls, conducting security audits and assessments, and making improvements based on lessons learned and emerging threats.

By adopting a cybersecurity management framework, organizations, including universities, can enhance their resilience to cyber threats, protect sensitive data, maintain operational continuity, and build trust among stakeholders.

CHAPTER THREE RESEARCH METHODOLOGY

3.1 INTRODUCTION

This chapter introduces the approach and process utilized in this investigation. It is structured with the subsequent sub-sections:

- Research design
- Sampling and sampling method
- Research instrument
- Validity of the instrument
- Method of data collection and
- Method of data analysis

3.2 RESEARCH DESIGN.

With the use of questionnaires, this study employs a quantitative approach to learn more about people's knowledge, attitudes, and behavior around the impact of Covid-19 pandemic on the educational sector of Nigeria and effectiveness of the e-learning strategy adopted by its various stakeholders and the level of cybersecurity awareness on cyber users. The descriptive approach was used because it facilitates comprehension of the "what" of the research as well as the assessment, description, and evaluation of the issue being studied.

3.3 SAMPLING AND SAMPLING METHOD

This study used probability sampling, where the specific sampling technique used was simple random sampling. A total of 124 valid responses were collected from 22 higher institutes of learning and 5 secondary schools. The descriptive information of participants can be found in figure 4.1

3.4 RESEARCH INSTRUMENT

The research instrument of this study is a customized self-structured questionnaire. Appropriate questions describing the research goals were formulated in the questionnaires to extract relevant information from the respondents. The questionnaire was designed in a close-ended format to accommodate questions such that the essence of the study can be realized. To further enhance this

research, a comparison between the values obtained from this survey was compared with a similar survey carried out on various databases online.

The format of the questionnaire was close-ended and divided into sections A through D. Section A was used to gather sociodemographic data about the respondents, and sections B to D used a 4point Likert scale to gather responses from research participants on their level of the impact of digital technologies on the educational sector, cyber awareness, the precautions they take to prevent cybersecurity incidents and its implications on educational stakeholders and the influence of ongoing governmental initiatives on cybersecurity awareness and education.

3.5 VALIDITY OF THE INSTRUMENT

The survey questionnaire was presented to and approved by the research supervisor, who attested for the survey's content and construct validity as well as its appropriateness and suitability, in order to ensure the authenticity of the validity and reliability of the research instrument for this study. Hence, the instrument is valid, accurate and reliable.

3.6 METHOD OF DATA COLLECTION

Survey questionnaires were delivered to respondents in person and online via emails and WhatsApp groups to collect information from respondents on the implication of cyber awareness and education related to cybersecurity when accessing and using cyberspace. The inclusion of online administration of survey questions allowed the research to cover a broader and more random population sample for the study.

3.7 METHOD OF DATA ANALYSIS

Data collected for this study was analyzed using the SPSS software and the python jupyter notebook respectively. Question and/or statement items used in assessing respondents when answering a particular research question were ranked on a Likert scale as follows:

Table 3.1: Likert scale rank

Scale	**Score(x)**
Not aware	0
Slightly aware	1
Very aware	2
Extremely aware	3
Mean mark	**1.5**

Scale	**Score(x)**
Strongly disagree	1
Disagree	2
Agree	3
Strongly agree	4
Mean mark	**2.5**

CHAPTER FOUR

DATA PRESENTATION AND ANALYSIS

4.1 INTRODUCTION

This chapter deals with the presentation of quantitative data collected for this research. It also analyses the results and research findings elicited from the respondents of this study as obtained through the questionnaire which was the primary instrument of research and datasets were gotten from various database such as kaggle.com, etc. Finally, findings from quantitative data collected are discussed.

4.2 DATA PRESENTATION

This research work was embarked to assess the level of cyber awareness and education of Nigerians. To facilitate this assessment, survey questions were distributed and administered to a target population of 100 respondents. However, a total of 87 responses were recovered from both distributed questionnaires and online responses. Therefore, the data presentation of the research is based on the number of submitted responses which were analyzed as explained below.

For clarity and understanding, data gathered is presented in a tabular form in frequencies and percentages.

Table 4.1: gender distribution of respondents

	Frequency	**Percentage**
Male	63	50.8
Female	61	49.2
Total	**124**	**100.0**

Table 4.1 shows the gender distribution of study respondents. The data gathered reveals that 63 respondents representing 50.8% were males while 61 representing 49.2% were females. Generally, more females participated in the survey compared to their female counterparts.

Table 4.2: age distribution of respondents

	Frequency	Percentage
16 – 20	34	27.4
21 – 25	32	25.8
26 – 30	22	17.7
31 – 35	23	18.5
41 – above	13	10.5
Total	**124**	**100.0**

Table 4.2 shows the age distribution of respondents used for his study. Data collected showed that ages 16 – 20yrs were 34 in number representing 27.4%; 21 – 25yrs were 32 representing 25.8%; 26 – 30yrs were 22 representing 17.7%; 31 – 35yrs were 23 in all representing 18.5%; and 41yrs – above were 13 representing 10.5%.

Table 4.3: educational level of respondents

	Frequency	Percentage
Post - graduate	30	24.2
Secondary	20	16.1
Tertiary	66	53.2
Others	7	5.6
None	1	0.8
Total	**124**	**100.0**

Table 4.3 shows the educational level of respondents. Data gathered reveals that most respondents had tertiary education (OND and higher) and were a total of 66 representing 53.2% of the study population. Those with post - graduate education were 30 representing 24.2%; secondary level had 20 representing 16.1% while 7 (5.6%) represents other levels.

Table 4.4: designation status of respondents

	Frequency	Percentage
Educators	23	18.5
Educators, Students	6	4.8
Others	28	22.6
Student	67	54.0
Total	**124**	**100.0**

Source: Primary (Questionnaire). Feb, 2023

Table 4.4 shows the designation status of study respondents. Collected data showed that 67 respondents representing 54.0% were students only; 23 representing 18.5% were educators; and 6 representing 4.8% of the respondents indicated that they were both students and educators, while 28 respondents (22.6%) indicated they were neither students nor educators.

Fig 4.5

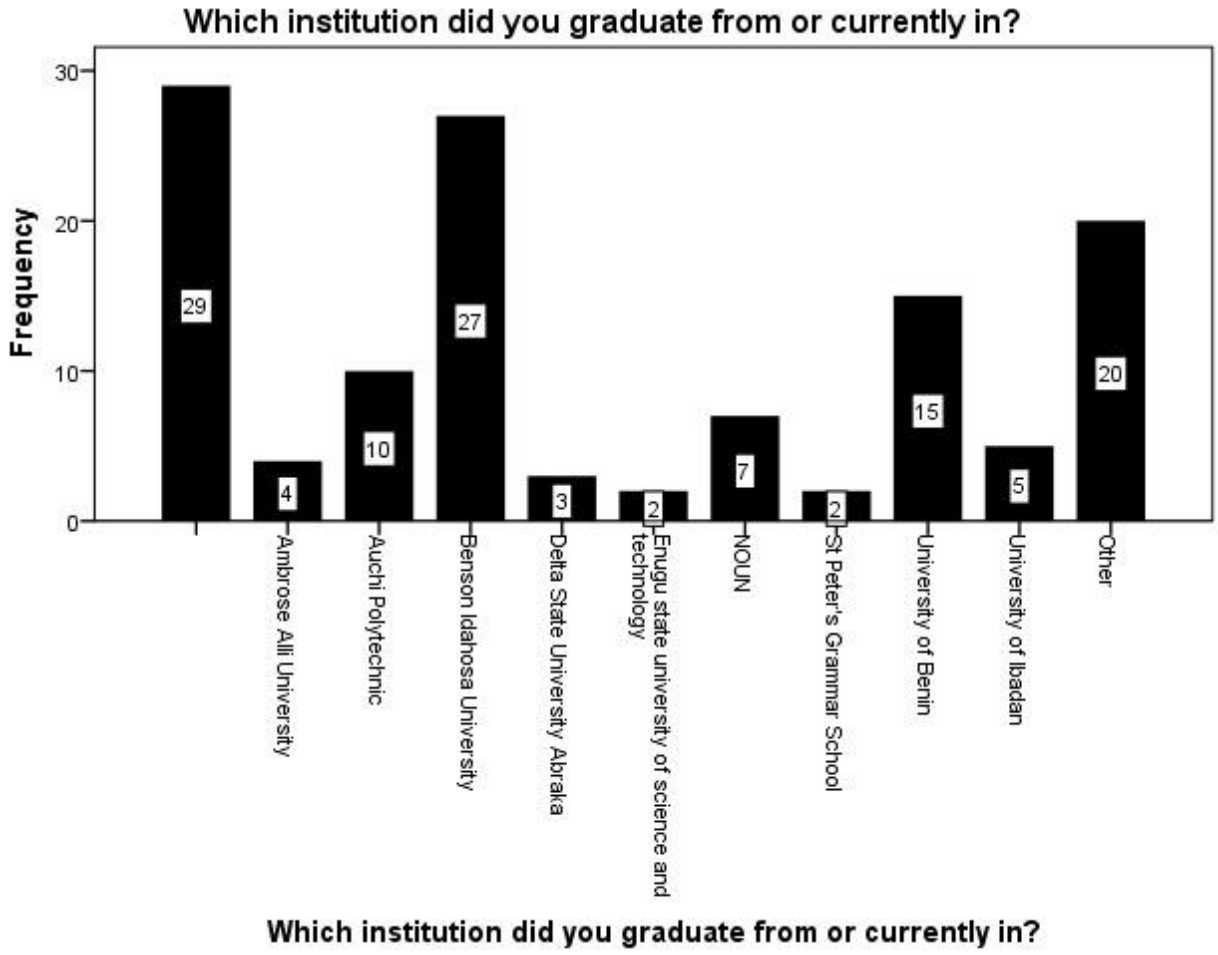

Which institution did you graduate from or currently in?
Frequency
30
20
10
0
29
4
10
27
3
2
7
2
15
5
20
Ambrose Alli University
Auchi Polytechnic
Benson Idahosa University
Delta State University Abraka
Enugu state university of science and technology
NOUN
St Peter's Grammar School
University of Benin
University of Ibadan
Other
Which institution did you graduate from or currently in?

Fig 4.2:

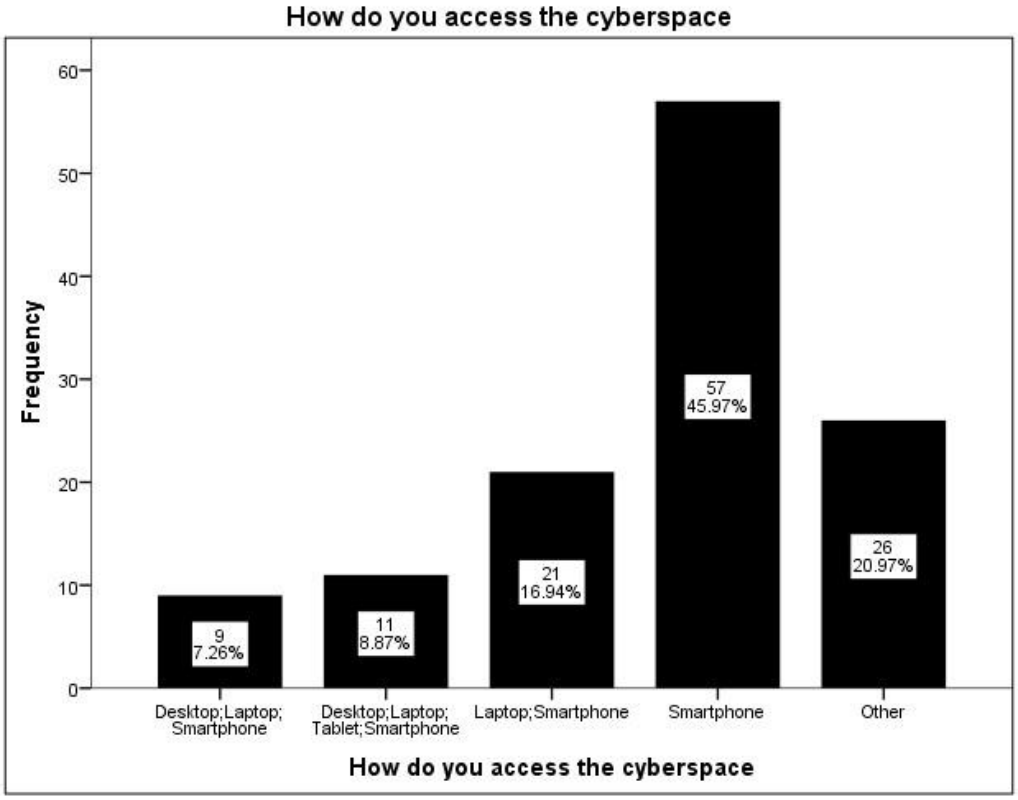

How do you access the cyberspace
Frequency
60
50
40
30
20
10
0
9
7.26%
11
8.87%
21
16.94%
57
45.97%
26
20.97%
Desktop;Laptop; Smartphone
Desktop;Laptop; Tablet;Smartphone
Laptop;Smartphone
Smartphone
Other
How do you access the cyberspace

Fig 4.5

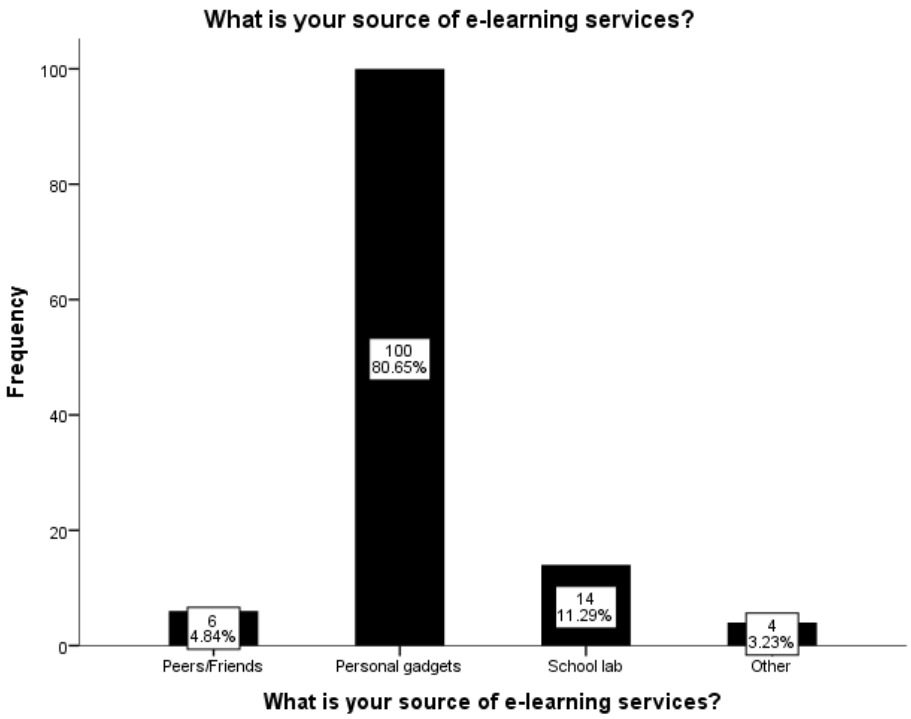

What is your source of e-learning services?
Frequency
100
80
60
40
20
0
6
4.84%
100
80.65%
14
11.29%
4
3.23%
Peers/Friends
Personal gadgets
School lab
Other
What is your source of e-learning services?

Fig 4.4:

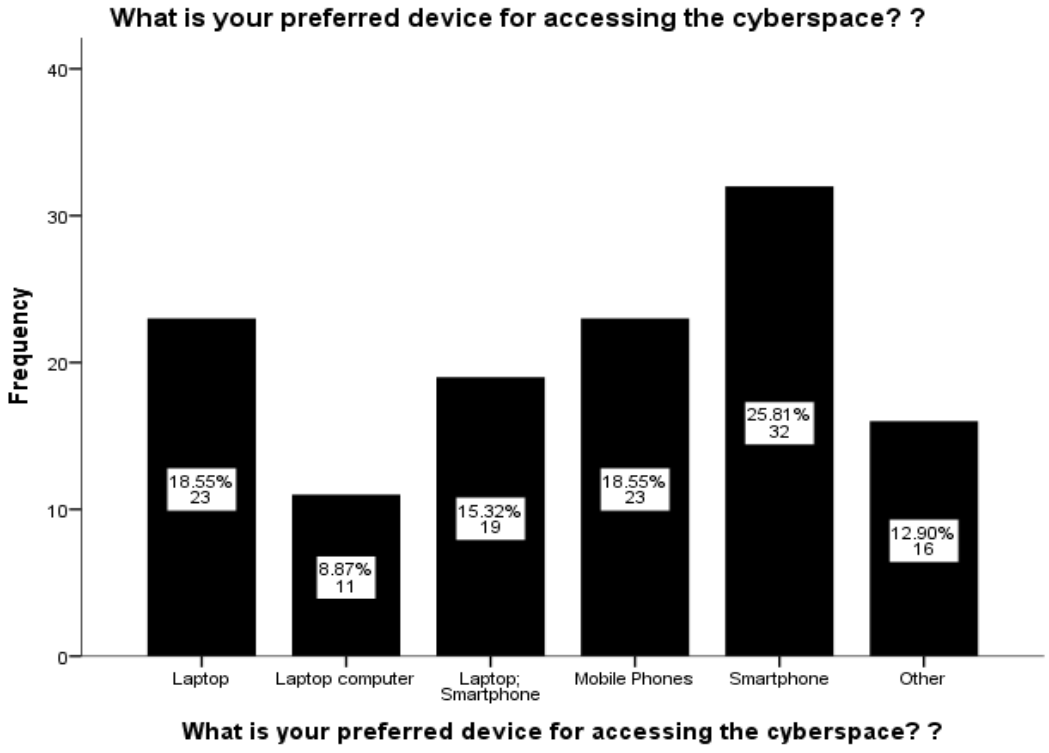

What is your preferred device for accessing the cyberspace? ?
Frequency
40
30
20
10
0
18.55%
23
8.87%
11
15.32%
19
18.55%
23
25.81%
32
12.90%
16
Laptop
Laptop computer
Laptop; Smartphone
Mobile Phones
Smartphone
Other
What is your preferred device for accessing the cyberspace? ?

Fig 4.5

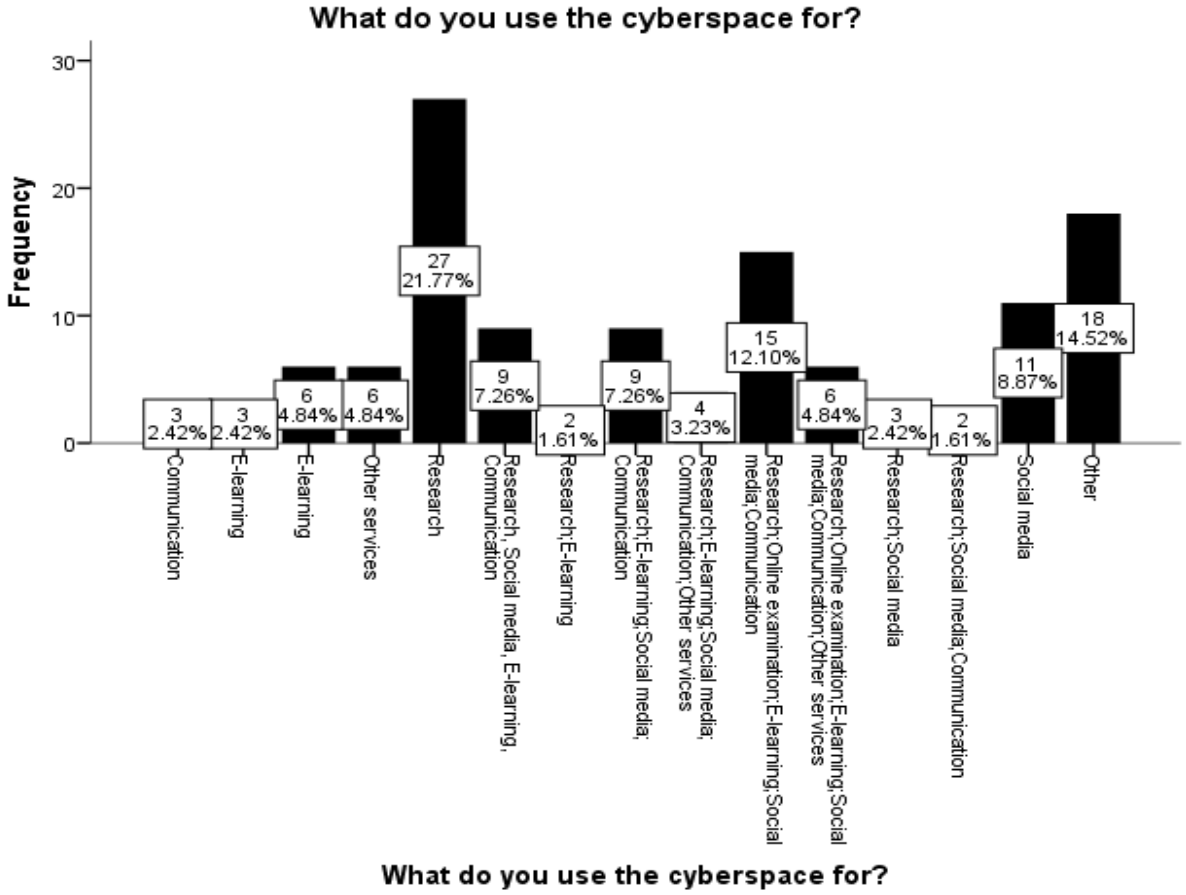

What do you use the cyberspace for?
Frequency
30
20
10
0
3
2.42%
3
2.42%
6
4.84%
6
4.84%
27
21.77%
9
7.26%
2
1.61%
9
7.26%
4
3.23%
15
12.10%
6
4.84%
3
2.42%
2
1.61%
11
8.87%
18
14.52%
Communication
E-learning
E-learning
Other services
Research
Research, Social media, E-learning, Communication
Research;E-learning
Research;E-learning;Social media; Communication
Research;E-learning;Social media; Communication;Other services
Research;Online examination;E-learning;Social media;Communication
Research;Online examination;E-learning;Social media;Communication;Other services
Research;Social media
Research;Social media;Communication
Social media
Other
What do you use the cyberspace for?

Fig 4.6:

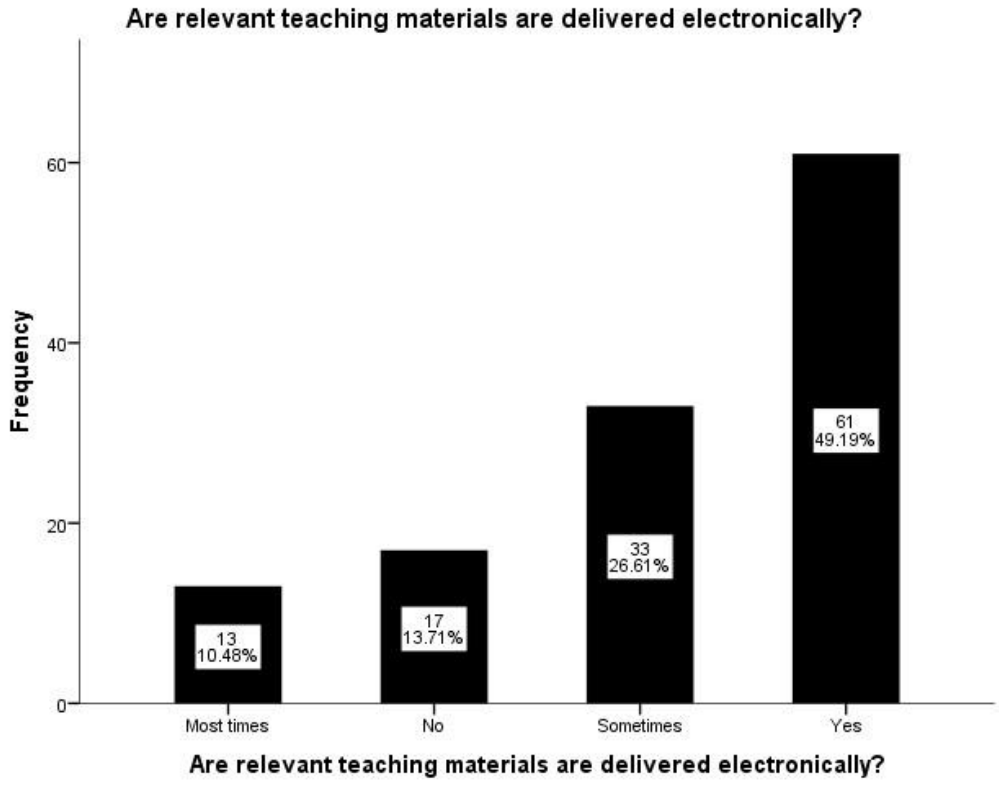

Are relevant teaching materials are delivered electronically?
Frequency
60
40
20
0
13
10.48%
17
13.71%
33
26.61%
61
49.19%
Most times
No
Sometimes
Yes
Are relevant teaching materials are delivered electronically?

Fig 4.7:

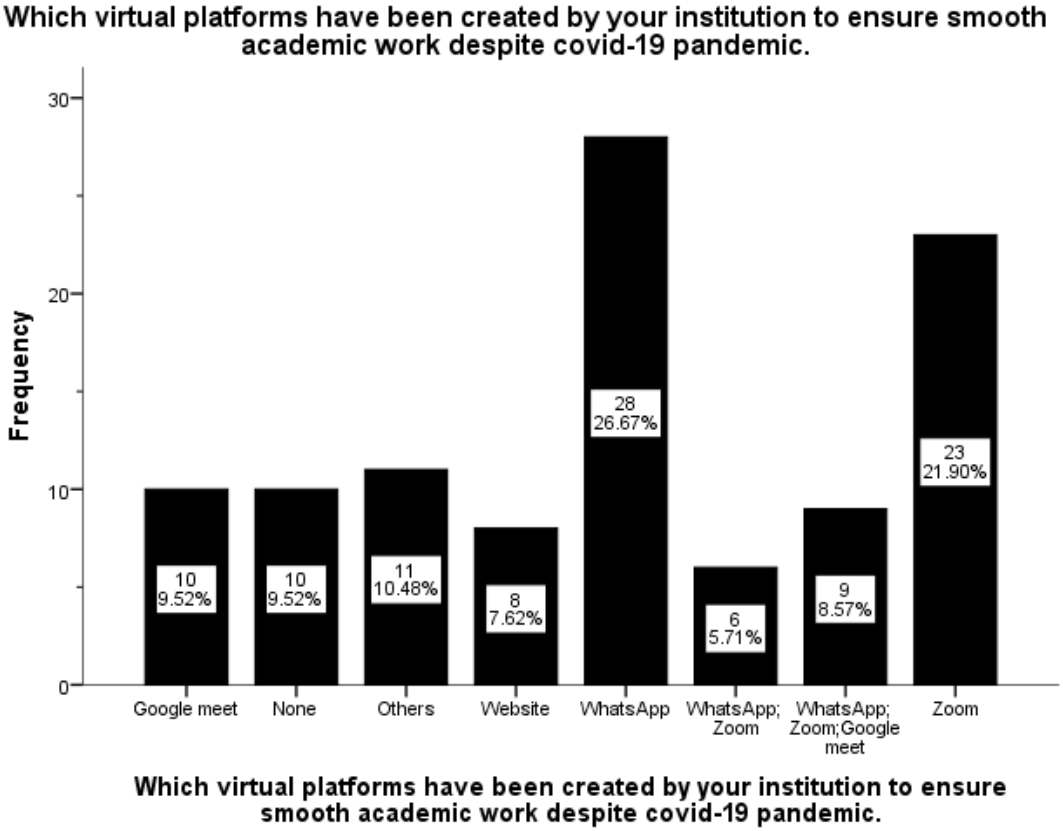

Which virtual platforms have been created by your institution to ensure smooth academic work despite covid-19 pandemic.
Frequency
30
20
10
0
10
9.52%
10
9.52%
11
10.48%
8
7.62%
28
26.67%
6
5.71%
9
8.57%
23
21.90%
Google meet
None
Others
Website
WhatsApp
WhatsApp; Zoom
WhatsApp; Zoom;Google meet
Zoom
Which virtual platforms have been created by your institution to ensure smooth academic work despite covid-19 pandemic.

Fig 4.8:

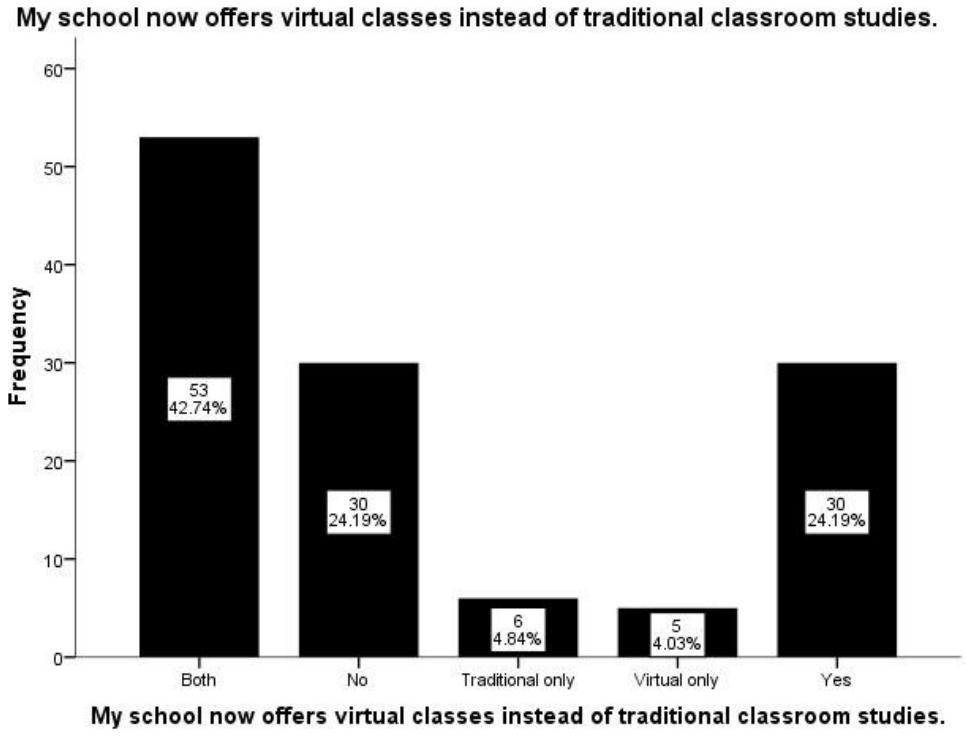

My school now offers virtual classes instead of traditional classroom studies.
Frequency
60
50
40
30
20
10
0
53
42.74%
30
24.19%
6
4.84%
5
4.03%
30
24.19%
Both
No
Traditional only
Virtual only
Yes
My school now offers virtual classes instead of traditional classroom studies.

Table 4.5: Awareness of Cybercrime

Question Item	Extremely aware (EA)	Very aware (VA)	Slightly aware (SA)	Not aware (NA)	Mean Score	Standard deviation
To what extent are you aware of the cybercrime?	24 (19.4%)	60 (48.4%)	39 (31.5%)	1 (0.8%)	1.863	0.7251
To what extent are you aware about phishing?	11 (8.9%)	22 (17.7%)	47 (37.9%)	44 (35.5%)	1.000	0.9457
To what extent are you aware about cyberbullying?	25 (20.2%)	44 (35.5%)	34 (27.4%)	21 (16.9%)	1.589	0.9960
To what extent are you aware of anti-malware or antivirus?	23 (18.5%)	51 (41.1%)	4 (7.3%)	19 (15.3)	1.629	0.9582
To what extent are you aware about identity theft?	25 (20.2%)	48 (38.7%)	34 (27.4%)	17 (13.7%)	1.653	0.9546
To what extent are you aware that you are a likely cybercrime target?	17 (13.7%)	44 (35.5%)	40 (32.3%)	23 (18.5%)	1.444	0.9483

Source: Questionnaire, 2023. Frequencies (percentages) of responses are shown in the table

Table 4.5 shows respondents' awareness of cybercrime. Data depicts majority of the respondents to be very aware of cybercrime (48.4%), cyber bullying (35.5%), malware/viruses (41.1) %, and identity theft (38.7%) and that they are likely cybercrime targets (35.5%) and slightly aware about phishing (37.9%). Respondents generally showed a poor awareness particularly on phishing.

Table 4.6: Awareness of Cybersecurity

Question Item	Extremely aware (EA)	Very aware (VA)	Slightly aware (SA)	Not aware (NA)	Mean Score	Standard deviation
To what extent are you aware of the importance of cybersecurity?	30 (24.2%)	50 (40.3%)	37 (29.8%)	7 (5.6%)	1.831	0.8622
To what extent are you aware of the risks with using the cyberspace?	26 (21.0%)	48 (38.7%)	33 (26.6%)	17 (13.7%)	1.669	0.9604
To what extent are you aware of system security updates?	23 (18.5%)	43 (34.7%)	47 (37.9%)	11 (8.9%)	1.629	0.8877
To what extent are you aware of anti-malware or antivirus?	30 (24.2%)	43 (34.7%)	37 (29.8%)	14 (11.3%)	1.718	0.9590
To what extent are you aware of the use of a VPN?	23 (18.5%)	37 (29.8%)	41 (33.1%)	23 (18.5%)	1.484	0.9999

Source: Questionnaire, 2023. Frequencies (percentages) of responses are shown in the table

Table 4.6 shows the levels of awareness of study respondents on cybersecurity. Across all items used to assess respondents' awareness, most of the respondents were very aware of the importance of cybersecurity (40.3%), awareness of being risky online (38.7%), awareness of antimalware/antivirus (34.7%). Respondents representing (37.9%) are slightly aware of system security update, and (33.1%) respondent's shows slight awareness about VPN.

Table 4.7: Measures Taken by Nigerian Cyber-users to Forestall Cybersecurity Incidents

Statement Item	Strongly agree (SA)	Agree (A)	Disagree (D)	Strongly disagree (SD)	Mean score	Standard deviation
I always perform security updates whenever I see them	7 (5.6%)	73 (58.9%)	27 (21.8%)	17 (13.7%)	2.806	0.7400
I always perform anti-virus updates whenever I see them	15 (12.1%)	68 (54.8%)	35 (28.2%)	6 (4.8%)	2.742	0.7311
Changing passwords regularly is necessary	21 (16.9%)	53 (42.7%)	42 (33.9%)	8 (6.4%)	2.702	0.8262
Cyber awareness and education will improve my cybersecurity	51 (41.1%)	67 (54.0%)	3 (2.4%)	3 (2.4%)	3.339	0.6488
I download free files from the cyberspace no matter the source	8 (6.5%)	33 (26.6%)	69 (55.6%)	14 (11.3%)	2.282	0.7496
I always use a free Wi-Fi connection when I notice one	10 (8.1%)	43 (34.7%)	52 (41.9%)	19 (15.3%)	2.355	0.8381

Table 4.7 shows behavioral measures taken by Nigerian cyber-users to forestall cybersecurity incidents. Data reveals that a higher percentage of study respondents agreed that they always perform security updates whenever they see them (58.9%), 68(54.8%) agreed also they always perform anti-virus update, (42.7%) also agreed they change passwords regularly, 67(54.0%) of respondents agreed that cyber awareness will improve the cybersecurity culture, however, 69(55.6%) disagreed that they download files from any source, and 52 respondents (41.9%) disagree that they always use free Wi- Fi.

Table 4.8: Impact of Cybersecurity Awareness and Education Initiatives

Statement Item	Strongly agree (SA)	Agree (A)	Disagree (D)	Strongly disagree (SD)	Mean score	Standard deviation
Certainly, the Covid-19 pandemic has triggered a noticeable improvement within my educational institution.	11 (8.9%)	63 (50.8%)	36 (29.0%)	14 (11.3%)	2.573	0.8082
I am of the opinion that the incorporation of e-learning will amplify the utilization of digital devices within the campus environment.	25 (20.2%)	88 (71.0%)	8 (6.5%)	3 (2.4%)	3.089	0.5983
My educational institution is providing students with a comprehensive introduction to elearning solutions and platforms.	14 (11.3%)	76 (61.3%)	23 (18.5%)	11 (8.9%)	2.750	0.7717
The National Cybersecurity Policy and Strategy on cyber awareness and education has been effective	10 (8.1%)	56 (45.2%)	48 (38.7%)	10 (8.0%)	2.532	0.7591
Overall, the government has performed well with its cybersecurity awareness and education initiatives	6 (4.8%)	39 (31.5%)	67 (54.0%)	12 (9.7%)	2.315	0.7142
The expansion of internet usage and engagement has increased significantly within my university.	18 (14.5%)	87 (70.2%)	8 (6.5%)	11 (8.9%)	2.903	0.7481
The Covid-19 pandemic has introduced the concept of ELearning to my academic journey, which is entirely new for me.	9 (7.3%)	64 (51.6%)	40 (32.3%)	11 (8.9%)	2.573	0.7563

Table 4.8 shows Impact of Cybersecurity Awareness and Education Initiatives. Data reveals that a higher percentage of study respondents agreed that introduction of e-learning as a result of the covid-19 pandemic has had a significant progress in the academic institutions (50.8%), 88(71.0%) agreed also e-learning will foster educational technologies in the academic sector, (61.3%) also agreed are receiving orientation on e-learning solutions, 56(45.2%) of respondents agreed that the NCPS cybersecurity awareness initiative have been effective, 87(70.2%) agreed also that internet patronage has intensified in their school, and (51.6%) agreed that e-learning is a new experience for them, however 67 respondents (54.0%) disagree that the government effort towards cybersecurity has being effective.

4.3 MODEL TRAINING

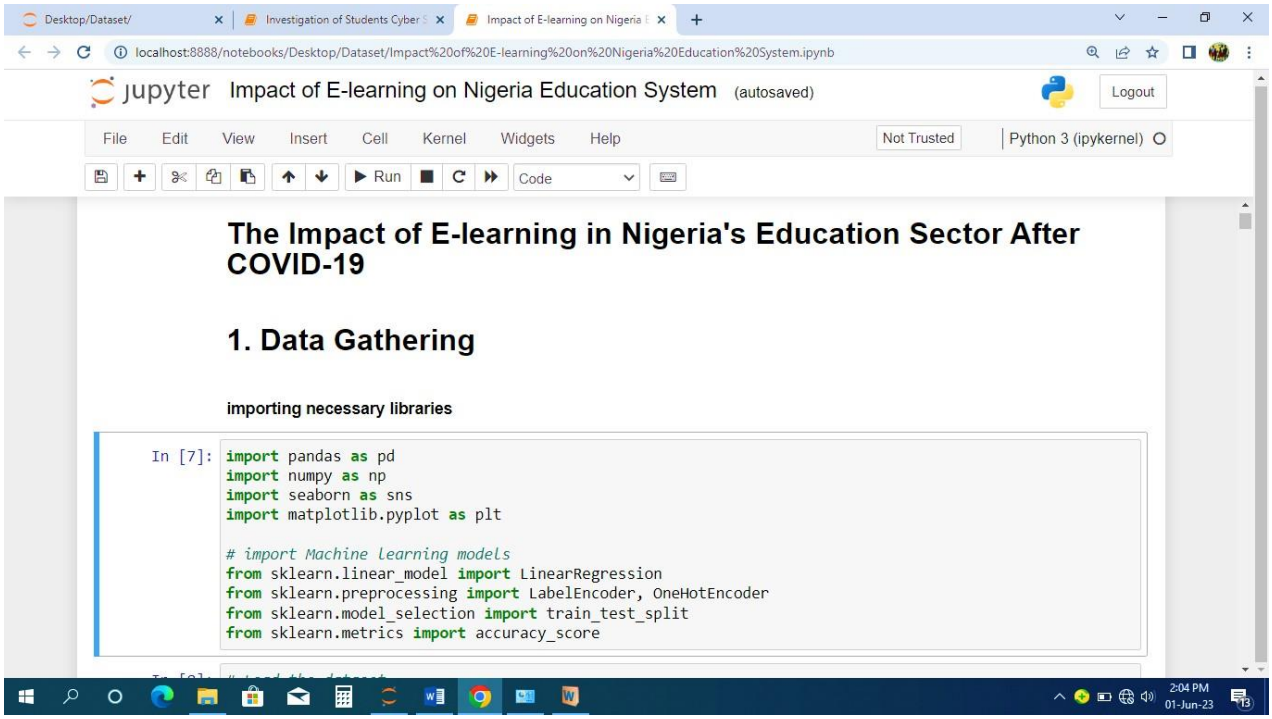
To further assess the impact of e- learning on the educational system, dataset was gotten online from kaggle database and this dataset was trained using both linear and logistic regression model to predict the performance of students and to also study the factors that can influence the performance of the users.

4.3.1 RESULT INTERPRETATION FOR LOGISTIC REGRESSION USING ONLINE SATISFACTION AS DEPENDENT VARIABLE

Data Preprocessing:

Before performing the logistic regression, the dataset was preprocessed by encoding the categorical variables using one-hot encoding. This was done to convert the categorical variables into numerical variables that can be used by the logistic regression model. The data was also checked for missing values and outliers.

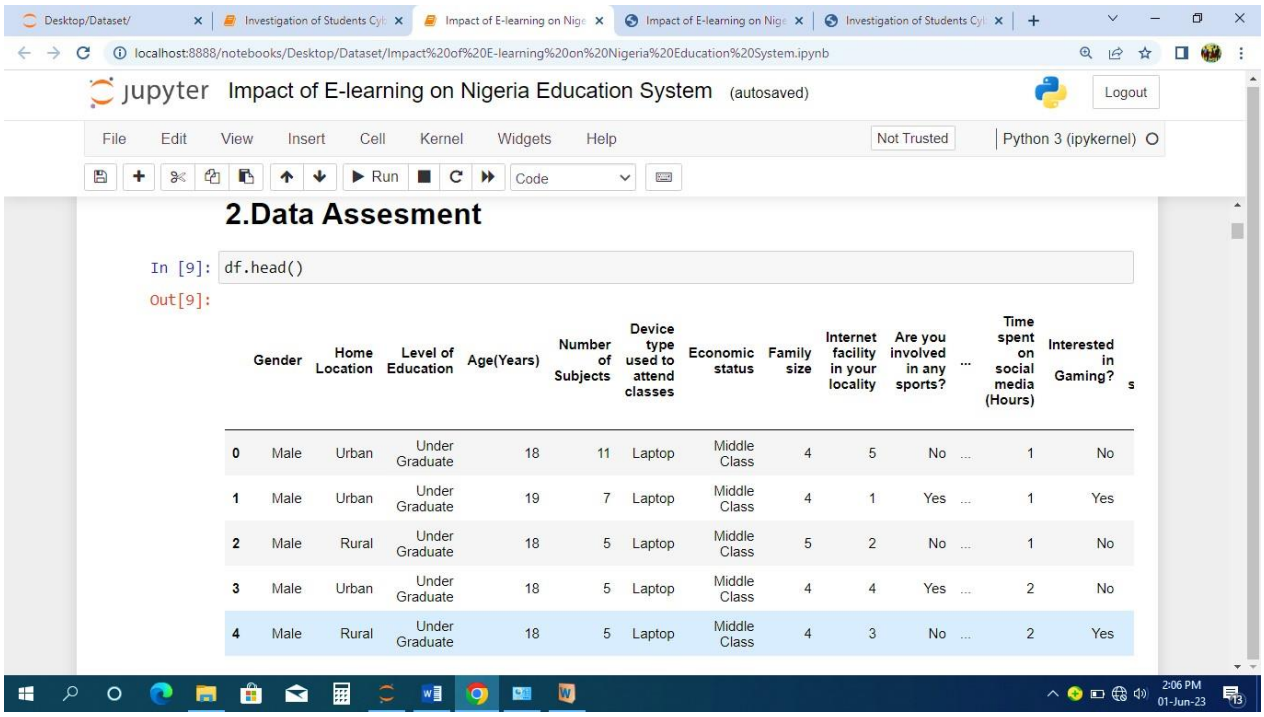
Fig 4.9:



Based on the provided dataset and problem statement, logistic regression analysis was used to examine the impact of e-learning on the online satisfaction of students in Nigeria's education sector after COVID-19. The independent variables included 'Gender', 'Home Location', 'Level of Education', 'Age', 'Subjects', 'Device_Type', 'Income', 'Family size', 'Internet_Availability',

'Sports_Involvement', 'Elderly_Monitoring', 'Study_Time', 'Sleep_Time', 'Social_Media_Time', 'Gaming_Interest', 'Separate_Study_Room', 'Group_Study_Involvement', 'Pre_Pandemic_Marks', 'Online_Interaction', 'Online_Doubt_Clearance', and 'Interest_In_Learning', while the dependent variable was 'Online_Satisfaction'.

Fig 4.10:



	Gender	Home Location	Level of Education	Age(Years)	Number of Subjects	Device type used to attend classes	Economic status	Family size	Internet facility in your locality	Are you involved in any sports?	...	Time spent on social media (Hours)	Interested in Gaming?	s
0	Male	Urban	Under Graduate	18	11	Laptop	Middle Class	4	5	No	...	1	No	
1	Male	Urban	Under Graduate	19	7	Laptop	Middle Class	4	1	Yes	...	1	Yes	
2	Male	Rural	Under Graduate	18	5	Laptop	Middle Class	5	2	No	...	1	No	
3	Male	Urban	Under Graduate	18	5	Laptop	Middle Class	4	4	Yes	...	2	No	
4	Male	Rural	Under Graduate	18	5	Laptop	Middle Class	4	3	No	...	2	Yes	

The evaluation of the logistic regression model produced the following confusion matrix:

[[88 8 5] [19 27 1] [35 0 24]]

The confusion matrix revealed that the model correctly predicted 88 students who were very satisfied with their e-learning experience, 27 students who were satisfied and 24 students who were not satisfied. However, the model misclassified some of the students, predicting that 19 students were very satisfied when they were satisfied, 8 students who were satisfied when they were very satisfied, 5 students who were not satisfied when they were very satisfied, and 1 student who was very satisfied when they were not satisfied.

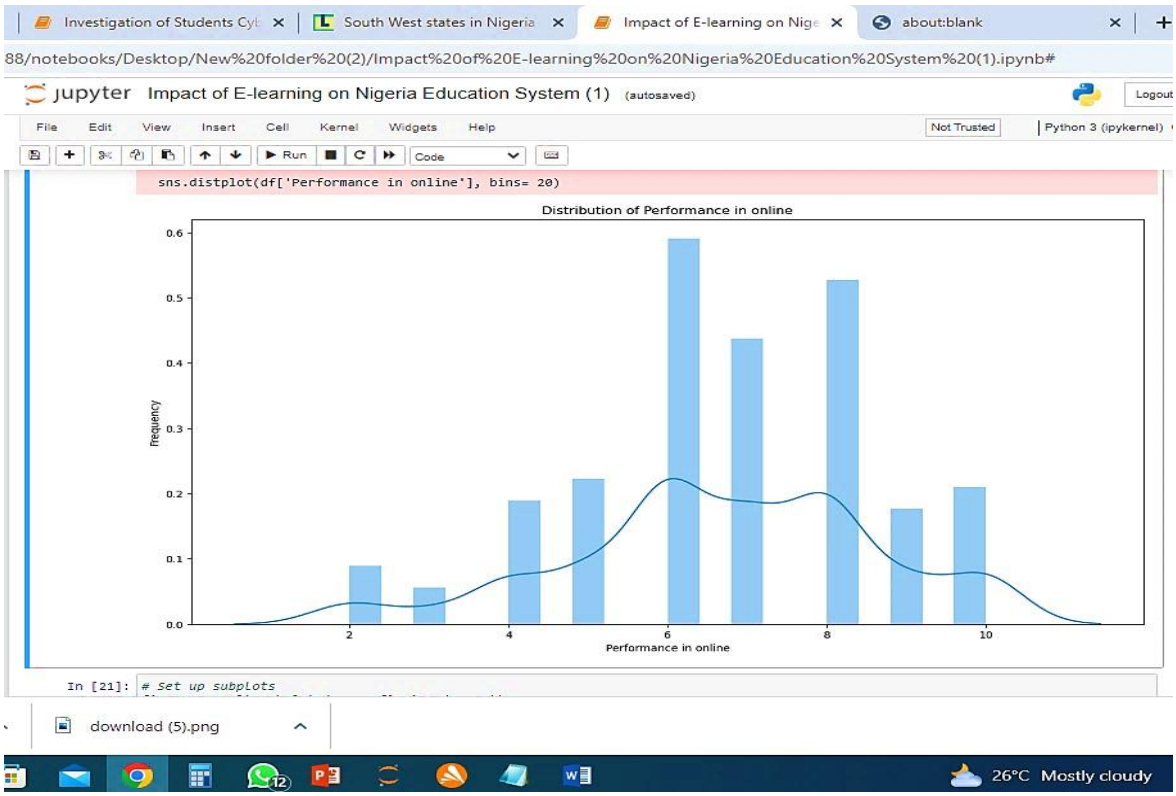
Classification Report:

	precision	recall	f1-score	support
0	0.62	0.86	0.72	101
1	0.75	0.57	0.65	47
2	0.80	0.41	0.54	59
accuracy			0.67	207
macro avg	0.72	0.61	0.64	207
weighted avg	0.70	0.67	0.65	207

4.3.2 RESULT INTERPRETATION FOR LINEAR REGRESSION USING PERFORMANCE IN ONLINE AS DEPENDENT VARIABLE

Linear Regression analysis was used to determine the relationship between Performance in online (dependent variable) and the other independent variables.

Fig 4.11:



Result Interpretation: The evaluation of the linear regression model using the Mean squared error (MSE), Root Mean Squared Error (RMSE), Mean Absolute Error (MAE), R-Squared (R2) Score, and Adjusted R-Squared Score produced the following values: Mean squared error: 2.576971569228601

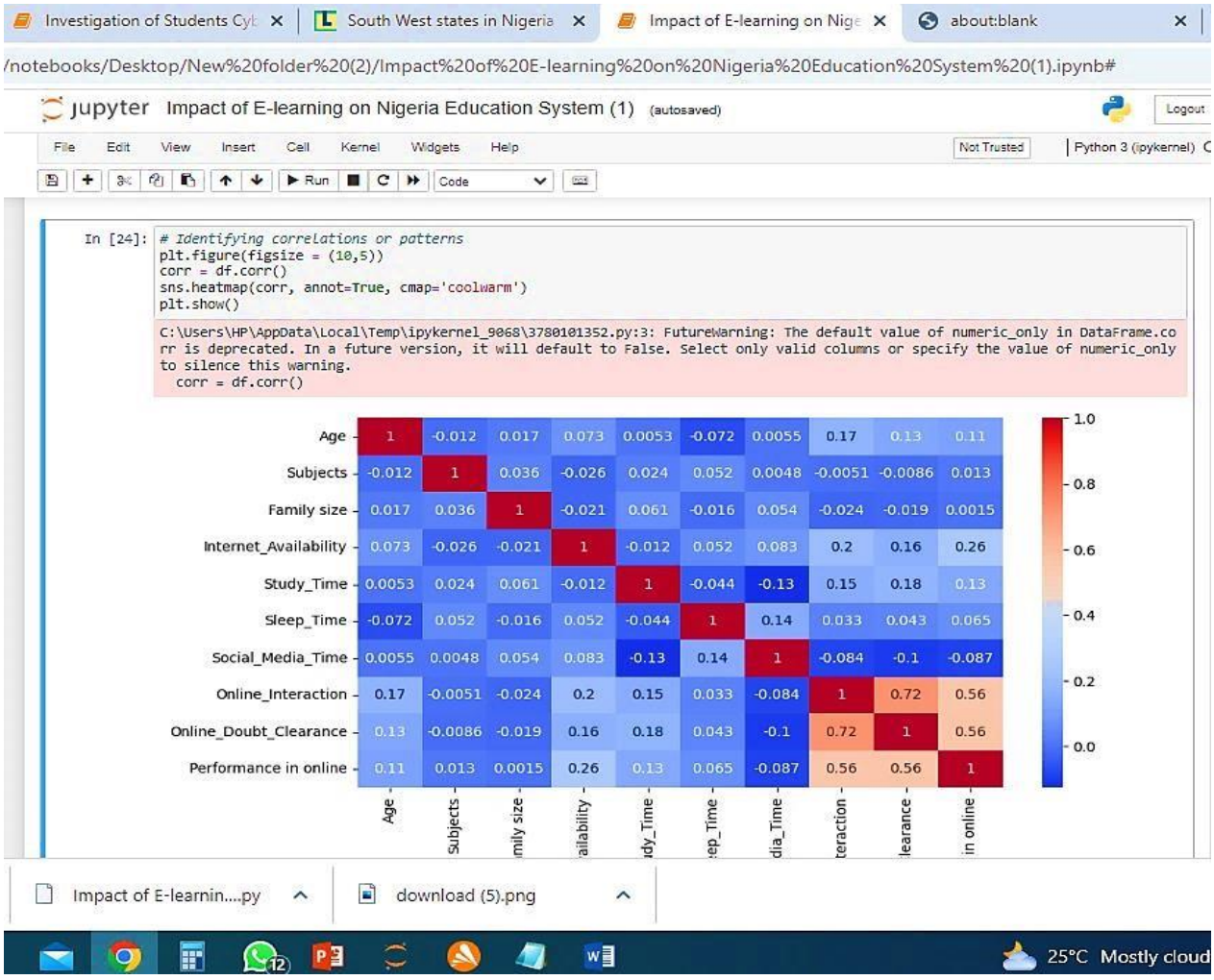
Root Mean Squared Error: 1.6052948542958085

Mean Absolute Error: 1.2501027100349797

R-Squared (R2) Score: 0.33865590923866007

Adjusted R-Squared Score: 0.26754364141486

Fig 4.12:



The Root Mean Squared Error (RMSE) of 1.605 suggests that, on average, the model's predictions have an error of 1.60 when estimating the Performance in online variable. The Mean Absolute Error (MAE) value of 1.25 indicates that the model's predictions are, on average, off by 1.25 units.

The R-Squared (R2) Score of 0.339 suggests that the model can explain approximately 33.86% of the variability in the dependent variable (Performance in online). This means that around 33.86% of the changes in the Performance in online variable can be attributed to the model's predictors.

However, the Adjusted R-Squared Score of 0.268 indicates that the model's goodness of fit is relatively low. The Adjusted R-Squared takes into account the number of predictors in the model and penalizes excessive complexity. A lower Adjusted R-Squared suggests that the model may not be the best fit for the dataset.

In summary, the model has some level of predictive ability with a moderate level of error (RMSE and MAE), but it can only explain a portion of the variability in the Performance in online variable (R2). The low Adjusted R-Squared suggests that the model's fit could be improved, indicating the need for further analysis or alternative modeling approaches.

Considering the statement problem, this analysis provides insights into the impact of e-learning on the online satisfaction of students in Nigeria's education sector after COVID-19. It shows that students who are very satisfied with their e-learning experience tend to have a higher likelihood of being accurately predicted by the model. It also shows that the level of satisfaction, performance online and level of awareness is affected by various independent variables, such as e-learning platforms, online interaction, and privacy concern. This information can be used by educational institutions and policymakers to improve the e-learning experience and increase student satisfaction.

4.4 DISCUSSION OF FINDINGS

This study aim to provide valuable insights and recommendations that can inform policymakers, educators, and stakeholders in Nigeria about the implications of disruptive technologies and cybersecurity in the educational sector. It seeks to contribute to the development of strategies that ensure a secure, resilient, and inclusive learning environment, taking into account the unique challenges and opportunities in the post-pandemic era.

The logistic regression model provides a fair accuracy in predicting the online satisfaction level of students in Nigeria's education sector after COVID-19. However, there is room for improvement in

the prediction of students who are satisfied and not satisfied. This could be achieved by identifying more relevant independent variables that affect students' online satisfaction and/or using a more complex machine learning algorithm.

The classification report showed that the model has an accuracy of 0.67, which indicates that 67% of the time the model was able to correctly predict the online satisfaction level of students. The precision values for the different levels of satisfaction were 0.62, 0.75, and 0.80 for very satisfied, satisfied, and not satisfied, respectively. The recall values for the different levels of satisfaction were 0.87, 0.57, and 0.41 for very satisfied, satisfied, and not satisfied, respectively. The f1-score values were 0.72, 0.66, and 0.54 for very satisfied, satisfied, and not satisfied, respectively.

The linear regression analysis showed that there is a relationship between Performance in online and the independent variables. However, the model performance could be improved. There may be other factors or variables that were not included in the data set, which could have a significant impact on the performance in online. It is recommended that further analysis be conducted to determine the possible missing variables and refine the model.

Online Doubt Clearance refers to the process of providing support and resolving doubts or questions that arise in an online learning environment. In the context of education, especially in online courses or remote learning settings, students may have questions or need clarification on various topics or concepts covered in their coursework. Online doubt clearance aim to address these queries and provide necessary guidance to help students understand and overcome their challenges.

Online Interaction refers to the communication and engagement that takes place between individuals or groups in a virtual or online environment. It involves the exchange of information, ideas, and experiences through various digital platforms and tools. Online interaction plays a significant role in connecting people, fostering collaboration, and facilitating learning and socialization in virtual settings.

Online doubt clearance and online interaction can take various forms depending on the platform or system used for instruction. Some common methods include:

1. **Discussion Forums**: Online platforms often provide discussion forums where students can post their questions or doubts. Instructors, teaching assistants, or fellow students can then respond and provide explanations or solutions.

2. **Live Chat or Messaging**: Real-time communication tools like live chat or messaging systems allow students to ask questions directly to instructors or teaching assistants. This method enables prompt responses and clarifications.

3. **Video Conferencing**: Virtual classrooms or video conferencing tools can be used to conduct live sessions where students can ask questions and receive immediate responses from the instructor or participate in group discussions.

4. **Email or Online Support Tickets**: Students can send their queries or doubts via email or through an online support ticket system. Instructors or support staff can then respond to these queries individually.

5. **Online Office Hours:** Instructors may set aside specific hours during which students can connect with them through video conferencing or other communication channels to seek clarification on course content.

6. **Social Media Platforms:** Social media platforms provide avenues for online interaction, enabling users to connect, share content, and engage in discussions through comments, likes, shares, and direct messages. These platforms offer a more informal and social environment for interaction.

7. **Collaborative Tools**: Online collaboration tools, such as shared documents, project management platforms, or virtual whiteboards, allow individuals or groups to work together on shared tasks or projects. They facilitate interaction by providing a centralized space for communication, file sharing, and real-time collaboration.

8. **Online Learning Platforms**: In educational settings, online learning platforms often incorporate interactive features such as discussion boards, chat rooms, or virtual classrooms. These features facilitate interaction between instructors and students, as well as among students themselves, promoting engagement and knowledge sharing.

The effectiveness of online doubt clearance depends on the responsiveness and availability of instructors or support staff, as well as the ease of access and usability of the communication platforms. Prompt and accurate responses to students' doubts can enhance their learning experience and help them progress in their studies.

Overall, online interaction serves as a vital means of communication and engagement in virtual environments, enabling collaboration, knowledge sharing, and socialization across various contexts.

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 SUMMARY

The research study aim to assess the impact of disruptive technologies and cyber security on the educational sector in Nigeria, specifically in the context of the post COVID-19 pandemic. The study focuses on understanding the challenges, opportunities, and implications of disruptive technologies and cyber security in Nigerian educational institutions.

The research methodology employed involves a comprehensive assessment of the current state of the educational sector in Nigeria, considering the effects of the COVID-19 pandemic on the adoption of technology in education. The study explores the various disruptive technologies that have emerged and their influence on teaching, learning, administration, and infrastructure in Nigerian schools.

Additionally, the research investigates the cyber security implications associated with the adoption of these disruptive technologies in the educational sector. It examines the vulnerabilities, risks, and threats that educational institutions in Nigeria may encounter in their digital transformation journey. The assessment covers areas such as data privacy, network security, protection against cyberattacks, and the role of policies and regulations in ensuring a secure educational environment. The findings of the study also provides insights into the current landscape of disruptive technologies and cyber security in the Nigerian educational sector. It highlights the challenges faced by educational institutions in adopting and integrating these technologies, as well as the potential benefits they offer. The research also identifies strategies and best practices for enhancing cyber security measures to mitigate risks and protect sensitive information.

The linear regression analysis showed that there is a relationship between Performance in online and the independent variables. However, the model performance could be improved. There may be other factors or variables that were not included in the data set, which could have a significant impact on the performance in online. It is recommended that further analysis be conducted to determine the possible missing variables and refine the model.

5.2 CONCLUSION

Emerging technologies hold the potential to integrate fresh methodologies into the educational landscape, fostering learning. The COVID-19 pandemic has prompted the adoption of online teaching and learning systems as an alternative to traditional face-to-face instruction in Nigerian schools. A structured questionnaire employing a five-point Likert scale was employed to assess the effectiveness of this online teaching/learning approach within a selected group of schools. The implementation of online teaching/learning proved to be a significant remedy for the disruption caused by the pandemic, ensuring uninterrupted educational progress and practical skill enhancement. The adoption of online teaching/learning systems is essential for the continual academic flow and establishment of a stable educational framework in Nigeria. In order to reduce the number of cyber threats and risks encountered using the cyberspace, awareness and education remain the starting point. Nigeria is rated as one of the countries with the highest levels of e-crime activities (Yakubu, 2017) as no one is immune to cyber threats thus, cyber users will always be prone and vulnerable to cyber-attacks. Nevertheless, raising awareness and providing education can substantially decrease the potential number of victims. When awareness is promoted, cyber users are educated of how risks occur. The more the awareness, the less likely the risks occur. Cyber awareness and education broadens the knowledge of cyber users resulting in enhanced positive attitude and behavior towards cybersecurity. User awareness and education also helps to strengthen the weakest links ensuring security of networks and information systems whether they are individuals, businesses or governments.

In conclusion, the government should see to it that cybersecurity awareness and education becomes a civic priority since a cyber-attack is a matter of when and not if. Awareness campaigns should be designed by the government that will effectively communicate the importance of cybersecurity and this should be established from an early stage in order to inculcate a cybersecurity culture where cyber users are completely aware of their actions and how to secure themselves when accessing the cyberspace.

5.3 RECOMMENDATIONS

It is investment in knowledge that creates our actual future. People who are unable to benefit from the digital age will be denied the education and resources necessary to fulfill their potential, because nothing empowers like access to opportunity. As long as the priceless potential of these marginalized communities remain untapped, we collectively deny ourselves the limitless innovation and opportunities possible. If we don’t close this digital divide, people in developing countries like Nigeria would never be able to compete with their counterparts globally and the future consequences are too dire to imagine.

5.4 CYBER SECURITY IMPLICATIONS:

1. First, our leaders must come to terms with the fact that technology carries the power to solve most of our problems if properly applied. We must accept this at once in our collective minds. With this in mind, leaders should strategically create sustainable data centers and tech hubs in every local government area across the country to improve access. This will empower people economically with the capacity to afford and access digital tools and resources.

2. Data Privacy and Protection: With increased reliance on digital platforms, educational institutions must prioritize data privacy and protection. They need to implement robust security measures to safeguard student and staff data from unauthorized access, breaches, and cyber-attacks.

3. Phishing and Social Engineering: Cybercriminals often exploit vulnerabilities by using phishing emails, deceptive websites, or social engineering techniques to gain unauthorized access. Educating students, teachers, and staff about these threats and implementing security awareness programs is crucial.

4. Network Security: Educational institutions must ensure the security of their networks and Wi-Fi infrastructure. Implementing firewalls, intrusion detection and prevention systems, and strong encryption protocols can help prevent unauthorized access and data breaches.

5. Device Security: As students and teachers use personal devices for remote learning, it is important to emphasize device security. Encouraging the use of up-to-date antivirus software, strong passwords, and regular software updates can mitigate the risk of malware infections and unauthorized access.

6. Secure Remote Learning Platforms: Educational institutions should carefully select and assess the security features of online learning platforms they adopt. Ensuring encryption of data transmission, secure login procedures, and regular security audits are essential for maintaining a secure learning environment.

7. Staff Training**:** Proper training and awareness programs for teachers and staff members are crucial to help them identify potential security risks and follow best practices. This can include training on password hygiene, recognizing phishing attempts, and handling sensitive information securely.

8. Incident Response and Disaster Recovery: Having an effective incident response plan in place is essential to minimize the impact of cyber-attacks. Regularly backing up data, maintaining off-site backups, and testing the restoration process can help in the event of a security incident.

5.5 SUGGESTIONS FOR FURTHER RESEARCH

Suggestions for further research as a result from the findings of this study are:

The present study has some limitations. First, we must confess that the sample size is rather small when compared to the makeup of the study participants, who were selected from public and private academic institutions. So, future research could use a larger sample size to boost the validity of the findings. In addition, further research into the successful implementation of e-learning strategies, tools, and platforms in less digitalized economies like Nigeria, with a focus on digital divide issues should be looked into.

Additionally, a case study approach could be utilized to identify unique difficulties and advancements of Nigerian education institutions. The research further suggest that this would list the difficulties that a variety of higher education institutions face in order to provide institutionspecific solutions that take into account the peculiarities of geographical locations as well as infrastructure issues.

REFERENCES

Adamu A. Garba, Maheyzah Md. Siraj et al - Cybersecurity Awareness among Students in Yobe State" University, Nigeria | International Journal on Emerging Technologies 11(5): 41-49(2020)

Adelakun Iyanuoluwa Samuel - Coronavirus (COVID-19) and Nigerian Education System: Impacts, management, responses and way forward https://www.researchgate.net/publication/344115847, vol. 3 issue 4, 2020 ISSN 2617- 4588

Adeoye, Itunuoluwa & Adanikin, Ayobami & Adanikin, Ariyo. (2020). COVID-19 and ELearning: Nigeria Tertiary Education System Experience. 5. 28-31.

Aidoo, F.K (2017). End Users Security Awareness Campaign from Information Security Threats, Vulnerabilities and Concurrent Cyber-Attacks. Texila International Journal of Academic Research, Vol. 4, Issue 2, ISSN: 2520-3088, DOI:10.21522/TIJAR.2014.04.02.Art020

Ajadi, Timothy & Salawu, Ibrahim & Adeoye, Femi. (2008). E-learning and distance education in Nigeria. Turkish Online Journal of Educational Technology. 7. 61-70.

Alaba Tolulope Agbele and Emmanuel Akinbami Oyelade - Impact of COVID-19 on the Nigerian Educational System: Strengths and Challenges of Online/Virtual Education | Agbele and Oyelade; AJESS, 13(1): 26-35, 2020; Article no. AJESS.62349, https://www.researchgate.net/publication/346528423

Allah Nawaz (2013) Using e-learning as a tool for 'education for all' in developing states Vol. 4(3), pp. 38-46, June, 2013 DOI: 10.5897/IJSTER10.057 ISSN 2141-6559 ©2013 Academic Journals http://www.academicjournals.org/IJSTER

Almeida, F. & Carneiro, P. (2021). Challenges of privacy in e-learning in the context of

Apu Pavithran December, 2020 https//www. helpnetsecurity.com/ as technology develops in education so does the need for cybersecurity

Augustine Sambo Azi - Managing Nigeria's Education amidst the Covid- 19 Pandemic Era: Implication on Educational Funding | Kampala International University ISSN: *2413-9580*; 8(1): 7–13

Aven, T., & Renn, O. (2010). Risk management. In Risk Management and Governance (pp. 121-158). Springer.

Badamasi, Bukhari & Utulu, Samuel. (2021). Badamasi Utulu - Cybercrime Framework for Nigerian Universities.

Bassey Moses Igwe - Covd-19 Pandemic and Education in Nigeria | Research and Reviews: Journal of Social Sciences Volume 8 | Issue 1| January, 2022

Bello, Rotimi-Williams and Otobo, Firstman Noah and Olubummo, Daniel Adebiyi and Abubakar, S. and Bello, Stella Nike. COVID-19 and Virtual World: The Implications on Nigeria Education (March 16, 2021).

BOLAJI Sefiu Olaitan - challenges of integrating mobile technologies into teaching and learning process in Nigerian primary schools during covid-19 pandemic, || Trailblazer International Journal of Educational Research, Volume 1, Number 1, August, 2020

Boothe, D. (2021). The global impact of the COVID-19 pandemic and online learning: A multinational study. In S. Jackowicz & I. Sahin (Eds.), *Online Education during the COVID-19 Pandemic: Issues, Benefits, Challenges, and Strategies* (pp. 1-18). ISTES Organization. 2020Pages 843-847,ISSN 1877-0509, https://doi.org/10.1016/j.procs.2020.05.121.

Bukhari Badamasi, Framework For Managing Cybercrime Risks In Nigerian Universities 2021 American University of Nigeria, bukhari.badamasi@aun.edu.ng Samuel C. Avemaria Utulu, American University of Nigeria, samuel.otulu@aun.edu.n

Bukhari, B. (2018). Effects of Security Protocols on Cybercrme in Ahmadu Bello University, Zaria [Academic Masters, University of KwaZulu Natal, South Africa].

Catherine Russell 9.7million Nigerian students may never return to school – UNICEF - Punch Newspapers (punchng.com)

Chapman, J. (2019). How safe is your data? Cyber-security in higher education. Higher Education Policy Institute Policy.

CISA (2019). Security Tip (ST04-002): Choosing and protecting passwords. Internet: https://uscert.cisa.gov/ncas/tips/ST05-017, Accessed 21/11/2020

CISA (2019). Security Tip (ST05-017): Cybersecurity for Electronic Devices. Internet: https://uscert.cisa.gov/ncas/tips/ST05-017, Accessed 19/11/2020

CISCO Networking Academy (2020). Cybersecurity. CISCO. Internet: https://www.netacad.com/sites/default/files/cybersecurity_infographic.pdf?utm_source=student_newsletter&utm_medium=email&utm_campaign=cyber_month

Conrad, D. & Openo, J. Assessment Strategies for Online Learning: Engagement and Authenticity (Athabasca Univ. Press, 2018).

Coopasami, M., Knight, S. & Pete, M. (2017), "e-Learning readiness amongst nursing students at the Durban University of Technology". Health SA Gesondheid, vol. 22, pp. 300–306.
COVID-19. In S. Jackowicz & I. Sahin (Eds.), *Online Education during the COVID-19*

Crawford, Joseph & Butler-Henderson, Kerryn & Jurgen, Rudolph & Malkawi, Bashar H. & Glowatz, Matt & Burton, Rob & Magni, Paola & Lam, Sophia. (2020). COVID-19: 20 countries' higher education intra-period digital pedagogy responses. Journal of Applied Learning & Teaching. 3. 10.37074/jalt.2020.3.1.7.

Daniel, S.J. Education and the COVID-19 pandemic. *Prospects* 49, 91–96 (2020).

https://doi.org/10.1007/s11125-020-09464-3

De Paoli, S., Johnstone, J., Coull, N., Ferguson, I., Sinclair, G., Tomkins, P., Brown, M., & Martin, R. (2020). A Qualitative Exploratory Study of the Knowledge, Forensic, and Legal Challenges from the Perspective of Police Cybercrime Specialists. Policing: A Journal of Policy and Practice.

Deb, S. (2011), "Effective distance learning in developing countries using mobile and multimedia technology". International Journal of Multimedia and Ubiquitous Engineering, vol. 6, no. 2, pp. 33–40.

Edeh Michael Onyema, Dr. Nwafor Chika Eucheria et al - Impact of Coronavirus Pandemic on Educatio | Journal of Education and Practice www.iiste.org ISSN 2222-1735 (Paper) ISSN 2222-288X (Online) Vol.11, No.13, 2020 May

EDUCAUSE (2021). *2021 EDUCAUSE Horizon Report® | Information Security Edition.* Boulder, CO: EDUCAUSE Publications

Ekpoh, U. I., Edet, A. O., & Ukpong, N. N. (2020). Security Challenges in Universities: Implications for Safe School Environment. Journal of Educational and Social Research, 10(6), 112-112.

EKRAN (2019). Twelve Best Cybersecurity Practices in 2020. Internet: https://www.ekransystem.com/en/blog/best-cyber-security-practices. Accessed 19/11/2020

Elliot Mbunge, Boluwaji Akinnuwesi et al 2020 - A critical review of emerging technologies for tackling COVID-19 pandemic | Hum Behav & Emerg Tech. 2021;3:25–39. wileyonlinelibrary.com/journal/hbe2

Eluwah, Daniel. (2021). CYBER AWARENESS AND EDUCATION IN NIGERIA: AN ASSESSMENT. 10.13140/RG.2.2.23425.79202.

Eze, Uchenna N.; Sefotho, Maximus M.; Onyishi, Charity N.; and Eseadi, Chiedu, "Impact of COVID-19 pandemic on Education in Nigeria: Implications for Policy and Practice of elearning" (2021). Library Philosophy and Practice (e-journal). 5651. https://digitalcommons.unl.edu/libphilprac/5651

Fulton, C. Information Learn. Sci. 121, 579–585 (2020)

Hedge and Hayword (2004) in Aboderin, O.S. (2011). The Status Information and Communication Technology (ICT) in Secondary Schools in Ondo State. (unpublished M.Ed. Thesis.).

Hollis, S. (2015). The role of regional organizations in disaster risk management. In The Role of Regional Organizations in Disaster Risk Management (pp. 1-12). Springer.

Internet users in Nigeria 2018-2022, with forecasts up until 2027 Doris Dokua Sasu Dec 5, 2022 https://www.statista.com/statistics/183849/internet-users-nigeria/

Isaac Oladipupo Millions of Kids in Nigeria Can't Learn Because They Don't Have Internet. How
Do We Close The 'Digital Divide'? (globalcitizen.org)
Issues, Benefits, Challenges, and Strategies. ISTES Organization.

Jackowicz, S. & Sahin, I. (Eds.). (2021). *Online Education during the COVID-19 Pandemic:*

Jiang X, Goh TT, Liu M. On Students' Willingness to Use Online Learning: A Privacy Calculus Theory Approach. Front Psychol. 2022 Jun 13;13:880261. doi: 10.3389/fpsyg.2022.880261. PMID: 35769738; PMCID: PMC9236193.

Joel Ogunyemi, Johnson Adesanya and Akin Salako - Application of Emerging Technologies for Innovation in Nigeria: Prospects and Challenges in Post Covid-19 Era. | NSE Ilaro Branch, 1st National Conference, Ilaro, 2-3 November, 2020.

Johnson, N., Veletsianos, G. & Seaman, J. Online Learn. 24, 6–21 (2020).

Kaspersky Lab (2020). Tips on how to protect yourself against cybercrime. Kaspersky Resource Centre. Internet: https://www.kaspersky.com/resource-center/threats/what-is-cybercrime. Accessed on 24/10/2020

Kaspersky Lab (2020). What is Cybersecurity? Kaspersky Resource Centre. Internet: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security. Accessed on 25/10/2020

Krejcie, R.V., & Morgan, D.W., (1970). Determining Sample Size for Research Activities. Educational and Psychological Measurement.

Krönke, Matthias. (2020). Africa's digital divide and the promise of e-learning.

Kruger, H. & Kearney, W.D. (2006). A prototype for assessing information security awareness. Computers & Security. 25. 289-296. 10.1016/j.cose.2006.02.008.

Linda Darling-Hammond, Monica Martinez, Adam K. Edgerton, Hanna Melnick, and Abby Schachner. Restarting and Reinventing School: Learning in the Time of COVID and Beyond (Learning Policy Institute, 2020).

Lohote Prathamesh Y. – need for cyber security education in schools | international journal of innovative research in technology, vol. 8 issue 2 | ISSN:2349-6002, July 2021

Makeri Ajiji, Yakubu. (2017). Cyber security issues in Nigeria and challenges. International journal of advanced research in computer science and software engineering. 7. 315321.10.23956/V6112/01204.

Malale, M., Gomba, G. & Dichaba, M. (2018), "Constraints to optimal adoption of e-learning resources by UNISA students: an open distance learning context". In U. Ogbonnaya, & S. Simelane-Mnisi (Ed.), Proceedings of the South Africa International Conference on Educational Technologies 2018 (pp. 182-192). Pretoria: African Academic Research Forum.

Meskhi, B., Ponomareva, S. & Ugnich, E. (2019), “E-learning in higher inclusive education - needs opportunities and limitations”. International Journal of Educational Management, vol. 33, no. 3, pp. 424–437.

Meskhi, B., Ponomareva, S. & Ugnich, E. (2019), “E-learning in higher inclusive education - needs opportunities and limitations”. International Journal of Educational Management, vol. 33, no. 3, pp. 424–437.

Mikkola, M., Oksanen, A., Kaakinen, M., Miller, B. L., Savolainen, I., Sirola, A., Zych, I., & Paek, H.-J. (2020). Situational and Individual Risk Factors for Cybercrime Victimization in a Cross-national Context. International Journal of Offender Therapy and Comparative Criminology, 0306624X20981041.

Morgan, S. (2020). Cybercrime To Cost The World $10.5 Trillion Annually By 2025 Cybercrime Magazine. In.

Nigerian Bureau of Statistics (NBS) (2020). Telecoms Data Q1 2020. https://nigerianstat.gov.ng/resource/Q1%202020%20Telecoms%20data.xlsx. Retrieved 23/9/2020

Obuekwe, G. & Eze, R.-A. (2017), “Promoting best practices in teaching and learning in Nigerian universities through effective e-learning: prospects and challenges”. International Conference on E-Learning (pp. 184-188). International Association for the Development of the Information Society.

OCHA 12 million Nigerian students to have increased access to education through new Learning Passport - Nigeria | ReliefWeb

Oguguo, B. C. E., Ocheni, C. A., & Oguguo, E. C. (2021). The role of COVID-19 in

Okereafor K. and Manny P. (2020): Understanding Cybersecurity Challenges of Telecommuting and Video Conferencing Applications in the COVID-19 Pandemic. International Journal in IT & Engineering (IJITE) Volume 8 Issue 6,

Omodunbi B.A., Olaniyan O.M., Adeyanju I.A, A.A Sobowale, Okomba Nnamdi, Esan Adebimpe, Adanigbo O.O. and Olusesi Ayobami T., Cyber Security Threats in the Era of Covid -19 Pandemic: A Case Study of Nigeria System, International Journal of Advanced Research in Engineering and Technology, 11(9), 2020, pp. 387-396. http://www.iaeme.com/IJARET/issues.asp?JType=IJARET&VType=11&IType=9

Osho, O., & Onoja, A. D. (2015). National Cyber Security Policy and Strategy of Nigeria: A Qualitative Analysis. International Journal of Cyber Criminology, 9(1).

Osterman (2021). Cybersecurity in Education – White Paper. *Osterman Research.*

OSU (2018). Antivirus. Cybersecurity. The Ohio State University. Internet:

https://cybersecurity.osu.edu/cybersecurity-you/use-right-tools/anti-virusAccessed 26/11/2020

Osuji Catherine U. Nwoke, Bright Ihechukwu (2019), Pre-service teachers' perception towards role of e-learning in science education in teacher training institutions | International Journal of Science and Technology

Osuji, C. & Nwoke, B. (2019). Pre-service teachers' perceptions towards role of e-learning in science education in teacher training institutions. International Journal of Science and Technology (STECH), Ethiopia. 8(1), 40-49. DOI: http://dx.doi.org/10.4314/stech.v8i1.4

Ouma, G., Awuor, F. & Kyambo, B. (2013), "E-learning readiness in public secondary schools in Kenya". European Journal of Open, Distance and e-Learning, vol. 16, no. 2, pp. 97–110.

Ouma, G., Awuor, F. & Kyambo, B. (2013), "E-learning readiness in public secondary schools in Kenya". European Journal of Open, Distance and e-Learning, vol. 16, no. 2, pp. 97–110.

Oye, N.D., Salleh, M. & Iahad, N. A. (2011), "Challenges of E-Learning in Nigerian University Education Based on the Experience of Developed Countries". International Journal of Managing Information Technology, vol. 3, no. 2, pp. 39-48

Pandemic: Issues, Benefits, Challenges, and Strategies (pp. 19-38). ISTES Organization.

Pandemic: Issues, Benefits, Challenges, and Strategies (pp. 281-292). ISTES Organization.

Pennisi, E. Science 369, 239–240 (2020).

Purohit, D. P., Siddiqui, N., Nandan, A., & Yadav, B. P. (2018). Hazard identification and risk assessment in construction industry. International Journal of Applied Engineering Research, 13(10), 7639-7667.

Rajasekharaiah, K. M., Dule, C. S., & Sudarshan, E. (2020). Cyber Security Challenges and its Emerging Trends on Latest Technologies. IOP Conference Series: Materials Science and Engineering, 981, 022062. https://doi.org/10.1088/1757-899x/981/2/022062 restructuring the education sector in Nigeria through information and communication

S. Gejendhiran, S. Arokia Anicia, S. Vignesh, M. Kalaimani,Disruptive Technologies - A promising key for Sustainable Future Education,Procedia Computer Science,Volume 172,

S. Nwachukwu, C. Ugwu and Joseph W, - "Digital Learning in Post COVID-19 Era: Policy Options and Prospects for Quality Education in Nigeria" (2021). | Library Philosophy and Practice (e-journal). 5122. https://digitalcommons.unl.edu/libphilprac/5122

Sanoo, J. (2018). Cyber Security Tutorials. Retrieved 26/06/2020 from https://www.javatpoint.com/cyber-security-introduction

Schneier, B. (2009). Schneier on security. John Wiley & Sons.

Setera K. (2020). *FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic.* Chelsea, MA: FBI Boston.

Singh V., Thurman A. (2019). How many ways can we define online learning? A systematic literature review of definitions of online learning (1988-2018). *Am. J. Distance Educ.* 33 289–306. 10.1080/08923647.2019.1663082

Swivelsecure 2022 https//www.swivelsecure.com/why cybersecurity needs to be a priority for the educational sector

Tabassum, L and Baker, S. (2020). Cybersecurity and Safety Measures. International Research Journal of Modernization in Engineering Technology and Science. Vol 02, Issue:06. June2020. Available at SSRN: https://ssrn.com/abstract=3641388

technology. In S. Jackowicz & I. Sahin (Eds.), *Online Education during the COVID-19* Uchenna N. Eze 2021 "Impact of COVID-19 pandemic on Education in Nigeria: Implications for Policy and Practice of e-learning"

U-EENI, (2022). E-learning as a disruptive innovation. U-EENI. Retrieved from http://www.u-eeni.edu.es.com

Uwa Ohiku 2017 Disruptive technologies & Nigeria's regulatory responsehttps://businessday.ng/analysis/article/disruptive-technologies-nigerias-regulatoryresponse/

Valeriano, B., & Maness, R. C. (2015). Cyber war versus cyber realities: Cyber conflict in the international system. Oxford University Press, USA.

Vaughan, N. D., Cleveland-Innes, M. & Garrison, D. R. Assessment in Teaching in Blended Learning Environments: Creating and Sustaining Communities of Inquiry (Athabasca Univ. Press, 2013)

Venter, I. M., Blignaut, R. J., Renaud, K., & Venter, M. A. (2019). Cyber security education is as essential as "the three R's." Heliyon, 5(12), e02855. https://doi.org/10.1016/j.heliyon.2019.e02855

WaterISAC (2016). 10 Basic Cybersecurity Measures: Best Practices to Reduce Exploitable Weaknesses and Attacks. WaterISAC Security Information Centre. Internet:https://www.waterisac.org/sites/default/files/public/10_Basic_Cybersecurity_Measures-WaterISAC_Oct2016%5B2%5D.pdf. Accessed 20/11/2020.

Webb, J., & Hume, D. (2018). Campus IoT collaboration and governance using the NIST cybersecurity framework.

WEF (2020) https://stripeolt.com/knowledge-hub/expert-intel/cybercrime-is-worldsthird-largesteconomy/#:~:text=our%20interconnected%20world.-

,According%20to%20the%20World%20Economic%20Forum%20(WEF)%2C%20cyber

crime%20has,reach%20%2410.5%20trillion%20by%202025%E2%80%A6

Whitehead, G. (2020). Investigation of factors influencing cybersecurity decision making in Irish SME's from a senior manager/owner perspective Dublin, National College of Ireland].

William Dawsey (2022) 5 Disruptive Technologies in Education | Chetu

Wolfswinkel, J. F., Furtmueller, E., & Wilderom, C. P. (2013). Using grounded theory as a method for rigorously reviewing literature. European Journal of Information Systems, 22(1), 45-55.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, L., Cetin, F. & Basim, H.N. (2020). Cyber Security Awareness, Knowledge and Behaviour: A Comparative Study. Journal of Comp. Info. Systems, 1-16. DOI: 10.1080/08874417.2020.1712269

APPENDIX A

SOURCE CODES

```
#!/usr/bin/env python
# coding: utf-8

# # The Impact of E-learning in Nigeria's Education Sector After COVID-19

# # 1. Data Gathering

# #### importing necessary libraries

# In[7]:

import pandas as pd import
numpy as np import
seaborn as sns
import matplotlib.pyplot as plt
```

```
# import Machine learning models  from sklearn.linear_model
import LinearRegression from sklearn.preprocessing import
LabelEncoder, OneHotEncoder
from sklearn.model_selection import train_test_split
from sklearn.metrics import accuracy_score

# In[8]:

# Load the dataset
df = pd.read_csv('ONLINE EDUCATION SYSTEM REVIEW.csv')

# # 2.Data Assesment

# In[9]:

df.head()

# In[10]:

df.tail()

# In[11]:


df.shape

# In[12]:

df.columns

# In[13]:

df.info()

# In[14]:

# Checking for null values
df.isnull().sum()

# In[15]:

# checking for duplicate row
df.duplicated().sum()

# In[16]:
```

```
# checking for statiscal info about the data
df.describe() # # 3. Data Cleaning
# Rename the columns to more intuitive

# In[17]:

# Define a dictionary to map old column names to new ones new_columns
= {
   'Age(Years)': 'Age',
   'Number of Subjects': 'Subjects',
   'Device type used to attend classes': 'Device_Type',
   'Economic status': 'Income',
   'Internet facility in your locality': 'Internet_Availability',
'Are you involved in any sports?': 'Sports_Involvement',
   'Do elderly people monitor you?': 'Elderly_Monitoring',
   'Study time (Hours)': 'Study_Time',
   'Sleep time (Hours)': 'Sleep_Time',
   'Time spent on social media (Hours)': 'Social_Media_Time',
   'Interested in Gaming?': 'Gaming_Interest',
   'Have separate room for studying?': 'Separate_Study_Room',
   'Engaged in group studies?': 'Group_Study_Involvement',
   'Average marks scored before pandemic in traditional classroom': 'Pre_Pandemic_Marks',
   'Your interaction in online mode': 'Online_Interaction',
   'Clearing doubts with faculties in online mode': 'Online_Doubt_Clearance',
   'Interested in?': 'Interest_In_Learning',
   'Your level of satisfaction in Online Education': 'Online_Satisfaction' }

# Rename the columns
df = df.rename(columns=new_columns)

# In[18]:

df.columns

# # 4. Data Exploration

# In[19]:

# Generating summary statistics
df.describe()

# In[20]:

# Visualizing the distribution of 'Performance in online' plt.figure(figsize
= (15,8))
sns.distplot(df['Performance in online'], bins= 20)
plt.xlabel('Performance in online') plt.ylabel('Frequency')
```

```
plt.title('Distribution of Performance in online') plt.show()

# In[21]:

# Set up subplots
fig, axs = plt.subplots(1, 3, figsize=(15, 5))

# Plot histograms axs[0].hist(df['Age'],
bins=20) axs[0].set_xlabel('Age')
axs[0].set_ylabel('Count')
axs[0].set_title('Histogram of Age')

axs[1].hist(df['Pre_Pandemic_Marks'], bins=20)
axs[1].set_xlabel('Pre-Pandemic Marks') axs[1].set_ylabel('Count')
axs[1].set_title('Histogram of Pre-Pandemic Marks')

axs[2].hist(df['Performance in online'], bins=20)
axs[2].set_xlabel('Performance in online')
axs[2].set_ylabel('Count') axs[2].set_title('Histogram
of Performance in online')

plt.show()

# In[22]:

# Define categorical columns
cat_cols = ['Gender', 'Device_Type', 'Sports_Involvement']

# Generate bar plots for each categorical variable for
col in cat_cols:
   plt.figure(figsize=(8, 6))     ax =
sns.countplot(x=col, data=df)
plt.title(f"{col} Distribution", fontsize=16)
plt.xlabel(col, fontsize=12)
plt.ylabel("Count", fontsize=12)
   plt.show()

# In[23]:

# define the columns for which to generate pie charts
pie_cols = ['Internet_Availability', 'Gender', 'Device_Type']

# loop through the columns and generate pie charts
for col in pie_cols:     counts =
df[col].value_counts()     labels =
counts.index.tolist()     values =
counts.values.tolist()     plt.pie(values,
labels=labels, autopct='%1.1f%%')     plt.title(col)
```

```
    plt.show()

# In[24]:

# Identifying correlations or patterns
plt.figure(figsize = (10,5)) corr =
df.corr()
sns.heatmap(corr, annot=True, cmap='coolwarm')
plt.show()

# In[25]:

df['Online_Satisfaction'].value_counts()

# In[26]:

df['Online_Satisfaction'].value_counts().plot(kind = "bar") plt.xticks(rotation=0)
plt.show()

# In[27]:

df['Performance in online'].value_counts()

# In[28]:

df['Performance in online'].value_counts().plot(kind  = "bar")

plt.xticks(rotation=0)
plt.show()

# # 5. checking for outliers

# In[29]:

# Identifying outliers in
sns.boxplot(x=df['Performance in online']) plt.show()

# In[30]:

# create box plot for 'Performance in online'
sns.boxplot(data=df, y='Performance in online') plt.show()

# create scatter plot for 'Study time (Hours)' vs. 'Performance in online'
sns.scatterplot(data=df, x='Study_Time', y='Performance in online') plt.show()

# create scatter plot for 'Sleep time (Hours)' vs. 'Performance in online'
sns.scatterplot(data=df, x='Sleep_Time', y='Performance in online') plt.show()
```

```
# create scatter plot for 'Time spent on social media (Hours)' vs. 'Performance in online'
sns.scatterplot(data=df, x='Social_Media_Time', y='Performance in online') plt.show()

# # 6. Feature Selection

# After checking fot the correlation of all the independent variable with the dependent variable which is Perromance in online, I decided to drop the following colums 'Subjects', 'Family size', 'Social_Media_Time' and 'Sleep_Time'  because they don't have correlation with the independent variable.

# In[31]:

df.drop(['Subjects', 'Family size', 'Sleep_Time', 'Social_Media_Time'], axis = 1, inplace = True )

# # 7. Feature Engineering

# In[32]:

df.head()

# ## Encodings

# In[33]:

# Define the categorical columns for encoding
cat_cols_one_hot = ['Gender', 'Sports_Involvement', 'Elderly_Monitoring', 'Separate_Study_Room', 'Group_Study_Involvement', 'Gaming_Interest', 'Interest_In_Learning']
cat_cols_label = ['Home Location','Device_Type', 'Level of Education', 'Income','Online_Satisfaction', "Performance in online", 'Internet_Availability']

from sklearn.preprocessing import OrdinalEncoder

ordinal_encoder = OrdinalEncoder()

df[['Pre_Pandemic_Marks']] = ordinal_encoder.fit_transform(df[['Pre_Pandemic_Marks']])

# Perform One-Hot Encoding
one_hot_encoder = OneHotEncoder(sparse=False, drop='first') one_hot_encoded_cols = pd.DataFrame(one_hot_encoder.fit_transform(df[cat_cols_one_hot]))
one_hot_encoded_cols.columns = one_hot_encoder.get_feature_names_out(input_features=cat_cols_one_hot)
df = pd.concat([df, one_hot_encoded_cols], axis=1) df = df.drop(columns=cat_cols_one_hot)
```

```
# Perform Label Encoding label_encoder =
LabelEncoder() for col in cat_cols_label:
df[col] = label_encoder.fit_transform(df[col])

# In[34]:

df.head(15)

# In[35]:

df.shape

# In[36]:

df["Pre_Pandemic_Marks"].value_counts()

# # 8. Model Training

# # Result Interpretation for logistic regression using online satisfaction as dependent variable

# In[40]:

# import libraries import
pandas as pd
from sklearn.model_selection import train_test_split
from sklearn.preprocessing import StandardScaler from
sklearn.linear_model import LogisticRegression
from sklearn.metrics import classification_report, confusion_matrix

# split the dataset into training and testing sets
X = df.drop(['Online_Satisfaction'], axis=1) y
= df['Online_Satisfaction']
X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.2, random_state=42)

# scale the numerical features scaler
= StandardScaler()
X_train = scaler.fit_transform(X_train.select_dtypes(include='number')) X_test
= scaler.transform(X_test.select_dtypes(include='number'))

# train the logistic regression model lr
= LogisticRegression()
lr.fit(X_train, y_train)

# make predictions on the test set
y_pred = lr.predict(X_test)
```

```
# evaluate the model print('Confusion Matrix:\n',
confusion_matrix(y_test, y_pred)) print('\nClassification Report:\n',
classification_report(y_test, y_pred))


# The evaluation of the logistic regression model produced the following confusion matrix: #
# [[88 8 5]
# [19 27 1]
# [35 0 24]]

# In[32]:

# Split the dataset into training and testing sets
X = df.drop(['Performance in online'], axis=1) y
= df['Performance in online']
X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.2, random_state=42)

# Scale the numerical features
from sklearn.preprocessing import StandardScaler

scaler = StandardScaler()
X_train = scaler.fit_transform(X_train)
X_test = scaler.transform(X_test)

# Train the linear regression model lr
= LinearRegression()
lr.fit(X_train, y_train)

# Make predictions on the test set
y_pred = lr.predict(X_test)

# In[33]:

# Plot the actual vs predicted values for training and test sets plt.figure(figsize
= (10,5))
plt.scatter(y_train, lr.predict(X_train), label='Training')
plt.scatter(y_test, y_pred, label='Test')
plt.xlabel('Actual') plt.ylabel('Predicted')
plt.title('Actual vs Predicted') plt.legend()
plt.show()

# ## Model Evaluation

# In[34]:

# Evaluate the model using mean squared error from
sklearn.metrics import mean_squared_error
print("Mean squared error:", mean_squared_error(y_test, y_pred))
```

```
# Evaluate the model using root mean squared error rmse
= np.sqrt(mean_squared_error(y_test, y_pred))
print("Root Mean Squared Error:", rmse)

# Evaluate the model using Mean Absolute Error (MAE)
from sklearn.metrics import mean_absolute_error mae =
mean_absolute_error(y_test, y_pred)
print("Mean Asolute Error:", mae)

# Evaluate the model using R-Squared (R2) Score
from sklearn.metrics import r2_score r2 =
r2_score(y_test, y_pred)
print("R-Squared (R2) Score:", r2)

# Evaluate the model using Adjusted R-Squared Score
n = X_test.shape[0] p = X_test.shape[1] def
adjusted_r2_score(y_test, y_pred, n, p):     r2 =
r2_score(y_test, y_pred)     adj_r2 = 1 - ((1 - r2) * (n -
1)) / (n - p - 1)     return adj_r2

adj_r2 = adjusted_r2_score(y_test, y_pred, n, p)
print("Adjusted R-Squared Score:", adj_r2)
```

APPENDIX B

QUESTIONNAIRES

CYBER SECURITY IMPLICATION IN EDUCATIONAL SECTOR IN NIGERIA – A POST COVID-19 ASSESSMENT

Dear Respondent,

This questionnaire is purely an academic exercise and is intended to provide insight to the level of awareness Nigerians have with regards cyber related activities including security and crime. Your sincere responses will help me attempt to solve the problem. Be assured that your data is protected and treated with utmost confidentiality. I appreciate your cooperation.

Moses A. Triumphant (Researcher)

SECTION A: Personal Data (Please tick which applies)

S/N	I. Demographic Data	
1	Gender	Male ☐ Female ☐
2	Age bracket	16 – 20 ☐ 21 – 25 ☐ 26 – 30 ☐ 31 – 35 ☐ 36 – 40 ☐ 41 plus ☐
3	Educational qualification	Secondary ☐ Tertiary ☐ Postgraduate ☐
4	Designation status	Educators ☐ Student ☐ Others ☐
S/N	**II. Cyberspace Access and Usage**	
1	How do you access the cyberspace? (Tick all that applies)	Desktop ☐ Laptop ☐ Tablet ☐ Smartphone ☐ Others ☐
2	What is your preferred device for accessing the cyberspace?	Desktop ☐ Laptop ☐ Smartphone ☐ Other devices ☐ Tablet ☐
3	What is your source of e-learning services?	Personal gadgets ☐ School lab ☐ Office ☐ Family members ☐ Peers ☐
4	What do you use the cyberspace for?	Research ☐ Online examination ☐ E-learning ☐ Social media ☐ Communication ☐ Other services ☐
5	My school has moved from traditional class room studies to a virtual one.	Yes ☐ No ☐ Virtual only ☐ Traditional only ☐ Both ☐
6	Which virtual platforms have been created by your institution to ensure smooth academic work despite covid-19 pandemic.	Website _ WhatsApp ☐ Zoom ☐ Google meet ☐ Others ☐
7	Relevant teaching materials are delivered electronically.	Yes ☐ No ☐ Sometimes ☐ Most times ☐

SECTION B: Level of Cyber Awareness and Education among Nigerian Cyber Users

Kindly respond by ticking using the appropriate ratings;

S/N	I. Awareness of Cybercrime	Not Aware	Slightly Aware	Very Aware	Extremely Aware
1	To what extent are you aware about cybercrime?				
2	To what extent are you aware about phishing?				
3	To what extent are you aware about cyberbullying?				
4	To what extent are you aware about malwares/viruses?				
5	To what extent are you aware about identity theft?				
6	To what extent are you aware that you are a likely cybercrime target?				

S/N	II. Awareness of Cybersecurity	Not Aware	Slightly Aware	Very Aware	Extremely Aware
1	To what extent are you aware of the importance of cybersecurity?				
2	To what extent are you aware of the risks with using the cyberspace?				
3	To what extent are you aware about system security updates?				
4	To what extent are you aware of an anti-malware or anti-virus?				
5	To what extent are you aware of the use of a Virtual Private Network (VPN)?				

SECTION C: Measures Taken By Nigerian Cyber Users to Forestall Cybersecurity Incidents

Kindly respond by ticking using the appropriate ratings;

S/N	I. Behavioural Measures	Strongly Disagree	Disagree	Agree	Strongly Agree
1	I always perform system security updates whenever I see them				
2	I always perform anti-virus updates whenever I see them				
3	Changing passwords regularly is necessary				
4	Cyber awareness and education will improve my cybersecurity				
5	I download free files from the cyberspace no matter the source				
6	I always use a free Wi-Fi connection when I notice one				
7	Using same passwords on different online accounts is safe				

SECTION D: Impact of Cybersecurity Awareness and Education Initiatives

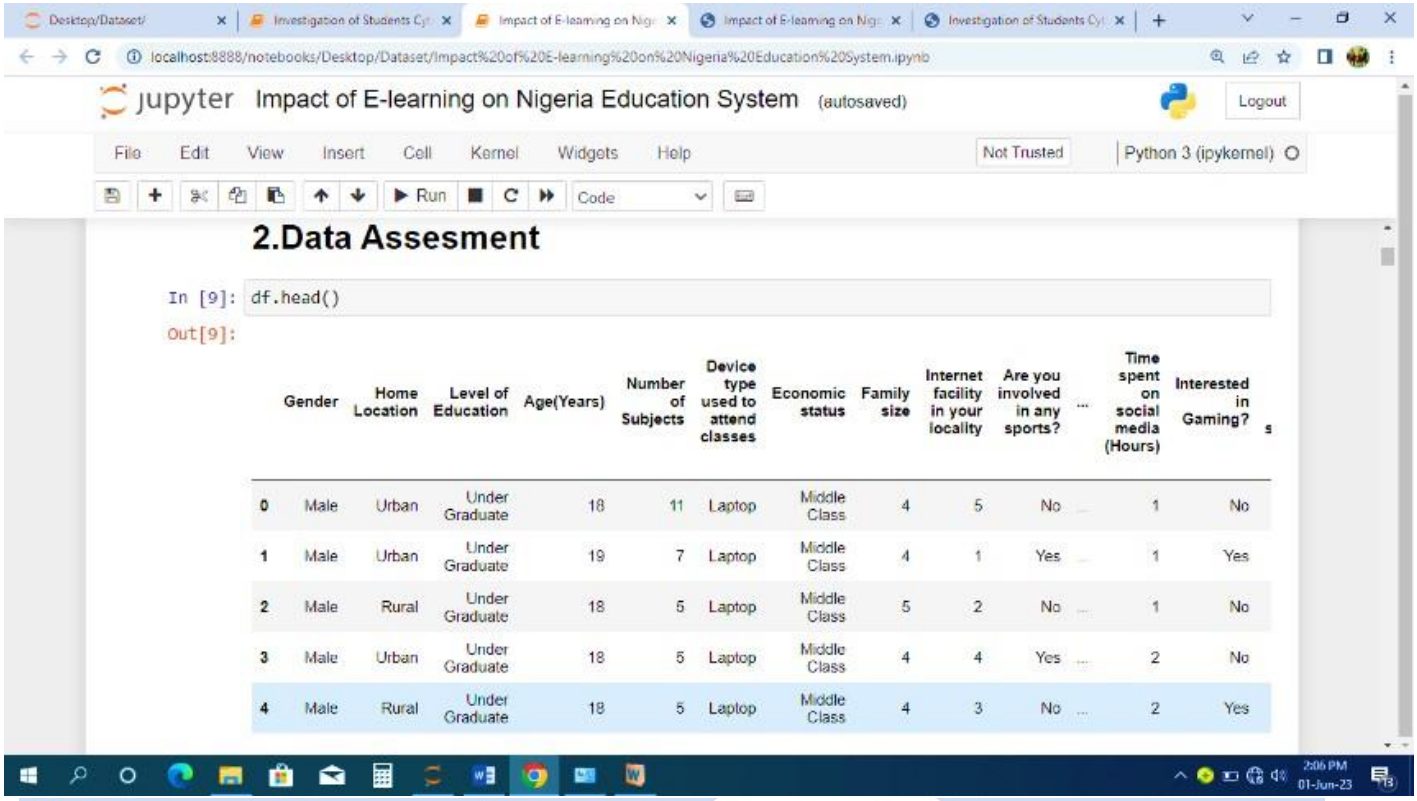
Kindly respond by ticking using the appropriate ratings;

S/N		Strongly Disagree	Disagree	Agree	Strongly Agree
1	Undoubtedly, the Covid - 19 pandemic has brought a face-lift (progress) in my academic institution.				
2	I believe the introduction of e-learning will intensify the use of digital devices on campus.				
3	My institution is giving student a good orientation on the e-learning solutions/ platforms.				
4	The National Cybersecurity Policy and Strategy on cyber awareness and education has been effective				
5	Overall, the government has performed well with its cybersecurity awareness and education initiatives				
6	The growth of internet patronage and usage has heightened (intensified) in my university.				
7	E-Learning is a new thing for me in my academic life as a result of the Covid-19 pandemic.				

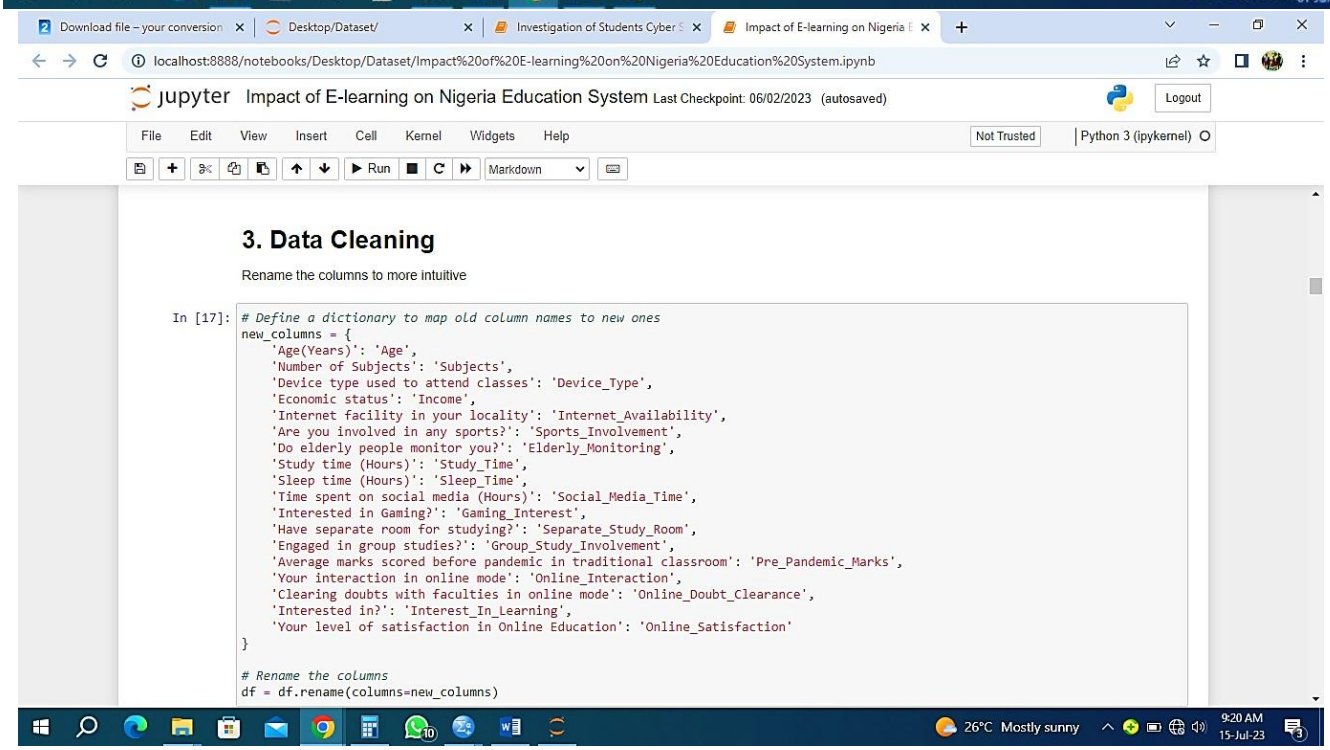
APPENDIX C

PROGRAM OUTPUT





	Gender	Home Location	Level of Education	Age(Years)	Number of Subjects	Device type used to attend classes	Economic status	Family size	Internet facility in your locality	Are you involved in any sports?	...	Time spent on social media (Hours)	Interested in Gaming?	s
0	Male	Urban	Under Graduate	18	11	Laptop	Middle Class	4	5	No	...	1	No	
1	Male	Urban	Under Graduate	19	7	Laptop	Middle Class	4	1	Yes	...	1	Yes	
2	Male	Rural	Under Graduate	18	5	Laptop	Middle Class	5	2	No	...	1	No	
3	Male	Urban	Under Graduate	18	5	Laptop	Middle Class	4	4	Yes	...	2	No	
4	Male	Rural	Under Graduate	18	5	Laptop	Middle Class	4	3	No	...	2	Yes	



Download file – your conversion | Desktop/Dataset/ | Investigation of Students Cyber S | Impact of E-learning on Nigeria E

localhost:8888/notebooks/Desktop/Dataset/Impact%20of%20E-learning%20on%20Nigeria%20Education%20System.ipynb

jupyter Impact of E-learning on Nigeria Education System Last Checkpoint: 06/02/2023 (autosaved)

Logout

File Edit View Insert Cell Kernel Widgets Help Not Trusted Python 3 (ipykernel)

Run Markdown

```
'Performance in online', 'Online_Satisfaction'],
dtype='object')
```

4. Data Exploration

In [19]:
```
# Generating summary statistics
df.describe()
```

Out[19]:

	Age	Subjects	Family size	Internet_Availability	Study_Time	Sleep_Time	Social_Media_Time	Online_Interaction	Online_Doubt_Clearance	Pe
count	1033.000000	1033.00000	1033.000000	1033.000000	1033.000000	1033.000000	1033.000000	1033.000000	1033.000000	10
mean	19.798645	7.03485	4.413359	3.586641	4.325266	6.947725	2.636980	2.930300	2.833495	
std	3.199158	2.81034	1.236750	1.026063	2.134233	1.324039	1.859625	1.105387	1.163629	
min	9.000000	1.00000	2.000000	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	
25%	18.000000	6.00000	4.000000	3.000000	3.000000	6.000000	1.000000	2.000000	2.000000	
50%	19.000000	7.00000	4.000000	4.000000	4.000000	7.000000	2.000000	3.000000	3.000000	
75%	20.000000	8.00000	5.000000	4.000000	6.000000	8.000000	3.000000	4.000000	4.000000	
max	40.000000	20.00000	10.000000	5.000000	10.000000	10.000000	10.000000	5.000000	5.000000	

In [20]:
```
# Visualizing the distribution of 'Performance in online'
plt.figure(figsize = (15,8))
sns.distplot(df['Performance in online'], bins= 20)
plt.xlabel('Performance in online')
plt.ylabel('Frequency')
```

26°C Mostly sunny 9:20 AM 15-Jul-23

Desktop/New folder (2)/ | Impact of E-learning on Nigeria E

localhost:8888/notebooks/Desktop/New%20folder%20(2)/Impact%20of%20E-learning%20on%20Nigeria%20Education%20System%20(1).ipynb

jupyter Impact of E-learning on Nigeria Education System (1) (autosaved)

Logout

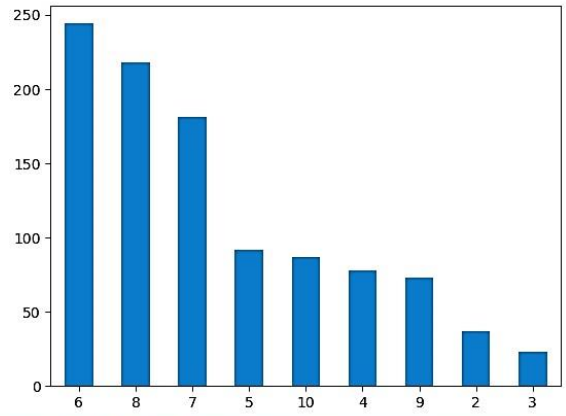
File Edit View Insert Cell Kernel Widgets Help Not Trusted Python 3 (ipykernel)

Run Code

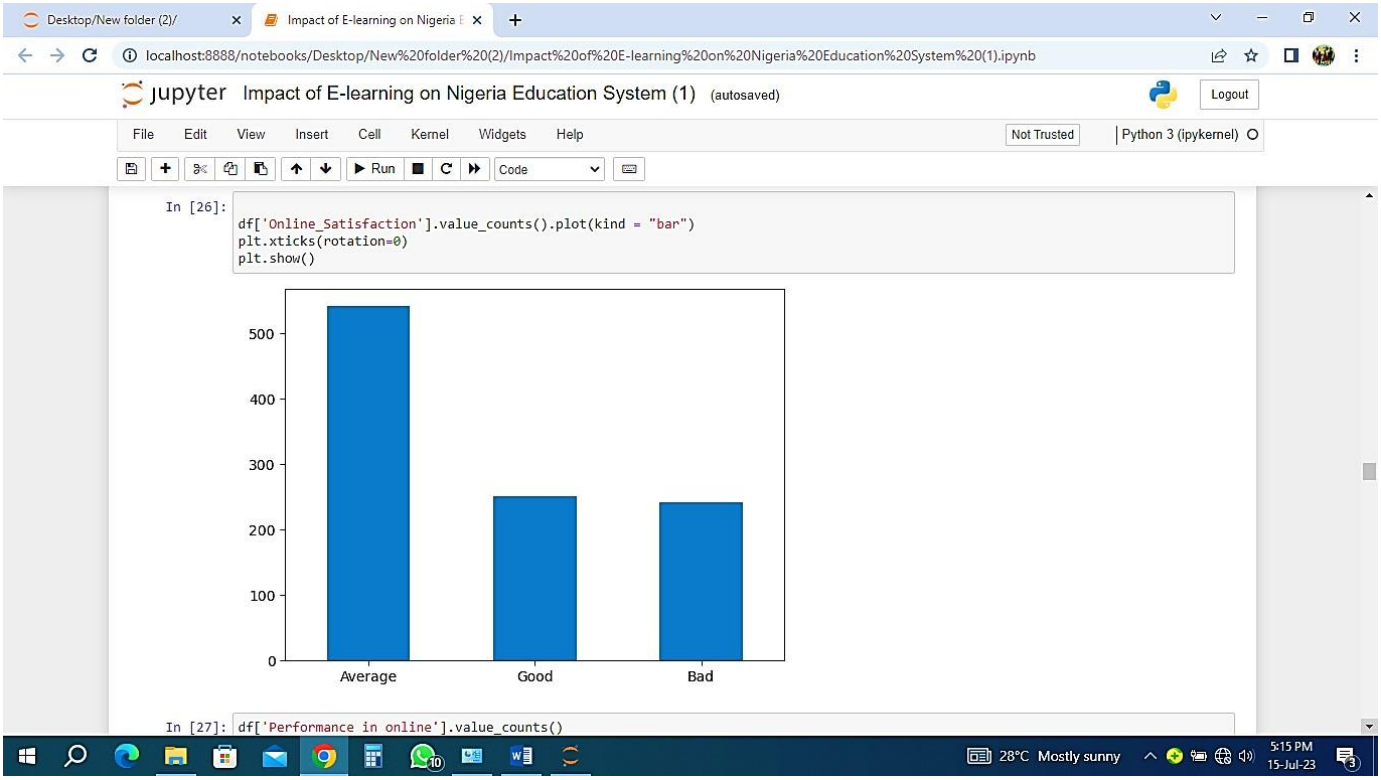
```
Name: Performance in online, dtype: int64
```

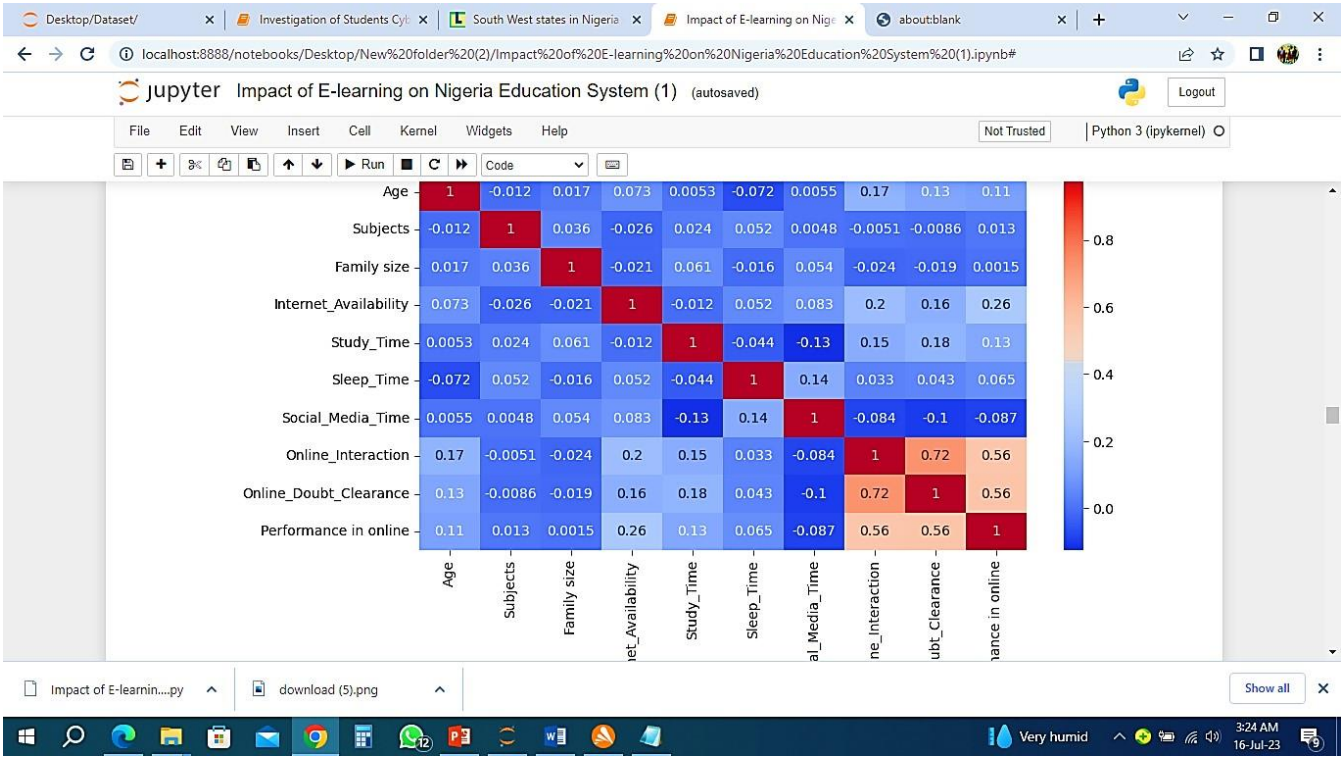
In [28]:
```
df['Performance in online'].value_counts().plot(kind  = "bar")

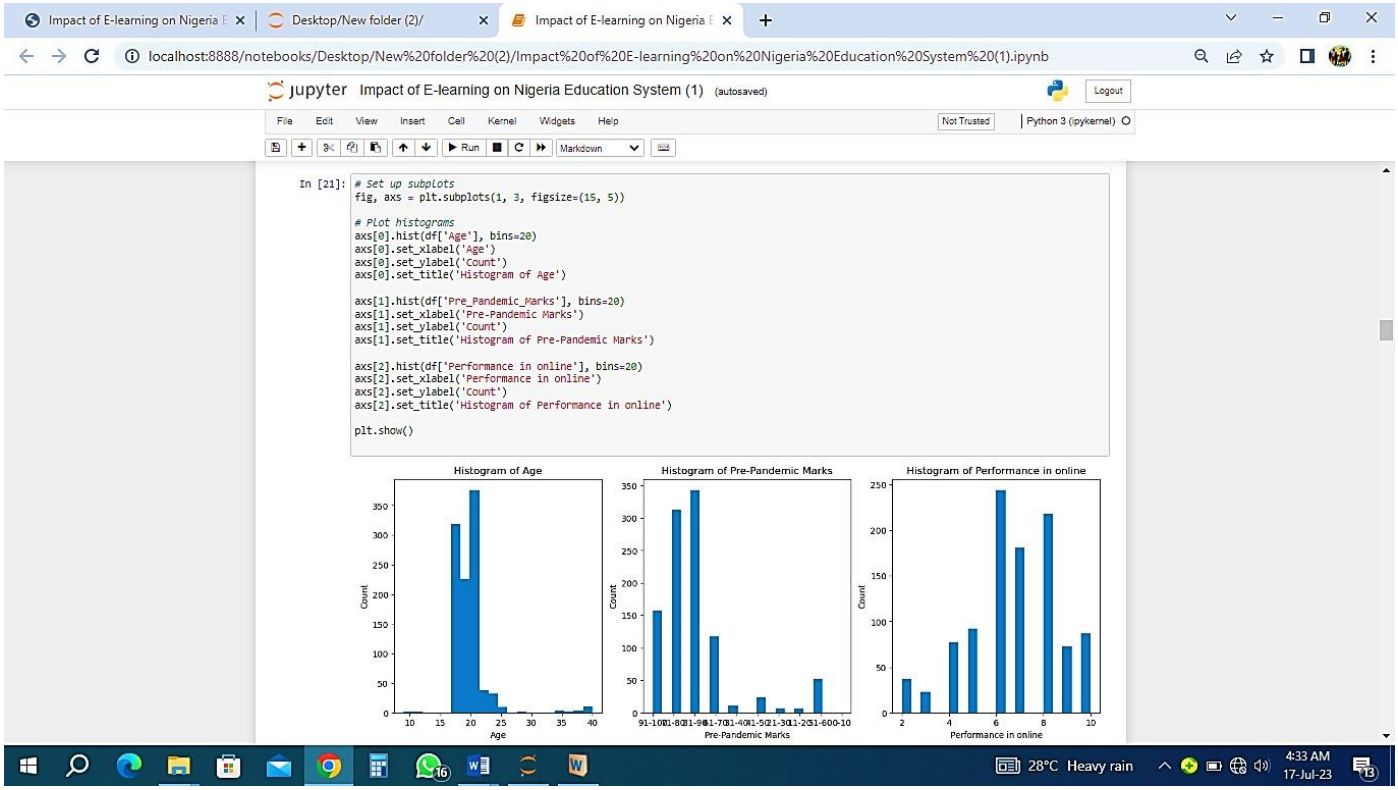
plt.xticks(rotation=0)
plt.show()
```



28°C Mostly sunny 5:16 PM 15-Jul-23


Desktop/New folder (2)/
Impact of E-learning on Nigeria
localhost:8888/notebooks/Desktop/New%20folder%20(2)/Impact%20of%20E-learning%20on%20Nigeria%20Education%20System%20(1).ipynb
jupyter Impact of E-learning on Nigeria Education System (1) (autosaved)
Logout
File Edit View Insert Cell Kernel Widgets Help
Not Trusted
Python 3 (ipykernel)
Run
Code
In [26]:
df['Online_Satisfaction'].value_counts().plot(kind = "bar")
plt.xticks(rotation=0)
plt.show()
500
400
300
200
100
0
Average
Good
Bad
In [27]:
df['Performance in online'].value_counts()
28°C Mostly sunny
5:15 PM
15-Jul-23


Impact of E-learning on Nigeria Education System (1) (autosaved)
Logout
File Edit View Insert Cell Kernel Widgets Help
Not Trusted
Python 3 (ipykernel)
Run
Code
Age 1 -0.012 0.017 0.073 0.0053 -0.072 0.0055 0.17 0.13 0.11
Subjects -0.012 1 0.036 -0.026 0.024 0.052 0.0048 -0.0051 -0.0086 0.013
Family size 0.017 0.036 1 -0.021 0.061 -0.016 0.054 -0.024 -0.019 0.0015
Internet_Availability 0.073 -0.026 -0.021 1 -0.012 0.052 0.083 0.2 0.16 0.26
Study_Time 0.0053 0.024 0.061 -0.012 1 -0.044 -0.13 0.15 0.18 0.13
Sleep_Time -0.072 0.052 -0.016 0.052 -0.044 1 0.14 0.033 0.043 0.065
Social_Media_Time 0.0055 0.0048 0.054 0.083 -0.13 0.14 1 -0.084 -0.1 -0.087
Online_Interaction 0.17 -0.0051 -0.024 0.2 0.15 0.033 -0.084 1 0.72 0.56
Online_Doubt_Clearance 0.13 -0.0086 -0.019 0.16 0.18 0.043 -0.1 0.72 1 0.56
Performance in online 0.11 0.013 0.0015 0.26 0.13 0.065 -0.087 0.56 0.56 1
0.8
0.6
0.4
0.2
0.0
Age
Subjects
Family size
Study_Time
Sleep_Time
Impact of E-learnin....py
download (5).png
Show all
Very humid
3:24 AM
16-Jul-23


Impact of E-learning on Nigeria Education System (1) (autosaved)
Logout
File Edit View Insert Cell Kernel Widgets Help
Not Trusted
Python 3 (ipykernel)
Run
Markdown
In [21]:
Set up subplots
fig, axs = plt.subplots(1, 3, figsize=(15, 5))
Plot histograms
axs[0].hist(df['Age'], bins=20)
axs[0].set_xlabel('Age')
axs[0].set_ylabel('Count')
axs[0].set_title('Histogram of Age')
axs[1].hist(df['Pre_Pandemic_Marks'], bins=20)
axs[1].set_xlabel('Pre-Pandemic Marks')
axs[1].set_ylabel('Count')
axs[1].set_title('Histogram of Pre-Pandemic Marks')
axs[2].hist(df['Performance in online'], bins=20)
axs[2].set_xlabel('Performance in online')
axs[2].set_ylabel('Count')
axs[2].set_title('Histogram of Performance in online')
plt.show()
Histogram of Age
Count
Age
Histogram of Pre-Pandemic Marks
Count
Pre-Pandemic Marks
Histogram of Performance in online
Count
Performance in online
28°C Heavy rain
4:33 AM
17-Jul-23