JOURNAL OF E-LEARNING AND KNOWLEDGE SOCIETY
Vol. 20, No. 2 (2024), pp. 55-66

Influence of Internet of Things Cybersecurity (IoTCS) on Educational Assessment Practices in University Learning Spaces in Nigeria

Basil C.E. Oguguo, Nnaji Anayo David, Uwakwe S.I.[1], Faith C. Omeke, Clifford O. Ugorji, Anthonia N. Ngwu, Chinwe Enyi, Obiageli .C. Njoku, Cletus Ugbor, Ugwu J. Okwudili, Cliff .I. Okebanama

University of Nigeri – Nsukka, Enugu State (Nigeria)

(submitted: 26/6/2024; accepted: 23/8/2024; published: 28/8/2024)

Abstract

The Internet of Things (IoT) presents a unique flexibility that facilitates higher productivity and rapid advancement in the educational sector, and more specifically in educational assessment. However, the huge cybersecurity issues associated with cyberspace pose a challenge for the IOT. The present study investigated the influence of the Internet of Things Cybersecurity (IoTCS) on educational assessment practices in university learning spaces. The researchers adopted a correlation research design involving a multistage sampling procedure with 297 lecturers as participants drawn from six universities in South-East Nigeria, who shared their opinions on the influence of IoTCS on assessment practices. The Internet of Things Cybersecurity Questionnaire (IoTCSQ) and Assessment Practices Scale (APS) were two instruments used for data collection and they were validated in line with the purpose of the study by three experts. The Cronbach Alpha reliability indices of the two instruments were 0.82, and 0.89 respectively. The result showed a significantly moderate positive relationship between the adoption of IoTCS and the effectiveness of assessment practices in university learning spaces, among others. The study concluded that the incorporation of IoTCS significantly influences assessment practices in university learning spaces, and recommended among others that school administrators should consider investing in IoT cybersecurity for the safety, fairness and reliability of assessment data.

KEYWORDS: Internet of Things Cybersecurity (IoTCS), Assessment Practices, Formative Assessment, Summative Assessment, Authentic Assessment.

DOI
https://doi.org/10.20368/1971-8829/1135973

CITE AS
Oguguo, B.C.E., David, N.A., Uwakwe S.I., Omeke, F.C., Ugorji, C.O., Ngwu, A.N., Enyi, C., Njoku, O.C., Ugbor, C., Okwudili, U.J., & Okebanama, C.I. (2024). Influence of Internet of Things Cybersecurity (IoTCS) on Educational Assessment Practices in University Learning Spaces in Nigeria. *Journal of e-Learning and Knowledge Society*, *20*(2), 55-66.
https://doi.org/10.20368/1971-8829/1135973

1. Introduction

Educational assessments have emphatically sustained as a critical component of the educational system, due to their role in the fulcrum of purifying, certifying and providing evidence for critical decisions that have to do with the credibility of the processes and products of the educational system. Over the years, educational assessment practices have developed from the orthodox paper-and-pencil tests (PPT) form to the real-time gathering of data through the use of smart devices in the league of Internet of Things (IoT), following the rapid advancement in communication technology which is significantly changing the natural way of life. However, this has highlighted the worries of researchers on the security of assessment cyberspaces especially in the recent global spike in the introduction of IoT in educational assessment practices, particularly in Nigeria as most examination bodies are adopting large-scale digital assessments. The Joint Admission and Matriculation Board (JAMB) has long adopted digital assessment, and recently the West African Examination Council (WAEC) has expressed commitment to the

[1] corresponding author - email: iroh.uwakwe@unn.edu.ng

same and likewise in most university learning spaces among others. These digital assessments are possible through the amazing role of IoT over the cloud.

The Internet of Things (IoT) has transformed the way we communicate with our environment, and its growing impact is being felt in the educational system. Ramlowat and Pattanayak (2019) opine that the advent of IoT has transformed all human interactions and the way we do things in education. Sheng et al. (2018) pointed out that, these transformations have given rise to new educational opportunities, especially for enhancing assessment practices in university learning spaces. Although the new opportunities, the American Council on Education (2017) highlighted that the prevalence of IoT devices in educational settings has been followed by a significant impact on the integrity and security of assessment processes due to the potential vulnerabilities occasioned by the unique characteristics of IoT, such as the diversity of interconnected devices, large attack surface and often limited security features, resulting in critical cybersecurity concerns. Literature notes that the emergence of IoT has not been without associated challenges which confound the digital approach for measuring focal constructs. Howbeit, these concerns have also highlighted the need for robust cybersecurity measures to protect sensitive educational data.

Cybersecurity issues are not exclusively the concerns of tech experts, but a general issue for users of tech devices. The growing influx of IoT in educational assessment practices have likewise been visited with such cybersecurity challenges, due to the activities of cybercriminals who continue to adapt their strategies to the new environment. According to Robles et al. (2017); Domeij (2019), such activities result in the theft and destruction of many forms of educational assessment data, ranging from delicate information, personally identifiable information (PII), protected health and personal data, intellectual property data, data about assessment questions task sand outcome scores, and information systems used for the assessment purposes. Therefore, this increasingly calls on teachers and educational assessment experts to take decisive measures to effectively tackle cybersecurity concerns, create a safer cyberspace for fair assessments, and maintain the role of educational assessments.

The role of assessment is to support and guide teaching and learning, as well as to inform educational stakeholders about student performance and program effectiveness (Nworgu, 2016). Assessment is concerned with the process of gathering data from a variety of sources on the activities of teaching and learning for understanding, describing and improving learning (Oguguo et al., 2023). Mertler (2019) emphasized that the core mandate of assessment should focus on improving student learning and understanding. In addition, Hattie and Timperley (2007); Wiliam and Leahy (2015) emphasized the need for timely feedback to support learning progressions based on information gathered from assessments. Nworgu and Ellah (2015); Wiliam (2017) agree that assessment practices should be embedded in instructional activities to enhance student learning and understanding. Klenowski (2020) strongly emphasized the importance of assessment and promulgated a variety of assessment practices which could find relevance in the university learning spaces. Assessment helps to validate the effectiveness of the teaching and learning process and it points out students' strengths and areas requiring more attention (Oguguo et al., 2023).

1.1. Formative Assessment

Various scholars and educators view assessment practices from a mired of perspectives based on the purpose for which the assessment is necessary, but generally to measure student learning and understanding. Popham (2018); Herman et al. (2020) provides an overview of various approaches to assessment as well as practical guide on implementing effective assessment practices. Assessment practices may be formative, summative or authentic (Monteiro et al., 2021). Formative assessments are assessments for learning, which stem from the pedagogical pole and seek to improve learning (Brown & Remesal, 2017). Adikwu et al. (2014) described formative assessment as assessments performed during the course of instruction. Formative assessments are not only for students; however, they also provide teachers with actionable feedback to improve the instruction (Nworgu & Ellah, 2015). Assessment for learning is a useful tool in tracking the trend in students' learning while instruction is ongoing (Stiggins & Chappuis, 2020). Formative assessments are ongoing assessments which often take the form of quizzes or classroom discussions, and are used to diagnose student difficulties, identify areas where students may need additional support, guide instruction, monitor student progress and provide feedback to both the student and the teacher to modify teaching and learning strategies. Although, it requires investment of time, it can be gainful in enhancing the effectiveness of instruction.

1.2 Summative Assessment

Summative assessments are assessments of learning, and often take the form of final exams, standardized tests and end-of-unit projects. Assessments of learning proceed from the societal pole by providing an overall measure of student achievement, and are used to evaluate student learning at the end of a unit, course or school year (Brown & Remesal, 2017). Summative assessment is the form of assessment carried out after teaching is concluded (Adikwu et al., 2014). Summative assessments for learning are judgmental, often used for high-stakes accountability, ranking, grading, and/or certification purposes (Emaikwu, 2011). Assessment of learning is the cumulative evaluation of students' achievement after complete exposure to a sequence of instruction. The goal of assessment of learning is to communicate student level of achievement rather than to

specifically provide detail feedback about the learning process or suggesting problem areas, although students can receive the latter during the examination.

1.3 Authentic Assessment

Authentic assessments are assessments as learning, which often take the form of performance assessments, portfolios and project-based assessments. Authentic assessments measure students' abilities to apply their learning (knowledge and skills) in meaningful and relevant ways to real-world tasks and problems (Fuchs & Fuchs, 2017; Brookhart, 2019). Authentic assessment is an approach to evaluating student learning through real-world, relevant tasks and activities. Authentic assessment focuses on evaluating students' ability to apply their knowledge and skills in meaningful contexts to real practical experiences, rather than just regurgitating memorized facts (Yip, 2021). Sewagegn and Diale (2020) view authentic assessment as that assessment which enhances students' learning and makes them competent in their study area. Authentic assessments are assessments which connect theoretical knowledge with real life application with the view of evaluating students' ability to solve real world problems using the knowledge of their learning.

Assessment practice according to American Educational Research Association, American Psychological Association, & National Council on Measurement in Education (AER, APA & NCME, 2014); Pellegrino and Chudowsky (2018); Gamito et al. (2022); Darling-Hammond and Adamson (2020) emphasized that educators must enthrone the principles of assessment when designing and implementing assessment practices by ensuring that assessments are valid, reliable, fair, and equitable for all students. Given the caution, it behoves squarely on educators to employ means that administer assessments that accommodate the principles of validity, reliability, fairness and equality in testing, which digital technologies offer through the Internet of Things (IoT). The drift to IoT summarizes a wide range of physical objects embedded with sensors, software and other technologies, and networked over the internet to enable them to communicate, share and exchange data with one another, as well as other devices and systems. According to Bosche et al. (2018) noted that the adoption of IoT devices has continued to increase, nearly doubling yearly; and Darina (2023), 127 new IoT devices are connecting to the web every second, from the status of billions of active IoT devices since 2019. This may imply favorable satisfaction due to IoT, leading to its global expansion. The composition of IoT fuses the first principles from the fields of electronics, communication and computer science engineering in a spectrum of programmable devices that function efficiently enough to address the target essence for their built by creating a smart and connected environment.

1.4 Application of Internet of Things (IoT)

The Internet of Things (IoT) is a network of uniquely identifiable objects, ranging from everyday devices to sophisticated industrial tools, each equipped with sensors to gather and transmit data for various purposes, so that they communicate without human interaction through the use of embedded systems, either through the internet or other means of connectivity (Atzori et al., 2010). Kortuem et al. (2010) described the Internet of Things (IoT) as encompassing the integration of sensors and actuators into a wide range of devices connected by the use of networks to allow diverse objects to communicate and exchange information for the purpose of automation, monitoring, and control via data exchange and provision of various services to individuals and organizations. The major insight about IoT is simply the improvement of everyday objects with some identification, sensor, network and processing capabilities that will enable them to communicate with each other, as well as with other devices and services through the internet, according to Rakić (2023). Immediately after the upgrade, the regular objects become smart objects and become capable of generating, exchanging, collecting, analyzing and managing data with minimal or even no human intervention. The IoT encompasses the extension of Internet connectivity into physical devices and everyday objects; a collective network of interrelated devices and smart objects, and the technology that facilitates communication between them and other objects over the cloud. IoT encapsulates technology that allows us to add a device to an inert object to aid the measurement of environmental parameters, generate associated data and transmit the data through a communication network for others to access.

IoT can be effectively used in almost every facet of human life, including education. IoT has long been applied in the health sector as microchips and wearable devices such as fitness trackers and remote monitoring tools for collecting and analyzing data from patients for personalized healthcare to better manage chronic conditions (Iqbal & Qadir, 2021). IoT in healthcare integrates wearable devices, medical equipment and remote patient monitoring systems to gather health data, support telemedicine, and improve patient outcomes through continuous monitoring and personalized care (Rezaee et al., 2016; Catarinucci et al., 2015). This also covers consumer IoTs such as home appliances (including thermostats, lighting systems, and door locks), wearable devices (including fitness trackers, and smartwatches) and connected car technologies designed for personal use for improved convenience. Tao et al. (2018) pointed out that industrial IoT such as smart manufacturing systems, remote equipment monitoring, and asset tracking solutions focuses on the deployment of connected devices and sensors in industrial settings to optimize processes, monitor equipment performance and enable predictive maintenance. IoT is also applied in Agriculture through connected sensors, drones and automated machinery to monitor crop conditions,

optimize irrigation, monitor livestock and birds, and general farm management to improve farm productivity (Liu et al., 2018). Zanella et al. (2014) accounted that smart cities can also implement IoT by deploying of interconnected sensors, smart infrastructure and data analytics to enhance urban services, optimize traffic management, improve energy efficiency, and support environmental monitoring. Environmental IoT involves the use of connected sensors and monitoring devices to gather real-time data on air quality, water pollution, and weather conditions, enabling environmental monitoring and management systems (Perera et al., 2014).

1.5 Benefits of Internet of Things (IoT) in Assessment Practices in Education

Scholars have pointed out the beneficial impasse of IoT across the educational system, especially in university learning spaces for collecting and analyzing relevant data such as student learning behaviors, engagement levels and performance in real-time, thereby providing valuable insights to educators and administrators. IoT devices can track students' progress and customize learning materials according to individual needs, leading to improved learning outcomes and student engagement (Haque, 2019). Chen and Zhu (2019) pointed out that IoT devices can help teachers manage the classroom more effectively and teachers focus more on teaching and student interaction, by automating routine tasks such as attendance, grading and classroom organization. Rifkin (2019) argues that IoT devices can also be used to ensure and monitor the safety of staff and students on campus by identifying potential threats, tracking movement and alerting authorities in case of emergencies. IoT devices in the form of extended realities can be used to connect students to a pseudo-real-world experience through virtual realities to access risky locations remotely, expel experimental or real-world hazards and make learning more relevant and engaging (Agah et al., 2023). In addition, since IoT devices are automated by programming, they can be used to streamline administrative processes such as resource management, scheduling and facility maintenance, leading to improved efficiency and cost savings in educational institutions. The growing penetration of IoT in the educational sector cuts across its length and breadth, and is finding more relevance in educational assessment practices in university learning spaces due to the strategic role of higher education in nation-building. The IoT provides an opportunity for smart campuses across university learning spaces (Gikas & Grant, 2013; Le et al., 2020; Chen et al., 2021).

Literature affirms the significant role of IoT in educational assessment practices in university learning spaces by providing valuable data and insights into student performance, behavior, and learning environments (Blikstein, 2020; Al-Zou'bi, 2021; Mishra et al., 2021; Jiménez Sabino & Cabero Almenara, 2021; Valverde et al., 2021). For example, IoT sensors placed on desks and strategic places in the smart classroom can track students' attendance, movements, interactions and engagements with learning materials, and detect when students are participating actively in discussions or group activities by measuring movement and noise levels (Premalatha & Krishnan, 2020). This data can help provide teachers with valuable data to identify students who may need extra support or encouragement and inform teaching strategies. IoT-enabled smart pens and notebooks used in smart schools can record students' notes, sketches, and annotations during assessments (Wadowsky, 2023). These devices can analyze handwriting, note-taking patterns, and time spent on different sections to provide feedback on students' comprehension, study habits and suggest ways for students to improve their note-taking techniques or highlight key concepts they may have missed during a lecture. Also, IoT devices are used to monitor online exams and remote assessments to ensure academic integrity based on facial recognition technology in which students' identities are verified and eye-tracking or keystroke analysis can detect any irregularities during the assessment (Oncul, 2021). IoT devices can track and monitor students' progress by collecting real-time data on student engagement, behavior, and performance to identify areas for improvement (Nguyen Gia & Tam, 2020), since Reeve (2019) already highlights the interconnections of assessment practices with student engagement and psychological factors. Likewise, Kadam and Kadam (2017) opine that the data collected through IoT devices can become helpful to tailor instruction and assessment to meet each student's specific needs through personalized learning experiences that suit individual student preferences, learning styles, and performance. Data collected through IoT sensors can also help in creating more conducive learning spaces which optimizes assessment conditions by monitoring environmental factors, such as temperature, noise levels and air quality, which may be capable of impacting students' learning and performance (Spikol, 2018). Chappuis and Stiggins (2019) emphasis the importance of student involvement in assessment for which evidence shows that the practice enhances learning and understanding; and impacts on raising classroom standards (Black et al., 2019). Islam (2019) also pointed out that IoT data can be analyzed using machine learning and predictive analytics to identify patterns and trends in student performance. This information can help educators make informed decisions about assessment strategies and interventions for support. Brookhart (2018) believes that incorporating classroom assessment practices into instruction can improve higher-order thinking in students; and provide teachers with valuable information to inform their instruction (Chappuis, 2015). IoT devices are capable of sending and receiving data and can provide real-time feedback to both students and teachers, giving room for immediate identification of students' learning needs, adjustments and interventions for support (Datta, 2019). This real-time engagement is made possible over cyberspace.

1.6 IoT Cybersecurity in Educational Assessment

The impasse of the cyberspace over which the IoT operates presents us with unique challenges, some of which can be intentionally damaging with grave consequences. Projected to hit 75 billion IoT devices by 2025 (Fernandez-Carames & Fraga-Lames, 2020), an IoT global data collection of 73.1 zettabytes by 2025 (Bojan, 2022) and approximately 125 billion devices by 2030 (Jenalea, 2017), the worry has now drifted to cybersecurity, the securing of IoT in cyberspace. Cybersecurity is the state of being safe from, and the measures taken to forestall criminal or unauthorized use of electronic data and devices (Rahman et al., 2020). The Department of Homeland Security (DHS, 2014) defined cybersecurity as the activity, process, ability or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized modification, exploitation or use. Oguguo and Ocheni (2023) defined cybersecurity in educational assessment as security breaches in assessment over cyberspace. From the foregoing, it may be deduced that the essentials of cybersecurity are the securing and protection of data, devices and people connected in cyberspace. Therefore, IoT cybersecurity (IoTCS) can be seen as measures that ensure the safety of data, systems and people connected over the internet network through various IoT devices. The credibility of the security level of IoT devices is crucial in securing the IoT devices, however, it is difficult to ratify an acceptable IoT standard due to the heterogeneous and dynamic nature of the IoT devices (Matheu et al., 2019), which poses a significant challenge to the adoption of IoT in educational assessment issues. Educational assessments are serious businesses that cannot afford to entertain activities that mar the validity or reliability of its outcomes. Todorov and Vela (2023) identify cybersecurity issues as an important challenge in the integration of IoT in education, and assessment.

Scholars have identified several cybercriminal activities involving IoT in assessment practices. Oguguo and Ocheni (2023) revealed that hacking into assessment systems and websites to alter assessment scores, colluding via social media, phishing of login credentials or other assessment-sensitive materials to gain access or cheat on assessments via phishing links, using man-in-the-middle (MITM) attack are some of the cyberattacks on educational assessments. Other assessment cybersecurity issues include impersonating with the use of fake identities to take exams on behalf of other students, the deployment of ransomware to encrypt or disrupt the assessment system until demands are met, peer collaboration to cheat or plagiarize the assessment by accessing unauthorized information during assessment via using IoT devices, sharing or selling assessment questions with other students prior or during assessment through using IoT devices, bullying, harassing or intimidating teachers and students through IoT cyberspace to affect performance in the assessment, distributing malware and lunching of IoT denial of service attacks to flaw the assessment processes, distributing fake academic credentials, among others. These criminal activities in IoT cyberspace compromise the integrity of the assessment processes and require strict vigilance and implementation of strong cybersecurity measures by the lecturers and administrators in university learning spaces to curb the menace.

Several IoTCS tools have been tested and implemented in various sectors of society, some of which have proved effective for the purposes they were adopted. Among so many of them are Fore scout, Armis, Claroty, Check Point IoT Security, Trustwave IoT Security, Bastille, McAfee MVISION Endpoint, CyberX, NXM S.T.A.T, Zingbox, Amazon Web Service (AWS) IoT device defender, Broadcom, IoT Secure, Palo AltoNetworks, Entrust Authority, ForgeRock, DigiCert IoT Trust, Ordr, Asimily, Audra Homeshild Dotlines, Axonius Cybersecurity Asset Management, Sepio, Caarwall, Intel Enhanced Infrastructure Protection, Intel IoT Gateway Security, Pwine Express Pulse IoT Security, Karamba Security, Fortrust Cyber MDX, Tempered, Securithings, Sectrio, Overwatch, NanoLock, ForitNAC, FirstPoint, Cisco IoT Security, Azure IoT, Atonomi, Bastile, Trustwave, SensorHound, Google CloudIoT, Shodan (Fernandez-Carames & Fraga-Lames, 2020; Zakariyya, Kalutarage & Al-Kadri, 2023) among others. Eleje,et al. (2022) found that cybersecurity problems negatively influenced digital assessment. According to Oluga et al. (2014); AlSalem, et al. (2023); and Triplett, et al. (2023), cybersecurity issues are a serious challenge to the effectiveness of IoT for the purposes designed, and may influence assessment practices. However, Kandasamy, et al. (2020); and Lee (2020) have pointed out the paucity of research on the bearing of IoT cybersecurity for assessment practices, although IoT plays amazing roles in educational assessment. Owing to the numerous possibilities, convenience and efficiency IoT provides for assessment practices, the cybersecurity issues associated with the IoT cannot be overlooked. Therefore, the study investigated the impact of IoTCS on educational assessment practices in university learning spaces. The following specific issues were addressed:

1. What is the influence of IoT cybersecurity on the effectiveness of formative assessment practices in university learning spaces?
2. What is the influence of IoT cybersecurity on the effectiveness of summative assessment practices in university learning spaces?
3. What is the influence of IoT cybersecurity on the effectiveness of authentic assessment practices in university learning spaces?
4. What is the influence of IoT cybersecurity on the effectiveness of assessment practices in university learning spaces?

2. Materials and Methods

Correlation research design was adopted for this study which determined the impact of Internet of Things (IoT) Cybersecurity on educational assessment practices in university learning spaces. The research design explores the relationship between two or more variables in a study (Nworgu, 2015). The study was conducted in six universities in South-East, Nigeria, which comprised of Alex Ekwueme Federal University, Ndufu-Alike, Ikwo (AE-FUNAI); Alvan Ikoku Federal University of Education, Owerri (AIFUEO); Federal University of Technology, Owerri (FUTO); Michael Okpara University of Agriculture, Umudike (MOUAU); Nnamdi Azikiwe University, Awka (NAUA); and University of Nigeria, Nsukka (UNN). The study sampled 297 lecturers from the universities in the South-East, Nigeria. Multistage sampling procedure was adopted to recruit 297 (male = 202 and female = 95) respondents who participated in the study. The lecturers that participated in the study had between five and 30years of teaching experience. First, disproportionate stratified sampling technique was adopted to determine the proportion of university lecturers to be drawn from each university in the South-East. Simple random sampling technique was further applied in each stratum to select 40, 45, 58, 48, 40 and 68 lecturers from each of the six universities. Then, the researchers randomly sampled six Faculties in each university using simple random sampling procedure by balloting without replacement.

The instruments for data collection were two researchers developed four-point Likert scale questionnaire titled Internet of Things Cybersecurity Questionnaire (IoTCSQ) and Assessment Practices Scale (APS). The IoTCSQ consist of two sections (Section A elicited demographic data of the respondents while Section B holds the 12-item statements which sought to elicit information on IoT Cybersecurity tools and devices available at the disposal of the lecturers in university learning spaces). The APS consists of two sections (Section A elicited demographic information of the respondents, while Section B contains three clusters, A, B and C hold 8-item statements each on Formative, Summative and Authentic assessments, respectively, 24 items in all which sought to elicit information on respective assessment practices adopted by the lecturers in the university learning spaces). Both instruments were designed to elicit participants responses towards addressing the research issues raised for the study. The items of the instruments (IoTCSQ and APS) were validated in line with the purpose of the study by three experts in the area. Their suggestions and recommendations were incorporated into the final version of the instrument. Data collected from trial testing of the two instruments (IoTCSQ and APS) showed evidence of normality by Shapiro-Wilk test p-values of 0.34 and 0.95 respectively and then were subjected to Cronbach Alpha reliability test, IoTCSQ has a reliability index of 0.82 while the overall reliability index of APS was 0.85, and clusters A, B and C had reliability indices of 0.81, 0.92 and 0.84 respectively.

The instruments, IoTCSQ and APS were distributed by the faculty Deans to the sampled lecturers in the sampled faculties who served as research assistants after briefing on the purpose of the study. The instruments were retrieved from the Deans after the subjects had attended to them for analysis. Data was analyzed using SPSS v.25, and the research questions were addressed using Pearson Product Moment Correlation and Coefficient of Determination. The criterion adopted for interpreting the result was according to Schober and Boer (2018) which considered absolute values of correlation coefficient below 0.1 as negligible, 0.1-0.39 as weak, 0.40-0.69 as moderate, 0.70-0.89 as strong while 0.90-1.00 as high relationships.

3. Results

3.1 Participants Statistics

Figure 1 shows the population distribution of male and female lecturers in the South-East universities. The chart shows that males are more in number than females among lecturers in all the federal universities in South-East, Nigeria. This implies that the responses of the male lecturers could largely infer the influence of IoT Cybersecurity on the effectiveness of formative, summative and authentic assessment practices in university learning spaces since they have a larger population. The chart also shows that UNN has more lecturers among the six federal universities in South-East, Nigeria.

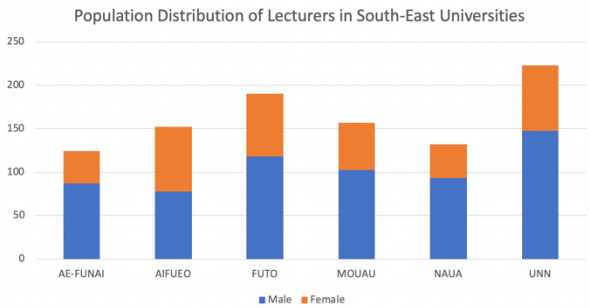

Figure 1 - Population Distribution of Lecturers in South-East Universities.

3.2 IoT Cybersecurity on the Effectiveness of Formative Assessment Practices

Table 1 shows a moderate positive relationship between the incorporation of IoTCS and the effectiveness of formative assessment practice (r = 0.52). The result also shows a coefficient of determination of 0.2704, implying that the opinion of lecturers on the adoption of IoTCS explains 27.04% of the variation in formative assessment in university learning spaces.

3.3 Integration of IoT Cybersecurity in Summative Assessment Practices

The result in Table 2 shows a strong positive relationship between the incorporation of IoTCS and the effectiveness of summative assessment practices in university learning spaces (r = 0.70). With a coefficient of determination of 0.49, it implies that the adoption of IoTCS in the opinion of the lectures explains 49% of the variation in summative assessment in university learning spaces.

3.4 IoT Cybersecurity and Authentic Assessment Practices

The result in Table 3 shows a moderate positive relationship between the incorporation of IoTCS and the effectiveness of authentic assessment practices in university learning spaces (r = 0.41). The result also shows a coefficient of determination of 0.1681, implying that lecturers' adoption of IoTCS explains about 16.81% of authentic assessment in university learning spaces.

Table 1 - Integration of IoT in formative assessment practices in university learning spaces.

	r	r^2
IoT*FA	0.52	0.2704
r = Pearson's Correlation coefficient r^2 = Coefficient of Determination		

Table 2 - Integration of IoT in summative assessment practices in university learning spaces.

	r	r^2
IoT*SA	0.70	0.4900
r = Pearson's Correlation coefficient r^2 = Coefficient of Determination		

Table 3 - Integration of IoT in authentic assessment practices in university learning spaces.

	r	r^2
IoT*AA	0.41	0.1681
r = Pearson's Correlation coefficient r^2 = Coefficient of Determination		

3.5 IoT Cybersecurity on the Effectiveness of Assessment Practices

The result in Table 4 shows a moderate positive relationship between the incorporation of IoTCS and the joint effectiveness of assessment practices in university learning spaces (r = 0.62). The coefficient of determination of 0.3844, implies that the adoption of IoTCS by lecturers explains about 38.44% of assessment practices (the joint of formative, summative and authentic assessments) in university learning spaces.

Table 4 - Integration of IoT in assessment practices in university learning spaces.

	r	r^2
IoT*JAP	0.62	0.3844
r = Pearson's Correlation coefficient r^2 = Coefficient of Determination		

From Table 5, the F-ratio of 185.487 with an associated probability value of 0.000 was obtained for the incorporation of IoTCS and the effectiveness of assessment practices in university learning spaces. The associated probability value was found to be significant because 0.00 is less than 0.05 (the level of significance) when compared for testing the hypothesis. Therefore, the null hypothesis which stated that the influence of IoT cybersecurity on the effectiveness of assessment practices in university learning spaces is not significant was rejected. Hence, it is inferred that IoT cybersecurity adoption significantly influences the effectiveness of assessment practices in university learning spaces.

4. Discussion

The result of this study shows that the opinion of lecturers depicts a moderate positive relationship between the incorporation of IoTCS and the effectiveness of formative assessment practice. This finding suggests that IoTCS influences the effectiveness of formative assessments by preventing the threats on IoT devices for students to receive instant feedback that strengthens continuous and personalized learning.

This may be plausible because IoTCS technology can detect and intercept activities of malware, ransomware and other tools that endanger the data and effectiveness of IoT devices on the network during the assessment, so the assessment practice intended to provide the opportunity for the collection of real-time data and personalized feedback to students based on student progress is not distorted. However, this moderate relationship may have sufficed because most lecturers pay less attention to formative assessment practices in most Nigerian university learning spaces which may have graced their opinions about the influence of

Table 5 - ANOVA of the integration of IoT in assessment practices in university learning spaces.

		Sum of squares	Df	Mean square	F	Sig.
1	Regression	18942.380	1	18942.380	185.487	.000[b]
	Residual	30126.051	295	102.122		
	Total	49068.431	296			
a. Dependent Variable: Joint Assessment Practices b. Predictors: (Constant), Internet of Things Cybersecurity						

cybersecurity on the effectiveness of formative assessments. This finding is in line with the findings of Chelliah et al. (2017); Pollock and Satterthwaite (2018); Misra and Pal (2019); Lee (2020); Eleje et al. (2022); and Oguguo and Ocheni (2023).

We discovered a strong positive relationship in the opinion of lecturers between the incorporation of IoTCS and the effectiveness of summative assessment practice. This finding suggests that IoTCS provides confidence in the automated real-time data collection and analysis of students' achievement, leading to improved efficiency and objectivity in trust in the outcome of end-of-course assessments, although most hackers target this final assessment. This implies that IoTCS can enable the effective collection of diverse data that can be relied upon for comprehensive and holistic assessment of students' achievement. The strong positive relationship between the adoption of IoT and the effectiveness of summative assessment practices in university learning spaces may have turned out so because the emphasis has always been on the final examinations which often hold the largest chunk of scores, for which society attaches more relevance (Sewagegn & Diale, 2020) therefore, the tendency of protecting it from malicious activities is high. This finding agrees with the findings of Chalmers et al. (2017); Papapanagiotou et al. (2017); Sharma and Jain (2019); Kandasamy, et al. (2020); Eleje et al. (2022); and Oguguo and Ocheni (2023).

The result further revealed that the opinion of lecturers shows a moderate positive relationship between the incorporation of IoTCS and the effectiveness of authentic assessment practices in university learning spaces. This finding indicated that IoTCS contextual data collection can be defended in real time, leading to trustworthy data from real-world implications of meaningful learning. This result may also have turned out so because the assessment practices in most developing countries like Nigeria seldom focus on meaningful contexts that solve real-world problems, therefore the rate of defending the same by adopting IoTCS is expectedly relative. This finding supports the reports of Borges and Sthel (2018); Tom Dieck, and Jung (2018); and Alivernini et al. (2020); Kandasamy, et al. (2020); Eleje et al. (2022); and Oguguo and Ocheni (2023).

There was a moderate positive relationship between the adoption of IoTCS and the joint of formative, summative and authentic assessment practices in university learning spaces based on the opinion of lecturers. This moderate positive relationship was found to significantly influence assessment practices in university learning spaces. This result may have been plausible since more studies advocate the extension of cybersecurity in assessment practices to mitigate the challenges posed by cybercriminals which cannot be patronized over the many conveniences and possibilities of IoT assessment practices in university learning spaces as accounted by (Al-Zou'bi, 2021; Valverde et al., 2021). The findings of this study are consistent with the views of Oluga, et al. (2014); Chen and Zhu (2019); Le et al. (2020); Chen et al. (2021); Monteiro et al. (2021); Eleje, et al. (2022); Triplett (2023); and Oguguo and Ocheni (2023), to the extent that the integration of IoT influences assessment practices in university learning spaces.

5. Conclusions

Assessment has over time been an integral component of the educational system, with practices varying from the traditional summative form to the learning-informed assessment perspective. The influx of technology has been accompanied by advances in internet access enabling almost any object to share resources online in real time. The Internet of Things (IoT) presents a unique flexibility that injects more productivity and powers the previously impossible with less effort, even in facets of the educational sectors. However, the wave of cyberattacks experienced over the internet has not spared the IoTs wherever they are adopted, even in educational assessment practices. Evidence from this study shows that the opinion of the lecturers on the adoption of IoT Cybersecurity (IoTCS) can significantly influence the effectiveness of assessment practices in university learning spaces. Given the foregoing, it has become necessary for the university learning spaces to incorporate IoTCS tools into their assessment systems to improve the fairness and reliability of the data collected and the feedback generated by the IoT devices used in such assessment practices. Also, the fact suffices that if lecturers feel safe with the assessment tools used from a cybersecurity perspective, they could use a variety of teaching and assessment solutions, including online or at a distance. However, the novelty of IoT and the huge cybersecurity implications associated with Nigeria's educational system if not intercepted has prompted this study which the researchers hope would engender further exploration of the IoTCS issues for educational assessment practices in university learning spaces. Based on the findings of the study, the following recommendations were made.

1. School administrators should consider investing in IoT cybersecurity for the safety, fairness and reliability of assessment data.
2. The government should partner with tech agencies to provide special training and services for university lecturers for the detection of IoT vulnerabilities.
3. University lecturers should encourage the adoption of IoT cybersecurity measures in assessment practices in university learning spaces.
4. Due to the cost implications involved in opting for IoTcybersecurity tools, the government should fund universities to afford the same in their learning spaces.
5. Educational policies should strengthen the incorporation of IoTCS in assessment practices in university learning spaces.

References

Adikwu, O., Obinne, A. D. E. & Amali, A. O. (2014). Challenging Factors in Educational Assessment in Nigerian Secondary Schools. *Asian Journal of Education and e-Learning, 2*(3), 219-224

Agah, J. J., Nnaji, A. D. & Nwani, S. U. (2023). *Virtual and Augmented realities as Determinants of Students' Engagement in Test Development*. 9th Conference of Educational Assessment and Research Network in Africa (EARNiA).

Alivernini, F., Manganelli, B., Pontarelli, V., & Persico, D. (2020). IoT technologies for implementing Augmented Reality and Virtual Reality ecosystems in authentic learning contexts. *Telematics and Informatics, 51*, 101413.

AlSalem, T. S., Almaiah, M. A., & Lutfi, A. (2023).Cybersecurity Risk Analysis in the IoT: A Systematic Review. *Electronics, 12*, 1-19 3958. https://doi.org/10.3390/electronics12183958

Al-Zou'bi, M. (2021). The role of the Internet of Things (IoT) in shaping the education sector post COVID-19. *Education and Information Technologies,* 1-30.

American Council on Education. (2017). Internet of Things Insights: Smart Campuses of the Future.

American Educational Research Association, American Psychological Association, & National Council on Measurement in Education. (AERA, APA & NCME, 2014). *Standards for educational and psychological testing.* Washington, DC: American Educational Research Association.

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A Survey. Computer Networks, 54(15), 2787-2805. https://doi.org/10.1016/j.comnet.2010.05.010

Black, P., Harrison, C., Hodgen, J., Marshall, B., & Serret, N. (2019). *Inside the Black Box: Raising Standards Through Classroom Assessment*. London, UK: GL Assessment.

Blikstein, P. (2020). Educational data science: New technologies, new data sources, and new education research paradigms. *AERA Open, 6*(2), 1-14.

Bojan, J., (2022). Internet of things statistics for 2022 – taking things apart. https:// dataprot .net /statistics /iot -statistics/

Borges, M.R., & Sthel, M.S. (2018). *The Internet of Things in Education: The Inclusion of Authentic Assessment and the Development of Content.* In Proceedings of the Future Technologies Conference (FTC) 2018 (pp. 618-627). Springer, Cham.

Bosche, A., Crawford, D., Schallehn, M. & Schorling, C. (2018). *Unlocking Opportunities in the Internet of Things: Vendors can improve the market by addressing customer concerns over security, integration and returns on investment.* Bain and Company. Retrieved from https://www.bain.com/insights/unlocking-opportunities-in-the-internet-of-things/

Brookhart, S. M. (2019). *How to Assess Student Performance: Written and Oral Communications Skills (2nd edition)*. Alexandria, VA: ASCD.

Brown, G.T.L., & Remesal, A. (2017). Teachers' conceptions of assessment comparing two inventories with Ecuadorian teachers. Stud. Educ. Eval. 55, 68-74. https://doi.org/10.1016/j.stueduc.2017.07.003

Catarinucci, L., de Donno, D., Mainetti, L., Palano, L., Patrono, L., & Stefanizzi, M. L. (2015). An IoT-Aware Architecture for Smart Healthcare Systems. *IEEE Internet of Things Journal, 2*(6), 515-526. https://doi.org/10.1109/JIOT.2015.2425901

Chalmers, C., Singh, J., & Chen, T. (2017). *Big Data, IoT and Smart Learning in Education.* In Proceedings of the 3rd International Conference on Big Data Innovations and Applications (pp. 367-372). Springer, Singapore.

Chappuis, J. (2015). *Seven Strategies of Assessment for Learning (2nd edition).* Boston, MA: Pearson.

Chappuis, J., & Stiggins, R. (2019). *An Introduction to Student-Involved Classroom Assessment.* Portland, OR: Pearson.

Chelliah, S., Devasenapathy, S. & Kannan, T. (2017). Internet of Things in Education: A Review. *International Journal of Research in Engineering and Technology, 6*(8), 88-92.

Chen, X., & Zhu, Y. (2019). "Application of IoT Technology in the Smart Classroom." Retrieved from https://link.springer.com/chapter/10.1007/978-3-030-33206-1_19

Chen, Y., Qiu, M., Jiang, C., Yin, Y., & Yu, F. (2021). Enabling Smart Campus through Internet of Things. *IEEE Communications Magazine, 59*(1), 144-150.

Darina, L. (2023). *IoT Statistics and Trends to Know in 2023*. Retrieved from https://leftronic.com/blog/internet-of-things-statistics/

Darling-Hammond, L., & Adamson, F. (2020). Assessment to Support Equity. In D. L. McLaughlin & J. E. Talbert (Eds.), *Leading for Powerful Learning: A Guide for Instructional Leadership* (pp. 185-206). San Francisco, CA: Jossey-Bass.

Datta, S. K. (Ed.). (2019). *IoT in Education: Smart Infrastructure and Applications*. CRC Press.

DHS. (2014). *A glossary of common cybersecurity terminology*. National Initiative for Cybersecurity Careers and Studies: Department of Homeland Security. Retrieved from http://niccs.uscert.gov/glossary

Domeij, T. (2019). K-12 cybersecurity program evaluation and its application. *Bachelor's project, Bridgewater State University*. Virtual Commons. Retrieved from https://vc.bridgew.edu/honors_proj/366

Eleje, I. L., Metu, I. C., Ikwelle, A. C., Mbelede, N. G, Ezeugo, N. C., Ufearo, F. N., Okenwa-Fadele, I. A. & Ezenwosu, N. E. (2022). Influence of Cyber-security Problems in Digital Assessment on Students' Assessment Outcome: Lecturers' Perspective. *Journal of Scientific Research & Reports, 28(10): 11-20*

Emaikwu, S. O. (2011). *Fundamental of Test, Measurement and Evalaution with psychometric Theories.* Makurdi: Selfers Academic Press.

Fernandez-Carames, T. M., & Fraga-Lames, P. (2020). Teaching and learning IoT cybersecurity and vulnerability assessment with Shodan through practical cases. *Sensors, 20*, 1-25

Fuchs, L. S., & Fuchs, D. (2017). *Assessment for Reading Instruction (3rd edition)*. New York, NY: Guilford Press.

Gamito, R., Aristizabal, P., Basasoro, M. & León, I. (2022). The development of computational thinking in education: Assessment based on an experience with Scratch. *Innoeduca. International Journal of Technology and Educational Innovation, 8*(1), pp. 59-74 - ISSN: 2444-2925 DOI: https://doi.org/10.24310/innoeduca.2022.v8i1.12093

Gikas, J., & Grant, M. M. (2013). Mobile computing devices in higher education: Student perspectives on learning with cellphones, smartphones & social media. *The Internet and Higher Education, 19*, 18-26.

Haque, A. (2019). "Internet of Things (IoT) in Higher Education." Retrieved from https://doi.org/10.5281/zenodo.3997154

Hattie, J., & Timperley, H. (2007). The Power of Feedback. *Review of Educational Research, 77*(1), 81-112.

Herman, J. L., Osmundson, E., & Dietel, R. (Eds.). (2020). *Perspectives on Educational Assessment: Rethinking Assessment and Its Impact*. Cambridge, MA: Harvard Education Press.

Iqbal, M. H., & Qadir, J. (2021). Internet of Medical Things (IoMT) to Aid in Pandemics like Covid-19. *International Journal of Advanced Computer Science and Applications, 12*(1), 53-59.

Islam, M. R. (2019). Internet of Things in Education: A Systematic Mapping Study. *International Journal of Advanced Computer Science and Applications, 10*(6), 441-449.

Jenalea, H., (2017). Number of connected IoT devices will surge to 125 billion by 2030, HIS markit says. https://news .ihsmarkit .com /prviewer /release _only /slug /number - connected -iot -devices -will -surge -125 -billion -2030 -ihs -markit -says.

Jiménez Sabino, M. J., & Cabero Almenara, J. (2021). The technological, pedagogical and content knowledge of Andalusian university professors on ICT. Analysis from the TPACK model. *Innoeduca. International Journal of Technology and Educational Innovation, 7*(1), 4-18 https://doi.org/10.24310/innoeduca.2021.v7i1.11940

Kadam, S., & Kadam, P. (2017). Role of the Internet of Things in Education. *International Conference on I-SMAC (IoT in Social, Mobile, Analytics, and Cloud) (I-SMAC). IEEE,* 489-493

Kandasamy, K., Srinivas, S., Achuthan, & Rangan, V. P. (2020). IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. *EURASIP J. on Info. Security 2020,* 8 https://doi.org/10.1186/s13635-020-00111-0

Klenowski, V. (Ed.). (2020). *Assessment for Learning and Teaching in Primary Schools*. London, UK: Routledge.

Kortuem, G., Kawsar, F., Sundramoorthy, V., & Fitton, D. (2010). Smart Objects as Building Blocks for the Internet of Things. *IEEE Internet Computing, 14*(1), 44-51. https://doi.org/10.1109/MIC.2010.21

Le, N. T., Nouanthavong, S., & Hwang, D. (2020). Internet-of-Things (IoT) for Smart Classroom Management. *Journal of Computers in Education, 7*(3), 369-388.

Lee, I. (2020). Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. *Future Internet. 12*(9):157. https://doi.org/10.3390/fi12090157

Liu, B., Tang, S., You, X., Wang, G., & Luo, J. (2018). Agriculture 4.0: A Review. *Computers and Electronics in Agriculture, 143*, 98-110. https://doi.org/10.1016/j.compag.2017.11.018

Matheu, S. N., Hernandez-Ramos, J. L., & Skarmeta, A. F. (2019).Toward a cybersecurity certification framework for the Internet of Things. *IEEE Secur. Priv., 17*, 66–76.

Mertler, C. A. (2019). *Classroom Assessment: A Practical Guide for Educators*. New York, NY: Routledge.

Mishra, D., Singh, J., & Agarwal, A. (2021). Role of Internet of Things in Reshaping Educational Framework in Indian Universities Post COVID-19. *IEEE International Conference on Electron Devices and Solid-State Circuits (EDSSC)*, 1-4.

Misra, S. & Pal, S. (2019). Internet of Things in Education: A Systematic Mapping Study. *International Journal of Information and Education Technology, 9*(9), 605-609.

Monteiro, V., Mata, L. & Santos, N. N. (2021). Assessment Conceptions and Practices: Perspectives of Primary School Teachers and Students. *Front. Educ*. 6:631185. doi: 10.3389/feduc.2021.631185

Nguyen Gia, T., & Tam, V. (Eds.). (2020). *Internet of Things and Smart Education in Digital Age.* Springer.

Nworgu, B. G. (2015). *Educational Measurement and Evaluation Theory and Practice*. Nsukka-Enugu, University Trust Publishers.

Nworgu, B. G. (2016). Averting Pedagogical Failure in Science: Insight from Educational Measurement and Evaluation. *103rd Inaugural Lecture of the University of Nigeria*. *Nsukka-Enugu, University of Nigeria*.

Nworgu, L. N. & Ellah, B. O. (2015). Teachers Practice of School-Based Assessment (SBA) Techniques in Science Classes. *International Journal of Educational Research, 14*(2), 242-251, https://ssrn.com/abstract=2888858

Oguguo B. C. E, Ezechukwu R. I, Nannim F. A & Offor K. E. (2023). Analysis of teachers in the use of digital resources in online teaching and assessment in COVID times. *Innoeduca. International Journal of Technology and Educational Innovation. 9*(1), 81-96 https://doi.org/10.24310/innoeduca.2023.v9i1.15419

Oguguo, B. C. E. & Ocheni, C. A. (2023). Cybersecurity: a tool for curbing examination breaches and improvement of the quality of large-scale educational assessments, *Information Security Journal: A Global Perspective*, https://doi.org/10.1080/19393555.2023.2284761

Oluga, S. O., Ahmad, A. B. H., Alnagrat, A. J. A., Oluwatosin, H. S., Sawad, M. A. O., & Muktar, N. A. B. (2014). An Overview of Contemporary Cyberspace Activities and the Challenging Cyberspace Crimes/Threats. *International Journal of Computer Science and Information Security (IJCSIS), 12*(3), 62-100

Oncul, B. (2021). Dealing with Cheating in Online Exams: A Systematic Review of Proctored and Non-Proctored Exams. International Technology and Education Journal, 5(2), 45-54 https://files.eric.ed.gov/fulltext/EJ1338047.pdf

Papapanagiotou, P., Li, S., & Ni, Q. (2017). *The Future of IoT in Education and its Impact on Assessment: A Review.* 2017 IEEE 15th International Conference on Industrial Informatics (INDIN), 474-479.

Pellegrino, J. W., & Chudowsky, N. (Eds.). (2018). *Knowing What Students Know: The Science and Design of Educational Assessment.* Washington, DC: National Academies Press.

Perera, C., Zaslavsky, A., Christen, P., & Georgakopoulos, D. (2014). Sensing as a Service Model for Smart Cities Supported by Internet of Things. *Transactions on Emerging Telecommunications Technologies, 25*(1), 81-93. https://doi.org/10.1002/ett.2705

Pollock, L. & Satterthwaite, H. (2018). The Impact of the Internet of Things on Formative Assessment in Education. *International Journal of Information and Education Technology, 8*(5), 376-380.

Popham, W. J. (2018). *Classroom Assessment: What Teachers Need to Know (8th ed.).* Boston, MA: Pearson.

Premalatha, B., & Krishnan, J. H. (2020). IoT Based Smart Classroom. *International Journal of Scientific & Technology Research, 9*(2), 1644 – 1650. http://www.ijstr.org/final-print/feb2020/Iot-Based-Smart-Classroom.pdf

Rahman, N. A. A., Sairi, I. H., Zizi, N. A. M., & Khalid, F. (2020). The Importance of Cybersecurity Education in School. *International Journal of Information and Education Technology, 10*(5), 378-382.

Rakić, K. (2023). Internet of Things in Education: Opportunities and Challenges. In: Vasić, D., Kundid Vasić, M. (eds) Digital Transformation in Education and Artificial Intelligence Application. MoStart 2023. Communications in Computer and Information Science, vol 1827. Springer, Cham. https://doi.org/10.1007/978-3-031-36833-2_8

Ramlowat, D. D., & Pattanayak, B. K. (2019). Exploring the Internet of Things (IoT) in Education: A Review. In: Satapathy, S., Bhateja, V., Somanah, R., Yang, XS., Senkerik, R. (eds) Information Systems Design and Intelligent Applications. Advances in Intelligent Systems and Computing, vol 863. Springer, Singapore. https://doi.org/10.1007/978-981-13-3338-5_23

Reeve, J. (2019). *Understanding Motivation and Emotion.* Hoboken, NJ: Wiley.

Rezaee, M., Basiri, A., Aung, Z., Musavian, L., & Nallanathan, A. (2016). A Survey on Indoor Positioning Systems and Context-Aware Methods in Healthcare. *IEEE Communications Surveys & Tutorials, 18*(3), 1975-2003. https://doi.org/10.1109/COMST.2016.2535040

Rifkin, J. (2019). "The Internet of Things and the Future of Education." Retrieved from https://www.edweek.org/technology/the-internet-of-things-and-the-future-of-education/2019/11

Robles, G., Wamba, S. F., & Akter, S. (2017). The role of IoT in education: a systematic literature review. *Computers in Human Behavior, 72*, 577-589.

Schober, P. & Boer, C. (2018). Correlation Coefficients: Appropriate Use and Interpretation. *Anesthesia and Analgesia,126*(5), 1763-1769.

Sewagegn, A. & Diale, B. M. (2020). Authentic assessment as a Tool to Enhance Student Learning in a Higher Education Institution: Implication for Student Competency. 256-271. DOI: 10.4018/978-1-7998-2314-8.ch013

Sharma, P., & Jain, S. (2019). *Internet of Things and Big Data Analytics in Education.* In Internet of Things and Big Data Technologies for Next

Generation Healthcare (pp. 89-104). Springer, Singapore.

Sheng, Q. Z., Zhang, L. J., & Yao, L. (2018). The Internet of Things for education: A brief survey. IEEE/CAA Journal of AutomaticaSinica, 5(1), 37-44.

Spikol, D. (2018). Using the Internet of Things in Education: A Connectivist Approach. In I. Aedo, J. Meyr, & B. P. K. Macías (Eds.), *Interactivity, Game Creation, Design, Learning, and Innovation* (pp. 435-439). Springer.

Stiggins, R. J., & Chappuis, J. (2020). *Assessment FOR Learning: An Action Guide for School Leaders (4th edition)*. Portland, OR: Assessment Training Institute.

Tao, F., Cheng, J., Qi, Q., Zhang, M., Zhang, H., & Sui, F. (2018). Digital Twin-Driven Smart Manufacturing. *Journal of Manufacturing Systems, 48*, 157-169. https://doi.org/10.1016/j.jmsy.2018.08.005

Todorov, T., & Vela, P. (2023). Internet of Things in Education, *Science Series "Innovative STEM Education", 5*, 193-200, https://doi.org/10.55630/STEM.2023.0522

Tom Dieck, M. C., & Jung, M.R. (2018). *The Potential of the Internet of Things for Authentic Learning and Assessment.* In M. Ebner, & M. Schön (Eds.), Learning with MOOCS 2018 (pp. 409-418). Springer, Cham.

Triplett, W. J. (2023). Addressing Cybersecurity Challenges in Education. *International Journal of STEM Education for Sustainability, 3*(1), 47-67

Valverde, J. U., Ariza, F., & Álvarez, M. R. (2021). Internet of Things in Education: A Review of the State of the Art. *Sensors, 21*(8), 2673.

Wadowsky, L. (2023). Smart notebooks, tablets & smart pens to bring your handwritten notes into the digital era. Retrieved from https://shorturl.at/UiXu5

Wiliam, D. (2017). *Embedded Formative Assessment.* Bloomington, IN: Solution Tree Press.

Wiliam, D., & Leahy, S. (2015). *Embedding Formative Assessment: Practical Techniques for K-12 Classrooms*. West Palm Beach, FL: Learning Sciences International.

Yip, D. (2021). Applying Project-Based Learning (PBL) in assessment design for preservice teacher education: Authenticity in the authentic context. *Assessment & Evaluation in higher education, 46*(1), 162-177.

Zakariyya, I., Kalutarage, H., & Al-Kadri, O. M. (2023). Towards a robust, effective and resource efficient machine learning technique for IoT security monitoring Computers & Security 133, 1-14

Zanella, A., Bui, N., Castellani, A., Vangelista, L. & Zorzi, M. (2014). Internet of Things for Smart Cities. *IEEE Internet of Things Journal, 1*(1), 22-32. https://doi.org/10.1109/JIOT.2014.2306328