Journal of Infrastructure, Policy and Development 2024, 8(8), 3736.
https://doi.org/10.24294/jipd.v8i8.3736

Article

Data architectures and the prevalent cyberattacks encountered by West African higher educational institutions in the COVID-19 era

Ismaila Idris Sinan[1], Vivian Nwoacha[1], Kingsley Eghonghon Ukhurebor[2,*], Jules Degila[3], Adebukola Onashoga[4], Esosa Enoyoze[5], Lyda Emmanuel[1]

[1] Africa Centre of Excellence on Technology Enhanced Learning, National Open University of Nigeria, Abuja 900001, Nigeria
[2] Department of Physics, Edo State University Uzairue, P.M.B. 04, Auchi 312001, Nigeria
[3] African Center of Excellence on Mathematical Sciences, Computer Science and Applications, University of Abomey-Calavi (UAC) Campus d'Abomey-Calavi, 01 BP 526 Cotonou, Benin
[4] Department of Computer Science, University of Agriculture, P.M.B 2240, Abeokuta 110008, Nigeria
[5] Department of Mathematics, Edo State University Uzairue, P.M.B. 04, Auchi 312001, Nigeria
*** Corresponding author:** Kingsley Eghonghon Ukhurebor, ukeghonghon@gmail.com, ukhurebor.kingsley@edouniversity.edu.ng

CITATION

Sinan II, Nwoacha V, Ukhurebor KE, et al. (2024). Data architectures and the prevalent cyberattacks encountered by West African higher educational institutions in the COVID-19 era. Journal of Infrastructure, Policy and Development. 8(8): 3736. https://doi.org/10.24294/jipd.v8i8.3736

ARTICLE INFO

Received: 18 December 2023
Accepted: 19 February 2024
Available online: 7 August 2024

Abstract: The growing interconnectedness of the world has led to a rise in cybersecurity risks. Although it is increasingly conventional to use technology to assist business transactions, exposure to these risks must be minimised to allow business owners to do transactions in a secure manner. While a wide range of studies have been undertaken regarding the effects of cyberattacks on several industries and sectors, However, very few studies have focused on the effects of cyberattacks on the educational sector, specifically higher educational institutions (HEIs) in West Africa. Consequently, this study developed a survey and distributed it to HEIs particularly universities in West Africa to examine the data architectures they employed, the cyberattacks they encountered during the COVID-19 pandemic period, and the role of data analysis in decision-making, as well as the countermeasures employed in identifying and preventing cyberattacks. A total of one thousand, one hundred and sixty-four (1164) responses were received from ninety-three (93) HEIs and analysed. According to the study's findings, data-informed architecture was adopted by 71.8% of HEIs, data-driven architecture by 24.1%, and data-centric architecture by 4.1%, all of which were vulnerable to cyberattacks. In addition, there are further concerns around data analysis techniques, staff training gaps, and countermeasures for cyberattacks. The study's conclusion includes suggestions for future research topics and recommendations for repelling cyberattacks in HEIs.

Keywords: COVID-19; cybersecurity; cyberattacks; data architecture; higher educational institutions

1. Introduction

Data architecture (DA) was born of the need to save an unlimited volume of data to analyse it effectively and make decisions (Vista, 2021). It is a set of models, strategies, rules, and standards that govern how data is collected, stored, processed, integrated, and used in data systems and organizations (Zheng et al., 2010). The use of and dependency on the Internet have increased dramatically during the COVID-19 era (Chigada and Madzinga, 2021; Horgan et al., 2021; Khan et al., 2021; Nneji et al., 2022). As more individuals engage in online activities like remote jobs, online shopping, and others (Asanga et al., 2023; Hussaini et al., 2023; Ndunagu et al., 2023), higher educational institutions (HEIs) particularly West African Universities (WAUs) have been severely impacted, compelling them to completely abandon face-to-face learning in favour of digital learning (Adam, 2021; Ncube and Garrison, 2010; Zhang-

Kennedy and Chiasson, 2021) as the only way to carry on the educational process. As a result, HEIs produced substantially more data. According to some estimates, the world will have produced 94 zettabytes of data by the end of 2022, up from 74 zettabytes in 2021 (Fouad, 2021), with the great majority coming from educational sectors or academic institutions. HEIs were forced to select between the three types of DA, with some opting for data-informed architecture (DIA), others opting for data-driven architecture (DDA), and yet others opting for a data-centric architecture (DCA).

Furthermore, during the migration to digital learning, data security was not a significant factor; this makes them attractive targets for cyberattacks, with many high-profile events already occurring, because they manage enormous volumes of vital research and sensitive personal data (Aslan et al., 2023; Ncube and Garrison, 2010). The threat comes mostly from opportunists seeking financial benefit, and the university's data security difficulty is exacerbated by the free flow of staff, guests, and regular student rotations. Additionally, the lack of cybersecurity awareness programs and training for staff managing university learning management systems, websites, portals, and databases (Zhang-Kennedy and Chiasson, 2021) makes it very easy for cyber criminals to penetrate and gain access to sensitive data.

According to Kariuki et al. (2023), the increasing interrelationships in the world have led to an escalation in cybersecurity risks (cyberattacks). Even though it is increasingly conventional to utilize technological means to promote commercial transactions, exposure to these risks should be reduced to allow business owners to do transactions in a secure manner. Reportedly, there are several studies that have been undertaken concerning the influences of cyberattacks on several sectors of human endeavours. Nevertheless, there are limited studies that focus on the influences of cyberattacks on the educational sector (Gourisetti et al., 2020; Kariuki et al., 2023; Lallie et al., 2021; Vuță, et al., 2022), in particular the HEIs in West Africa.

According to Adam (2020), cybercrime against academic institutions doubled between 2019 and 2020, costing more than $20 million to ransomware attacks; Fouad (2021) found that the University of California lost more than $1.4 million to ransomware; and Ulven and Wangen (2021) discovered several cybercrimes against universities and more in Africa. These attacks are also present in WAUs, and while the demand for data security grows by the day, cybercrime and data breaches in WAUs have received little or no attention. Consequently, the following research questions have been established for this survey:

- What are the types of DA employed by WAUs?
- What types of cyberattacks did these universities face during the COVID era?
- What countermeasures did WAUs use to mitigate these attacks?
- To what extent are data analysis results used in decision-making at WAUs?

Data-architectures

Different researchers have established descriptions for DA, but the definition by Zheng et al. (2010) is the one that is most frequently used. It describes DA as a collection of models, policies, guidelines, and standards that regulate the collected data types and how they are organized, integrated, stored, and utilized in data systems and organizations. According to Ascend (2020); Carol (2021); and Kampakis (2018),

between 400 BC and 2022, DA progressed through four major stages (Sinan et al., 2022):

- Traditional architecture
- DIA
- DDA
- DCA

However, this study will concentrate on data-informed, data-driven, and DCA because these are the only ones now in use by businesses and institutions (Sinan et al., 2022). The following are definitions taken from the literature:

- DIA: Data is collected from various sources, including flash drives, computers' internal and external hard drives, and so on. The data is analysed using a spreadsheet, and the results are used as inputs in decision-making (Ascend, 2020).
- DDA: In this approach, algorithms are utilized to generate decisions based on the data gathered from several data silos, including the cloud, data lakes, and other sources (Alfonso, 2018). Kampakis (2018), defines it as a DA in which storage devices or silos are scattered across several places and algorithms are used to preserve, analyse, and derive decisions from the analysis results. It is defined as a distributed storage architecture employing technology to gather and analyse data to make better business decisions.
- DCA: Alfonso (2018) refers to a system in which data is the primary and permanent asset, whereas applications come and go. In the studies of Dave (2020) and Vista (2021), organizations and institutions create a single data model that is shared by all of the organization's information systems; data science is used as the bedrock for decision-making; and all data are linked and connected using a graph database to eliminate data silos and redundancy.

2. Previous work (literature review)

In the present contemporary globalised world, the utilisation of cyber technologies has increased, transforming and evolving society, business communities, economies, and every aspect of human endeavours in ways never seen before (Aslan et al., 2023; Breitinger et al., 2020; Dupont and Whelan, 2021; Furnell et al., 2020; Monteith et al., 2021). However, due to the exponential growth in the utilisation of cyberspace, cybercriminal activities in the form of cyberattacks have increased as well, with the primary cause being the excessive use of web-based applications, given the reality of the COVID-19 pandemic that has given rise to online interaction (Buil-Gil et al., 2021) and other online activities such as the online education (Asanga et al., 2022; Hussaini et al., 2023; Ndunagu et al., 2023; Nneji et al., 2022), in addition to some medical, environmental and social impacts (Aidonojie et al., 2022; Paladhi et al., 2022; Ukhurebor et al., 2022; Ukhurebor et al., 2021). Cybercriminals use web applications to get confidential information and data and disrupt financial transactions (as well as other damages to every sectors of human endeavours) by businesses, governments, institutions, and regular people (Monteith et al., 2021; Palmieri et al., 2021; Syed, 2020). In light of these developments, cybersecurity research has gained traction among both researchers and other relevant stakeholders and practitioners

(Kariuki et al., 2023).

The Kariuki et al. (2023) reported that since Africans interact on digital platforms, particularly during the COVID-19 epidemic, they have been susceptible to cybersecurity vulnerabilities. The majority of these dealers lack sufficient protection from threats and hazards associated with the internet. The COVID-19 era has seen a rise in cybercrime in tandem with an increase in online business (Kariuki et al., 2023). Therefore, it is advised that traders themselves be involved in a multifaceted strategy to reduce cybersecurity dangers. Governments, business chambers, internet service providers (ISPs), and locally based migrant business groups must work together to provide a variety of support systems that will help merchants adapt to the shifting digital and economic trading landscape in the diaspora (Kariuki et al., 2023; Zaripova et al., 2021).

The cyberattacks cases in the educational sector are hardly reported in the headlines of most news, unlike breaches (cyberattacks cases) in other sectors, but educational sectors such as colleges, schools, and universities, as well as other HEIs, are also vastly targeted by today's threat (cyberattacks) actors and continually under attack (Wolf, 2023). However, there are some reports regarding cyberattacks on the educational sector in most advanced nations. According to reports from "Verizon's 2022 Data Breach Investigations" (Wolf, 2023), the educational services sector in America witnessed 1241 cyberattacks in 2021, with 282 linked to confirmed data disclosure. In all these attacks, 75% resulted from external sources, while the remaining 25% were from internal sources. These cyberattacks were devastatingly inspired by monetary recompenses, with 95% involving a fiscal motive. These reported cyberattack incidents demonstrate how ransomware has become a major issue for the educational sector, affecting various educational institutions such as colleges, schools, and universities (as well as other HEIs and other sectors of the educational systems) of all sizes worldwide, with varied degrees of expense and severity. These cyberattack assaults frequently result in postponed classes, high remedial costs, harm to an institution's image, and unanswered doubts about its capacity to fend off future attacks. Furthermore, teachers, students, and government representatives scrutinise educational institution executives following a ransomware cyberattack assault.

However, few articles with specifics on data security and cyberattacks in universities were found in our literature review, but none of them was relevant to WAUs, nor were they within the scope of the COVID-19 epidemic era, nor were they related to DA. Examples of such papers are highlighted in this section.

Adams and Blanford (2003) investigated security in online learning and discussed the security-availability trade-off. The authors were the first to discuss the security culture of North American academia in depth. Whitman and Mattord (2016) mapped cybersecurity threat agents, events, and risks for a broad range of universities in 2016. Chen and He (2013) examine the security risks and protections that online learning entails. The findings mostly revolve around technical attacks and countermeasures. Beaudin (2015, 2017) explores the legal ramifications of data breaches in universities while keeping student data, as well as state and federal cybersecurity regulations. Hussain et al. (2018) look into the dangers of online social networking in Malaysian universities, focusing on the threat of cybersecurity to lecturers. A related study by Ajie (2019) focuses on the cybersecurity vulnerabilities

that university libraries face. Cuchta et al. (2019) and Diaz et al. (2020) both demonstrate a high rate of phishing attacks in academics and recommend mitigation techniques. Dadkhah et al. (2017) identify cyberattacks in scholarly publishing, such as the fraudulent call for papers, and examine the techniques used by attackers to deceive researchers. Sinam and Lawan (2019) and Teixeira da Silva et al. (2020) have looked into the challenges and expenses of spam emails in academia. A root-cause analysis of physical security issues at a university college was undertaken by Wangen et al. (2017). Kashiwazaki (2018) describes a data breach incident that occurred at a Japanese university. The author provides insight into how the situation occurred and potential countermeasures.

3. Method

The research methodology used for this study was adopted from Georgiadou et al. (2021). Designing the survey questions (SQs) comes first, then participants, validity testing, and finally dissemination and analysis.

3.1. Design

A survey was determined to be the most effective technique for collecting data to answer the research questions posed. The SQs cover all loopholes, beginning by developing twenty (20) SQs in two different languages, English and French. SQ8 and SQ9 were created to get answers for the first research question, which inquired about the different types of DA used at the university. The second research question is concerned with cyberattacks and threats to institutions, and two SQs, SQ17 and SQ18, have been allocated to this task. To address the third research question, SQ18, SQ19, SQ20, SQ21, and SQ22 were designed and used to obtain full details of countermeasure techniques used in mitigating cyberattacks and threats within the universities. SQ10, SQ11, SQ12, SQ13, SQ14, and SQ15 were created to comprehensively investigate the extent of employing data in decision-making, which answered the fourth research question. SQ1, SQ2, SQ3, SQ4, SQ5, and SQ6 are for demography, and SQ7 is to aid in data analysis.

3.2. Participants

Due to the survey's peculiarities, only technical staff who work with learning management systems, university websites, portals, directors of IT units, and directors of academic planning were asked to participate. The targeted responses of the survey were to obtain at least 1000 responses from at least 90 HEIs, which is 70% of the 128 West African institutions that were registered with the Association of African Universities (AAU, 2022).

A total of one thousand, one hundred and sixty-four (1164) responses were received from ninety-three (93) HEIs wherein seventy-seven (77) are public universities and sixteen (16) are private, with Nigeria being the highest with forty-nine (49) HEIs, Ghana 23, Gambia 3, Senegal 3, Sierra Leone 3, Burkina Faso 2, Cote d'voire 2, Niger 2, and Togo 2. Benin, Liberia, Mauritania, and Mali with the fewest amounts of one (1) each, making a total of ninety-three (93) HEIs.

3.3. Validity testing

After creating a preliminary version of the SQs, the following phase was validity testing, which involved asking about 20 people to examine and complete the survey. During this phase, a group comprised survey specialists, experienced researchers and analysts, certified security and technology officers, and non-technical staff with a basic understanding of technology. Prior to being widely disseminated, it was designed to find unclear questions, vague instructions, or other issues (Draugalis et al., 2008). Respondent debriefing and cognitive interviewing were used to assess the clarity of the questions and the understanding of terms (Clark and Watson, 2019). To identify areas of potential misunderstanding, think-aloud and verbal probing techniques (Marra et al., 2020) were used. Taking feedback from this phase into account, the final version of the survey.

3.4. Dissemination and analysis

The survey was created using Google Forms on 26 February 2022, and disseminated to WAUs, private and public, via email and WhatsApp. It was in circulation for three (3) months, from 1 March to 31 May 2022. Because of the unique nature of this study, not all university staff were eligible to participate; only technical staff who work with learning management systems, university websites, portals, directors of IT units, and directors of academic planning were allowed to participate. We contacted them and asked them to participate in the survey as well as pass it along to more suitable participants. Association of African Universities (AAU) data were used to disseminate the survey.

We concluded that we had collected enough responses from knowledgeable participants after getting 1164 responses across the region from ninety-three (93) universities out of the one hundred and twenty-eight (128) institutions in the AAU database, or about 72% of WAUs. We also avoided duplicate responses by limiting each participant to one response. In addition, we removed 109 responses from participants who indicated that their institutions did not offer any workshops or training during the COVID-19 epidemic because our goal was to capture responses during the pandemic period. The remaining 1055 responses were used in this study.

We concluded that we had collected enough responses from knowledgeable participants after getting 1164 responses across the region from ninety-three (93) universities out of the one hundred and twenty-eight (128) institutions in the AAU database, or about 72% of WAUs. We also avoided duplicate responses by limiting each participant to one response. In addition, we removed 109 responses from participants who indicated that their institutions did not offer any workshops or training during the COVID-19 epidemic because our goal was to capture responses during the pandemic period. The remaining 1055 responses were used in this study.

In order to gain complete data that covers all angles, especially for SQs under the fourth research question, we use a four-point Likert scale devised by Pimentel (2010). Where we assign values to: extensively = 4, moderately = 3, a little = 2, and not at all = 1. Additionally, the collected data were analysed using SPSS.

4. Results

This section presents the survey's statistical analysis. The demography of the respondents will be discussed first, then data application and usability, and finally, cyberattacks and countermeasures.

4.1. Demography

The first part of the survey is for demography, including six SQs. This aids in getting descriptive data about the universities and participants' behaviours towards securing their university data. **Figure 1** presents the breakdown of the universities surveyed according to their countries, with Nigeria being the highest with forty-nine (49) institutions, Ghana 23, Gambia 3, Senegal 3, Sierra Leone 3, Burkina Faso 2, Cote d'Ivoire 2, Niger 2, and Togo 2. Benin, Liberia, Mauritania, and Mali with the fewest amounts of one (1) each, making a total of ninety-three universities.

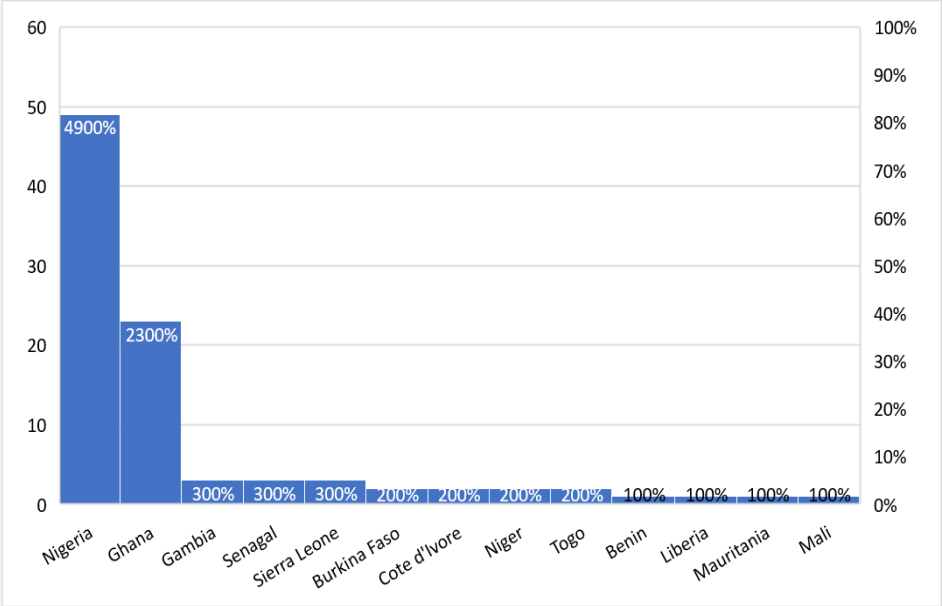

Figure 1. Number of universities according to countries.

Additionally, seventy-seven (77) are public universities and sixteen (16) are private. These institutions employed different modes of delivery (MOD); 44.4% of the responses came from universities using face-to-face, 45.4% from e-learning institutions, and 10.1% from blended MOD institutions. All universities regularly create vast amounts of data as a result of the plethora of online activity. Of the respondents, 10.5% claimed their institutions only complete applications (A) online, compared to 56.6% who completed application and registration (AR), 6.6% who completed applications, registrations, and examinations (ARE), 8.9% who agreed that their institutions are always online for applications, registrations, and lectures (ARL), and 24.4% who agreed on applications, registrations, lectures, and examinations (ARLE) (**Table 1**).

This demonstrates the significant reliance on online resources for the efficient operation of WAUs. In terms of DA, 4.1% of the participants believed they employed DCA, 24.1% DDA, and 71.8% DIA (**Table 1**).

Table 1. Demography of universities.

Online activities			
Frequency	**Frequency**	**Percent (%)**	**Cumulative percent (%)**
Application	111	10.5	10.5
Application and registration	591	56.0	66.5
Application, registration and examination	6	0.6	67.1
Application, registration and lectures	94	8.9	76.0
Application, registration, lectures and examination	253	24.0	100.0
Total	1055	100.0	
Mode of delivery			
Blended learning	117	10.1	10.1
E-learning	518	44.5	54.6
Face-to-face learning	529	45.4	100.0
Total	1164	100.0	
DA			
DCA	43	4.1	4.1
DDA	254	24.1	28.1
DIA	758	71.8	100.0
Total	1055	100.0	

The survey received huge responses from both males and females; 76% are males and 24% are females. This is of particular importance as the ratio of females to males is the ideal ratio for productive work in a cybersecurity environment (Fatokun et al., 2019). Additionally, 18.6% of participants were under 25 years old, followed by 39.6% between 26 and 35 years old, 27.7% from 35 to 45 years old, 10% from 46 to 55 years old, and 4.7% from participants over 56 years of age. **Figure 2** shows a histogram of age with a mean of 2.43. This is vital because it entails that university staff have the ideal age to learn new emerging cybersecurity techniques.

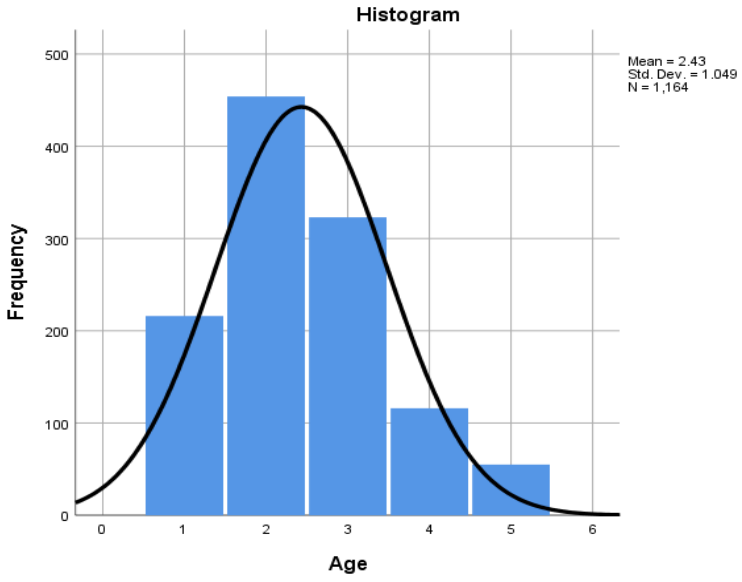

Figure 2. Histogram of age analysis.

Furthermore, among the participants, 19.8% have a diploma, 46.1% have a bachelor's degree, 20.6% have completed their master's, and 13.3% have a PhD (**Table 2**).

Table 2. Demography of participants.

Frequency	Frequency	Percent (%)	Cumulative percent (%)
Gender			
Female	279	24.0	24.0
Male	885	76.0	100.0
Total	1164	100.0	
Age			
26–35 year	454	39.0	39.0
36–45 year	323	27.7	66.8
46–55 year	116	10.0	76.7
56 and above	55	4.7	81.4
Below 25 years	216	18.6	100.0
Total	1164	100.0	
Qualification			
Bachelor	537	46.1	46.1
Diploma	231	19.8	66.0
Masters	240	20.6	86.6
PGD	1	0.1	86.7
PhD	155	13.3	100.0
Total	1164	100.0	

4.2. Data application and usability

In this survey, participants were given several questions on the use of data and analysis results in making decisions using a four-point Likert scale. The responders were initially questioned on the types of data they gathered for analysis prior to making decisions, the tools they used to execute the analysis, and the types of decisions they made.

Figure 3 presents the details of the type of data used for analysis for WAUs: 35.1% believed their institutions don't use data at all for decision-making; they rely on their gut feelings and experiences; 36.1% claimed they use data about what happened in the recent past (e.g., last year or last quarter); 21.1% agreed that their universities use past and recent data, including some longer-term trend analysis; and 7.6% said they use past, present, and forward-looking data.

Table 3 shows descriptive statistics of the tools employed for analysis by WAUs: spreadsheets (e.g., charts, counts, tables) have a mean of 3.09, website analytics (e.g., Google Analytics) have a mean of 2.22, databases (e.g., CRM analytics, reports) have a mean of 2.65, and specialized tools (e.g., SAS, R, Stata, Python, SPSS, GIS mapping) have a mean of 2.57.

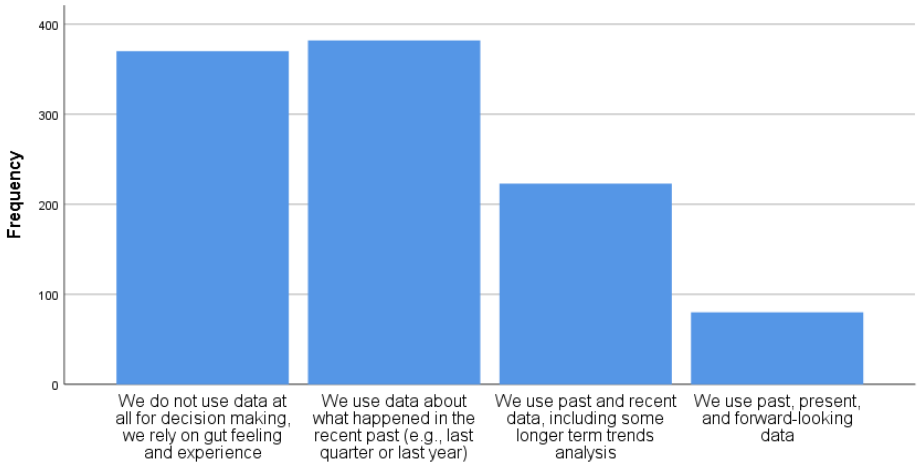

Figure 3. Breakdown of the types of data employed by WAUs.

Table 3. Descriptive statistics of tools used for analysis.

Tools	*N*	Minimum	Maximum	Mean	Std. deviation
Spreadsheet	1055	1	4	3.09	0.951
Website Analytics	1055	1	4	2.22	1.208
Database	1055	1	4	2.65	0.933
Specialize Tools	1055	1	4	2.57	0.974
Valid N (listwise)	1055				

The data analysis result is used by WAUs to make decisions on different categories; in terms of academic development decisions, it has a mean of 2.74, employment has a mean of 2.70, environmental impacts have a mean of 2.70, other societal impacts have a mean of 2.68, research opportunities have a mean of 2.70, and student satisfaction has a mean of 3.11 (**Table 4**).

Table 4. Descriptive statistics on the use of data analysis results.

Data usage	*N*	Mean	Std. deviation
Academic development	1055	2.74	0.913
Employment	1055	2.70	0.971
Environmental impacts	1055	2.70	0.964
Other societal impacts	1055	2.68	0.956
Research opportunities	1055	2.70	0.975
Students' satisfaction	1055	3.11	1.022
Valid N (listwise)	1055		

4.3. Cyberattacks and countermeasures

During the COVID-19 pandemic, WAUs was severely targeted by cyberattacks. 87.4% of the respondents indicated that they were victims of cyberattacks, and 12.6% were not. Of the victims who are knowledgeable enough about the security vulnerabilities at their institutions, 621 agreed their institutions were attacked by SQL injection, 752 by a denial-of-service attack, 565 by ransomware, 451 by a virus, 214 by a worm, 335 by a phishing attack, and 1 participant reported not knowing about

any cyberattacks (**Figure 4**).

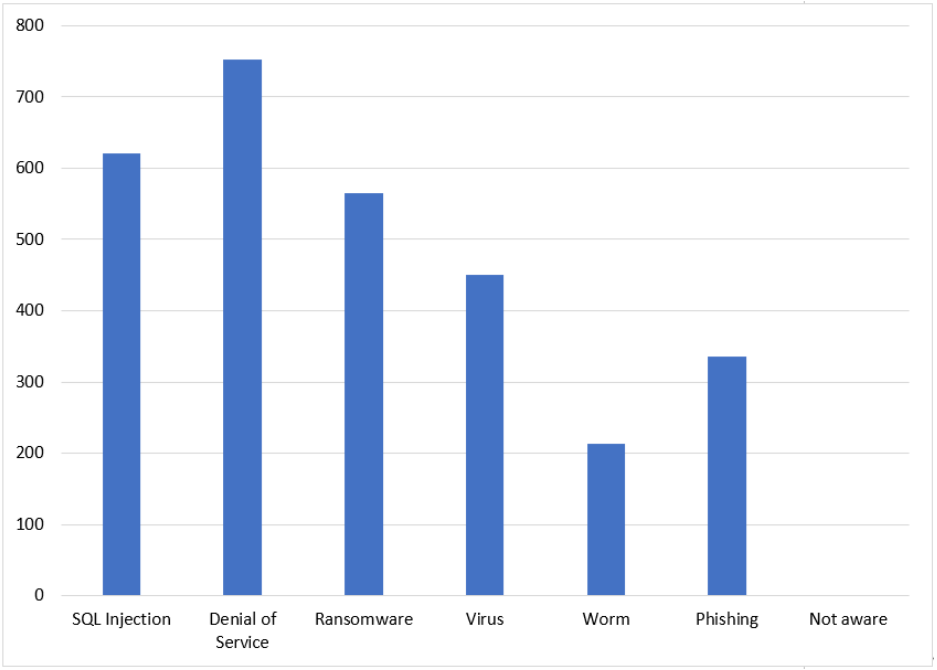

Figure 4. Summary of cyberattacks faced by WAUs.

Moreover, the participants receive cybersecurity training, but only 8.1% complete it after 3 months, 10.2% do so after 6 months, 40.3% do so after 12 months, and 41.1% have never attended any cybersecurity training (**Figure 5**).

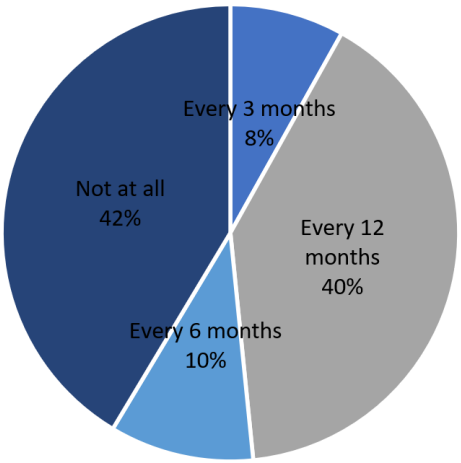

Figure 5. Summary of staff cybersecurity training.

Moreover, a variety of countermeasures are used by WAUs; **Table 5** breaks down these techniques. These institutions used a variety of techniques to ensure secure cyberspace for learning, and the majority of participants (52.9%) claimed their institutions only used firewalls and antivirus software for security, while 0.1% thought their institutions used firewalls, intrusion detection systems, and intrusion prevention systems.

Responders were asked about the level of satisfaction they had with their institution's data protection techniques; **Table 6** shows that it has a mean of 2.24.

Table 5. Countermeasures.

Countermeasures technique	Frequency	Percent (%)	Cumulative percent (%)
Anti-virus	28	2.7	2.7
Anti-virus, Intrusion detection system	173	16.4	19.1
Anti-virus, Intrusion detection system, Intrusion prevention system	12	1.1	20.2
Anti-virus, Intrusion prevention system	4	0.4	20.6
Firewall	22	2.1	22.7
Firewall, Anti-virus	558	52.9	75.5
Firewall, Anti-virus, Intrusion detection system	176	16.7	92.2
Firewall, Anti-virus, Intrusion detection system, Intrusion prevention system	38	3.6	95.8
Firewall, Anti-virus, Intrusion prevention system	9	0.9	96.7
Firewall, Intrusion detection system	13	1.2	97.9
Firewall, Intrusion detection system, Intrusion prevention system	1	0.1	98.0
Intrusion detection system	9	0.9	98.9
Intrusion detection system, Intrusion prevention system	8	0.8	99.6
Intrusion prevention system	2	0.2	99.8
Not known	2	0.2	100.0
Total	1055	100.0	

Table 6. Descriptive statistics on satisfaction.

Items	*N*	Mean	Std. deviation
Satisfaction	1055	2.24	0.795
Valid *N* (listwise)	1055		

5. Discussion

This study created a survey and distributed it to WAUs to determine the security vulnerability of their DA, techniques for preventing cyberattacks, and the effect of data analysis on decision-making. Industries that play a large part in developing, implementing, securing, and updating DA could greatly benefit from this work. In this section, first and foremost, we will discuss demographic analysis, data analysis and usability, and cyberattacks and countermeasures.

Looking at **Figure 2**'s age analysis, it has a mean of 2.43 (std. Dev 1.049), which indicates that the majority age of the participants is 25–35 years, and 46.1% have bachelor's degrees, which is the perfect age and educational background for the staff to learn new skills for fending off cyberattacks. Furthermore, analysis demonstrates that the gender ratio is favourable for staff to co-exist for effective work in a cybersecurity environment (Fatokun et al., 2019). In addition, WAUs have quickly made the switch to digital learning; 45.1% of the institutions surveyed used e-learning as a MOD, and every institution had at least one online activity. This makes it a challenge for both researchers and industries to provide safe and secure DA in this region.

In addition, WAUs are always looking for research gaps that may be addressed by academic researchers, in addition to staff employment, enrolling more students, and developing staff capacity. However, the results of this study indicate that, in order to

run these universities efficiently, there is a need to optimize the utilization of data analysis results. Moreover, **Table 5** shows that data analysis results for academic development have a mean of 2.74, employment has a mean of 2.70, environmental impacts have a mean of 2.68, research opportunities have a mean of 2.70, and student satisfaction has a mean of 3.11; this demonstrates the specific areas that need improvement, particularly areas with less than 3.0. Additionally, the type of data acquired for analysis before decision-making and the tools used for analysis are also causes for concern. According to the study's findings, only 7.6% of participants believed their institutions used past, present, and future-looking data for analysis, while 35.1% agreed that they used their intuition and experience instead. Furthermore, with a mean of 3.09, the majority of participants chose to use spreadsheet software for data analysis, compared to less than 2.6 for the other tools, which is worrying. This creates a vacuum for WAUs to enhance the type of data and analysis tools.

Findings show that WAUs are always conducting activities online, be it application, registration, lectures or facilitation, or examination, which yields data generation, and is yet to get a secured means of storing their data. Only 12.6% indicated that their universities were not victims of cyberattacks. These attacks are due to several factors, particularly:

- Inability to upgrade their DA to the newest, this study finds out that 71.8% use DIA, which is the most obsolete DA in existence, followed by DD with 24.1%, and 4.1% employ DCA, which is the most advanced DA in existence now, and it is highly secured with few security vulnerabilities (Kim, 2019).
- The technical staff maintaining learning management systems, websites, and portals lacks cybersecurity knowledge and training. This study reveals that 41.1% of the staff have never taken cybersecurity training, 40.3% have done so every 12 months, 10.2% have taken it after 6 months, and 8.1% have taken it after 3 months. The training has a mean of 1.85, indicating that the majority of participants have never taken cybersecurity training (**Table 6**), and the analysis of the cybersecurity skills of the participants reveals they have a mean of 3.43, demonstrating the need for frequent training and workshops.
- Lack of adequate countermeasures to efficiently prevent and detect cyberattacks. The findings of this study show that universities use several techniques when repelling cyberattacks; 52.9% use firewalls and anti-virus software, which is not efficient, while 0.1% believe their institution employs firewalls, intrusion detection systems, and intrusion prevention systems.

Additionally, on a scale of yes, neutral, and no, the participants were also asked to rate their level of satisfaction with their institution's countermeasures strategy. Analysis reveals that it has a mean of 2.24 (**Table 6**), indicating that the majority of participants are not satisfied with their institution's countermeasures strategy. In conclusion, upgrading to DCA and the creation of a strong cybersecurity framework are both necessary for WAUs to achieve a secured DA free from cyberattacks. These institutions also need to involve their staff in regular cybersecurity training and use data-science techniques when analysing and making future-oriented decisions.

6. Limitation, implication, conclusion and recommendations for future research direction

To learn more about the DA WAUs used, the cyberattacks they experienced, the role of data analysis in decision-making, and the countermeasures employed in identifying and preventing cyberattacks, this study developed a survey and distributed it to these universities. Only technical staff members who deal with learning management systems, university websites, portals, heads of IT units, and directors of academic planning were requested to participate in the survey, which yielded a total of 1164 replies. According to the survey, 71.8% of institutions employed DDA, 24.1% used DDA, and 4.1% used DCA, all of which were vulnerable to cyberattacks. Countermeasures for cyberattacks, a lack of cybersecurity training for staff, data analysis techniques, and decision-making based on analysis results are further issues to be concerned about. Researchers will benefit from this study by better comprehending the nature of DA in WAUs, their security faults, and the causes of these vulnerabilities. Universities should upgrade their DA to DCA, as well as include their staff in regular cybersecurity training and apply data-science approaches when analysing and making future-focused decisions.

Although the study examines cyberattacks on DA in universities, it is limited to West Africa. Since there are limited studies that focus on the impacts of cyberattacks on the educational sector, HEIs (WAUs to be specific), the study was, however, limited to only some HEIs particularly WAUs. This implies that the study has attempted to develop a survey and distribute it to HEIs, particularly WAUs, so as to examine the data architectures utilised and the cyberattacks encountered during the COVID-19 pandemic period, as well as the role of data analysis in decision-making and the countermeasures employed in identifying, mitigating, and preventing cyberattacks in HEIs. Consequently, this implies that the findings from this study cannot be generalised to all educational sectors globally. Hence, there is a need to organise a more detailed study that will involve the entire educational sector of all African countries as well as other regions of the world.

In the future, the scope of the survey should be expanded to include all of Africa and, if possible, the entire world. The survey also skipped over looking at the different e-learning solutions that the WAUs employed. Future research might improve this work by investigating e-learning solutions and their vulnerabilities and highlighting ways to improve them. Furthermore, future research might look into the implementation difficulties of DA, which were not covered in this study.

The increasing expansion of educational institutions' digital footprints to accommodate the demands of both in-person and remote learning has resulted in an increased danger from hackers, especially those skilled in ransomware attacks. To withstand the threat of ransomware or any other type of cyberattack, one has to have access to specific security solutions that may evolve to meet the changing demands of society. These solutions should also be supported by a round-the-clock team of specialists who are always on call and keep an eye on the larger context.

Author contributions: Conceptualization, IIS; methodology, IIS, VN and KEU; software, IIS; validation, IIS, VN and KEU; formal analysis, IIS, VN and KEU;

investigation, IIS, VN and KEU; resources, XX; data curation, IIS, VN and KEU; writing—original draft preparation, IIS, VN and KEU; writing—review and editing, IIS, VN, KEU, JD, AO, EE and LE; visualization, IIS, VN and KEU; supervision, VN and KEU; project administration, IIS, VN and KEU; funding acquisition, , IIS, VN, KEU, JD, AO, EE and LE. All authors have read and agreed to the published version of the manuscript.

Acknowledgments: The authors appreciate the authors and publishers, whose articles were used as guides for this study. Also, the authors express gratitude to their respective institutions and the Africa Centre of Excellence on Technology Enhanced Learning (ACETEL), National Open University of Nigeria, Abuja as well as the Digital Science and Technology Network (DSTN) for supporting this study.

Conflict of interest: The authors declare no conflict of interest.

References

AAU. (2022). List of Members—AAU. Available online: https://aau.org/members/list/ (accessed on 28 April 2023).

Adam, B. (2021). Bad education: Universities struggle to defend against surging cyber-attacks during coronavirus pandemic. Available online: https://portswigger.net/daily-swig/bad-education-universities-struggle-to-defend-against-surging-cyber-attacks-during-coronavirus-pandemic (accessed on 28 April 2023).

Adams, A., & Blanford, A. (2003). Security and online learning: To protect and prohibit. In Usability evaluation of online learning programs, 331–359. https://doi.org/10.4018/978-1-59140-105-6.ch018

Aidonojie, P. A., Okuonghae, N., & Ukhurebor, K. E. (2022). The Legal Rights and Challenges of COVID-19 Patients Accessing Private Healthcare in Nigeria. BESTUUR, 10(2), 183. https://doi.org/10.20961/bestuur.v10i2.68118

Ajie, I. (2019). A Review of Trends and Issues of Cybersecurity in Academic Libraries. Library Philosophy and Practice (ejournal).

Alfonso, F. Data-driven versus data-centric. Available online: https://blog.stratio.com/datadriven-versus-datacentric/ (accessed on 13 February 2023).

Asanga, M. P., Essiet, U. U., Ukhurebor, K. E., et al. (2023). Social Media and Academic Performance: A Survey Research of Senior Secondary School Students in Uyo, Nigeria. International Journal of Learning, Teaching and Educational Research, 22(2), 323–337. https://doi.org/10.26803/ijlter.22.2.18

Ascend. (2020). Data-Informed, Data-Driven, and Data-Centric: What's the Difference? Ascend Venture Capital. Available online: https://www.ascendstl.com/press/2020/4/28/data-driven-and-data-centric-whats-the-difference (accessed on 13 February 2023).

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., et al. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. Electronics, 12(6), 1333. https://doi.org/10.3390/electronics12061333

Beaudin, K. (2015). College and university data breaches: Regulating higher education cybersecurity under state and federal law. JC & UL, 41, 657.

Beaudin, K. (2017). The legal implications of storing student data: Preparing for and responding to data breaches. New Directions for Institutional Research, 2016(172), 37–48. https://doi.org/10.1002/ir.20202

Breitinger, F., Tully-Doyle, R., & Hassenfeldt, C. (2020). A survey on smartphone user's security choices, awareness and education. Computers & Security, 88, 101647. https://doi.org/10.1016/j.cose.2019.101647

Buil-Gil, D., Miró-Llinares, F., Moneva, A., et al. (2020). Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. European Societies, 23(sup1), S47–S59. https://doi.org/10.1080/14616696.2020.1804973

Carol, D. The Difference Between Data-centric and Data-driven. Available online: https://www.asti.com/the-difference-between-data-centric-and-data-driven/ (accessed on 28 April 2023).

Chen, Y., & He, W. (2013). Security risks and protection in online learning: A survey. The International Review of Research in Open and Distributed Learning, 14(5). https://doi.org/10.19173/irrodl.v14i5.1632

Chigada, J., & Madzinga, R. (2021). Cyberattacks and threats during COVID-19: A systematic literature review. SA Journal of

Information Management, 23(1). https://doi.org/10.4102/sajim.v23i1.1277

Clark, L. A., & Watson, D. (2019). Constructing validity: New developments in creating objective measuring instruments. Psychological Assessment, 31(12), 1412–1427. https://doi.org/10.1037/pas0000626

Cuchta, T., Blackwood, B., Devine, T. R., et al. (2019). Human Risk Factors in Cybersecurity. In: Proceedings of the 20th Annual SIG Conference on Information Technology Education. https://doi.org/10.1145/3349266.3351407

Dadkhah, M., Borchardt, G., & Maliszewski, T. (2017). Fraud in Academic Publishing: Researchers Under Cyber-Attacks. The American Journal of Medicine, 130(1), 27–30. https://doi.org/10.1016/j.amjmed.2016.08.030

Dave, M. (2020). The Data-Centric Revolution: Data-Centric vs. Data-Driven. Available online: https://tdan.com/the-data-centric-revolution-data-centric-vs-data-driven/20288 (accessed on 28 April 2023).

Diaz, A., Sherman, A. T., & Joshi, A. (2020). Phishing in an academic community: A study of user susceptibility and behavior. Cryptologia, 44(1), 53–67. https://doi.org/10.1080/01611194.2019.1623343

Draugalis, J. R., Coons, S. J., & Plaza, C. M. (2008). Best Practices for Survey Research Reports: A Synopsis for Authors and Reviewers. American Journal of Pharmaceutical Education, 72(1), 11. https://doi.org/10.5688/aj720111

Dupont, B., & Whelan, C. (2021). Enhancing relationships between criminology and cybersecurity. Journal of Criminology, 54(1), 76–92. https://doi.org/10.1177/00048658211003925

Fatokun, F. B., Hamid, S., Norman, A., et al. (2019). The Impact of Age, Gender, and Educational level on the Cybersecurity Behaviors of Tertiary Institution Students: An Empirical investigation on Malaysian Universities. Journal of Physics: Conference Series, 1339(1), 012098. https://doi.org/10.1088/1742-6596/1339/1/012098

Fouad, N. S. (2021). Securing higher education against cyberthreats: from an institutional risk to a national policy challenge. Journal of Cyber Policy, 6(2), 137–154. https://doi.org/10.1080/23738871.2021.1973526

Furnell, S., Heyburn, H., Whitehead, A., & Shah, J.N. 2020. Understanding the full cost of cyber security breaches. Computer Fraud & Security, 2020, (12), 6–12. https://doi.org/10.1016/S1361-3723(20)30127-5

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Working from home during COVID-19 crisis: a cyber security culture assessment survey. Security Journal, 35(2), 486–505. https://doi.org/10.1057/s41284-021-00286-2

Gourisetti, S. N. G., Mylrea, M., & Patangia, H. (2020). Cybersecurity vulnerability mitigation framework through empirical paradigm: Enhanced prioritized gap analysis. Future Generation Computer Systems, 105, 410–431. https://doi.org/10.1016/j.future.2019.12.018

Horgan, S., Collier, B., Jones, R., et al. (2021). Re-territorialising the policing of cybercrime in the post-COVID-19 era: towards a new vision of local democratic cyber policing. Journal of Criminal Psychology, 11(3), 222–239. https://doi.org/10.1108/jcp-08-2020-0034

Hussaini, A. R., Ibrahim, S., Ukhurebor, K. E., et al. (2023). The Influence of Information and Communication Technology in the Teaching and Learning of Physics. International Journal of Learning, Teaching and Educational Research, 22(6), 98–120. https://doi.org/10.26803/ijlter.22.6.6

Hussain, H. S., Din, R., Khidzir, N. Z., et al. (2018). Risk and Threat via Online Social Network among Academia at Higher Education. Journal of Physics: Conference Series, 1018, 012008. https://doi.org/10.1088/1742-6596/1018/1/012008

Kampakis, D. S. What are the differences between data-driven, data-informed and data-centric? Available online: https://thedatascientist.com/data-driven-data-informed-data-centric/ (accessed on 1 December 2023).

Kariuki, P., Ofusori, L. O., & Subramaniam, P. R. (2023). Cybersecurity threats and vulnerabilities experienced by small-scale African migrant traders in Southern Africa. Security Journal. https://doi.org/10.1057/s41284-023-00378-1

Kashiwazaki, H. (2018). Personal Information Leak in a University, and Its Cleanup. Proceedings of the 2018 ACM SIGUCCS Annual Conference. https://doi.org/10.1145/3235715.3235727

Khan, N. A., Brohi, S. N., & Zaman, N. (2020). Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic. https://doi.org/10.36227/techrxiv.12278792.v1

Kim, H. (2019). Research Issues on Data Centric Security and Privacy Model for Intelligent Internet of Things based Healthcare. Biomedical Journal of Scientific & Technical Research, 16(3). https://doi.org/10.26717/bjstr.2019.16.002856

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., et al. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & Security, 105, 102248. https://doi.org/10.1016/j.cose.2021.102248

Marra, D. E., Hamlet, K. M., Bauer, R. M., et al. (2020). Validity of teleneuropsychology for older adults in response to COVID-19: A systematic and critical review. The Clinical Neuropsychologist, 34(7–8), 1411–1452.

https://doi.org/10.1080/13854046.2020.1769192

Monteith, S., Bauer, M., Alda, M., et al. (2021). Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry. Current Psychiatry Reports, 23(4). https://doi.org/10.1007/s11920-021-01228-w

Ncube, C., & Garrison, C. (2010). Lessons learned from university data breaches. Palmetto Business & Economic Review, 13, 27–37.

Ndunagu, J. N., Ukhurebor, K. E., Adesina, A. (2023). Virtual Laboratories for STEM in Nigerian Higher Education: The National Open University of Nigeria Learners' Perspective. In: Proceedings of the Technology-Enhanced Learning in Laboratories Workshop (TELL 2023). pp. 38–48.

Nneji, C. C., Urenyere, R., Ukhurebor, K. E., et al. (2022). The impacts of COVID-19-induced online lectures on the teaching and learning process: An inquiring study of junior secondary schools in Orlu, Nigeria. Frontiers in Public Health, 10. https://doi.org/10.3389/fpubh.2022.1054536

Paladhi, A. G., Manohar, M., Pal, K., et al. (2022). Novel electrochemical biosensor key significance of smart intelligence (IoMT & IoHT) of COVID-19 virus control management. Process Biochemistry, 122, 105–109. https://doi.org/10.1016/j.procbio.2022.09.023

Palmieri, M., Shortland, N., & McGarry, P. (2021). Personality and online deviance: The role of reinforcement sensitivity theory in cybercrime. Computers in Human Behavior, 120, 106745. https://doi.org/10.1016/j.chb.2021.106745

Pimentel, J. L. (2010). A note on the usage of Likert Scaling for research data analysis. USM R&D Journal, 18(2), 109–112.

Sinam, I. I., & Lawan, A. (2019). An improved C4. 5 model classification algorithm based on Taylor's series. Jordanian Journal of Computers and Information Technology (JJCIT), 5(01).

Sinan, I. I., Degila, J., Nwaocha, V., et al. (2022). Data Architectures' Evolution and Protection. In: Proceedings of the 2022 International Conference on Electrical, Computer and Energy Technologies (ICECET). https://doi.org/10.1109/icecet55527.2022.9872597

Syed, R. (2020). Cybersecurity vulnerability management: A conceptual ontology and cyber intelligence alert system. Information & Management, 57(6), 103334. https://doi.org/10.1016/j.im.2020.103334

Teixeira da Silva, J. A., Al-Khatib, A., & Tsigaris, P. (2019). Spam emails in academia: issues and costs. Scientometrics, 122(2), 1171–1188. https://doi.org/10.1007/s11192-019-03315-5

Ukhurebor, K. E., Aigbe, U. O., Onyancha, R. B., et al. (2022). Greenhouse Gas Emission: Perception during the COVID-19 Pandemic. BioMed Research International, 2022, 1–12. https://doi.org/10.1155/2022/6166276

Ukhurebor, K. E., Singh, K. R., Nayak, V., et al. (2021). Influence of the SARS-CoV-2 pandemic: a review from the climate change perspective. Environmental Science: Processes & Impacts, 23(8), 1060–1078. https://doi.org/10.1039/d1em00154j

Ulven, J. B., & Wangen, G. (2021). A Systematic Review of Cybersecurity Risks in Higher Education. Future Internet, 13(2), 39. https://doi.org/10.3390/fi13020039

Vista. (2021). Data-centric Architecture—A Different Way of Thinking. Available online: https://www.vistaprojects.com/blog/data-centric-architecture/ (accessed on 28 April 2023).

Vuță, D. R., Nichifor, E., Țierean, O. M., et al. (2022). Extending the Frontiers of Electronic Commerce Knowledge through Cybersecurity. Electronics, 11(14), 2223. https://doi.org/10.3390/electronics11142223

Wangen, G., Hellesen, N., Torres, H., & Brækken, E. (2017). An empirical study of root-cause analysis in information security management. Rome. Conference SECURWARE, IARIA, 1–14.

Whitman, M. E., & Mattord, H. J. (2016). Threats to information protection-industry and academic perspectives: An annotated bibliography. Journal of Cybersecurity Education, Research and Practice, 2016(2), 4.

Wolf. A (2023). 8 Major Cyber Attacks Against Schools and Colleges. Available online: https://arcticwolf.com/resources/blog/cyber-attacks-against-schools-and-colleges/ (accessed on 7 January 2024).

Zaripova, D.A. 2021. Network security issues and effective protection against network attacks. International Journal on Integrated Education 4 (2): 79–85.

Zhang-Kennedy, L., & Chiasson, S. (2021). A Systematic Review of Multimedia Tools for Cybersecurity Awareness and Education. ACM Computing Surveys, 54(1), 1–39. https://doi.org/10.1145/3427920

Zheng, X., Li, Q., & Kong, L. (2010). A Data Storage Architecture Supporting Multi-level Customization for SaaS. In: Proceedings of the 2010 Seventh Web Information Systems and Applications Conference. https://doi.org/10.1109/wisa.2010.18