Journal of Contemporary Research in Educational Administration & Management

Volume 2, Issue 2, 2025, 11- 23

ISSN: 0795-9516 www.edufdns.ng/jcream/index

Research Article

Application of Digital Technologies in Combating Cybercrime in Nigerian Tertiary Institutions: A Study of Ebonyi State University, Abakaliki

Dr. Patrick N. Nwajioha[1] Uchenna Gideon Oshim[2]

[1& 2] Department of Educational Foundations, Eboyi State University, Abakaliki
uchennagideon007@gmail.com [1]nwajiohapatrick@yahoo.com 08162674899

Abstract

The alarming rate of cybercrimes, particularly in tertiary institutions in Nigeria has constituted a disturbing social problem that calls for urgent attention to curb the menace. This study focused on the application of digital technologies in combating cybercrime in Nigerian tertiary institutions; with particular reference to Ebonyi State University, Abakaliki. A descriptive survey research design was used for the study. The population of the study comprised of 5,259 four hundred level undergraduate students of the university. A sample size of 100 students was randomly drawn to participate in the study. Instrument for data collection was a researchers' structured questionnaire which was subjected to face validity of three experts. Data collected was analysed using mean score. The result showed that identification of unusual patterns of cyber-attack and discovering threat data from various sources are amongst the ways artificial intelligence powered systems will be effectively used to detect and prevent cybercrime in Nigeria tertiary institutions. The result also revealed that identification and prevention of malware infections, detecting and preventing unauthorized access to systems and networks are some of the roles of machine learning algorithms in combating cybercrimes in Nigeria tertiary institutions. The result also revealed that prevention of any attack that relies on stolen password, protecting sensitive information such as financial data, personal identifiable information are some of the roles of two-factor authentication in preventing cybercrimes in Nigeria tertiary institutions. Based on the findings, the study recommended among others that sensitisation on the application of digital technologies in combating cybercrimes should be regularly conducted in all the tertiary institutions in Nigeria; while calling for collaboration between ICT departments and cyber-security experts for smooth integration and maximising the benefits of digital technologies in tertiary institutions in Nigeria.

Keywords: Digital Technology, Artificial intelligence, Two-factor Authentication, Machine learning, Cybercrime.

Introduction

The swift adoption of digital technology (computers, smart phones, tablets, internet, etc) in Nigeria and the world generally has facilitated teaching and learning, business and other activities that are internet driven. The use of digital technology has no doubt impacted positively in everyday activities in the various sectors of human endeavours. The influence of digital technology in society has made it critical for all students in the 21st century to become literate with the use of digital tools, the development and proliferation of the internet have contributed to a revolution in teaching and learning (Hussaini, Ibrahim, Wali, Libata, Musa, 2020). It is argued that the emergence of internet has also provided new opportunities for delivering instruction through various media. The internet has brought about unprecedented breakthrough in every sphere of human endeavour in the world today; providing a medium for distance learning, online-learning, servicing as a source of income, enabling business transactions and online-business advertisement.

Pohekar (2018) stated that the emergence of computers has long made the world a global village because computers has shortened the distance, boost the economy and made learning easier and accessible even to a common man. However, Grynyshyna, Boiko, Boklan, Husakova & Pozniak (2023) stated that despite all the plentiful opportunities of learning through digital technology and improving access to education in the country at all levels, there are, however, some setbacks. The rapid growth, development and evolution of digital internet, including its global acceptance is generating increasing security threats to individuals, corporations, enterprise and the government as a whole. In Nigeria for instance, digital internet technology has made possible the perpetration of different forms of cybercrime on daily basis ranging from fraudulent electronic mails, advanced fee fraud 419 (Yahoonism or Yahoo-yahoo), sending spam email (spamming), stealing personal information (identity theft), breaking into someone's computer to view or alter data (hacking), and tricking someone into revealing their personal information (phishing), making internet services unavailable for users (Denial of service- DOS), credit card fraud (ATM), plagiarism and software piracy, pornography, stealing money bit-by-bit through tricks, virus dissemination, and so on. Rahman, Sairi, Zizi, & Khalid (2020) stated that undergraduates from tertiary institutions are capable of using computer and internet facilities for different kinds of cybercrime ranging from credit card fraud to pornography at the expense of their studies. Therefore, cybercrime covers every crime committed in cyberspace with the use of electronic equipment.

Hassan, Lass and Makinde (2012) conducted a systematic review of the literature on cybercrime prevention through technology and education. The authors found that technology and education play a critical role in preventing cybercrime and that a multi-layered approach that combines technology, education, and legal measures is necessary for effective cybercrime prevention. The continuity rate of cybercrime in Nigeria and other countries indicates that the traditional approach to cyber security is become ineffective in the 21 century, there is need for more effort to be channelled on the technological approaches such as Artificial intelligence, Machine learning algorithm, two-factor authentication, etc. towards combating cybercrimes in tertiary institutions and other sectors. This study sought to investigate the application of digital technology in combating cybercrimes in Nigerian tertiary institutions; a study of Ebonyi state University.

Statement of Problem

The incidences of cybercrime activities especially among students of tertiary institutions in Nigeria have become recurrent news on radios, televisions and social media platforms. Problems associated with cybercrimes especially in tertiary institutions are so threatening that stakeholders often watch helplessly as the standard of education continue to deteriorate. No doubt, the wave of cybercrimes has exposed the inadequacies of the traditional cyber security measures and consequently calls for innovative digital technology approaches to combat cybercrimes in Nigeria and the word over; hence the present study.

Purpose of the Study

The general purpose of this study is to examine the application of digital technologies in combating cybercrimes in Nigerian tertiary institutions, using Ebonyi state university as a case study. Specifically, the study sought to;

1. Find out how artificial intelligence powered system can be effectively used to detect and prevent cybercrime in Nigeria tertiary institutions.
2. Discover the roles of machine learning algorithms in combating cybercrimes.
3. Identify the roles of two-factor authentication in preventing cybercrimes.

Research questions

1. How can artificial intelligence powered systems be effectively used to detect and prevent cybercrime in Nigeria tertiary institutions?
2. What are the roles machine learning algorithms plays in combating cybercrimes in Nigeria tertiary institutions?
3. What are the roles of two-factor authentication in preventing cybercrimes in Nigeria tertiary institutions?

Conceptual Framework

Concept of Digital Technology

In the current world of technology**,** it is necessary to understand how digital technologies affect knowledge management and change educational paradigms. The use of digital technologies in higher education institutions has become increasingly prominent and influential, fundamentally reshaping various aspects of the educational landscape. The advent of online learning platforms and interactive software has expanded the boundaries of traditional learning. The digital technology education (internet) is one of the most revolutionary innovations of the 21st century. It has enabled instant information, transactions through e-mail, SMS, twittering, Google search, and video-conferencing. It has opened up doors and opportunities to free information, data and exposure as well as offering a cheaper information or data in educational sectors.

Many educational institutions have recently updated their online learning systems, creating favourable conditions for both non-traditional and traditional students and teachers to achieve their educational goals. Keser and Semerci (2019) noted that integrating digital technologies is not just an alternative that education institutions should consider but a key element of the educational process. In turn, using technology in higher education institutions establishes attitudes toward teaching and managing the educational process. Lucero, Victoriano, Carpio, Fernado (2021) argued that digital learning results from rational design and planning. The critical factor for successful integration is the competence of educators in determining when, where, and what practices to use. Student satisfaction is closely related to teaching approaches, and even teachers with no changes showed high levels of dissatisfaction.

The importance of successfully integration of digital technologies into the educational process largely depends on the ability of teachers to determine the optimal moments for their application, and it is also a great way to reduce costs and make better use of resources (Camilleri, Camilleri, 2017). Martin and Borup (2022) stated that the transition to online education provides certain benefits and prospects. Online platforms also provide modern communication and discussion, creating a conducive environment for academic interaction

In addition, digital technologies ensure the achievement of the goals and the intended result of educational activities (Keser and Semerci, 2019). Thus, technologies are used not only to conduct classes with students but also to increase the efficiency of the educational process through functions such as supervision, control, management, etc. Egoeze, Misra, Maskeliūnas, and Damaševičius (2018) noted that digital technologies are tools that improve the administrative activities of higher education institutions and transform teaching methods. Pohekar (2018) investigated various functional areas and found that using digital technology for data management in higher education institutions has an excellent impact on administrative services/management in universities. Haripriya, Chakravarthy and Siva Reddy, (2019) examined data collected from faculty and administrative staff of educational institutions who noted the positive use of digital trends in education.

Digital learning allows one to use various ways of providing educational materials. Hussaini, and Musa (2020) have shown that Google Classroom effectively improves student access and attentiveness to learning. The knowledge and skills gained through this digital learning platform make students active learners and provide meaningful feedback. In turn, many digital platforms are seen as the development of online learning using technology in a new normal environment for students and teachers, considering the use of Google Classroom, Zoom, Google Meet, Skype, etc. (Santiago and Callanta, 2021). The teaching process at all levels of education, including universities, has shown that most of the problems are related to Internet bandwidth and quotas (Grynyshyna, Husakova and Pozniak, 2023). The SWOT analysis showed that Zoom was most often used based on the analysis of teachers' practice.

Nevertheless, Microsoft Teams have significant potential for further development. From many perspectives, global involvement and active use of science and technology policies to achieve digital technology education goals should constitute the new focus and priority for technology policy advancement.

Cybercrime

Cybercrime is a combination of a prefix (cyber) which is used to express an idea as a component of the computer and information age, and root word (Crime) which can be defined as any activity that contravenes legal procedure mostly completed by individuals with criminal motive. The term cybercrime can be used to describe any criminal activity which involves the computer or the internet networks. It comprises of crimes such as fraud, theft, blackmail, forgery, and embezzlement, in which computers or networks are used. . Omodubbi (2013) cited Maitanmi who defined cybercrime as a type of crime committed by criminals who make use of a computer as tool and the internet as a connection in order to reach a variety of objectives such as illegal downloading of information and data, piracy, spam mailing and the likes. Chioma, (2017) defines cybercrimes as any activity in which computers or networks are used as a tool, a target or a place of criminal activity. Criminal activities done using computers and digital technology which include anything from downloading illegal data, or information or fraudulent electronic mails from the online sources.

Different authors have varying views but in simple terms, cybercrime encompasses all illegal activities carried out by a single or more individuals most times referred to as scammers, hackers, fraudsters, "419ners", using the internet through the medium of networked computers, telephones and other ICT equipment. Thus, the acts of cybercrime originated from the emergence of computers, telephones and other ICT inventions.

In today's era, numerous conventional crimes are being perpetrated with the use of ICT inventions. According to Ogwezzy (2012), the act of cyber criminality first occurred in the year 1820. This may not sound so strange, owing to the fact that Abacus as the oldest form of computer has been in existence since 3500BC in Asian countries such as China, India and Japan. Charles Babbage's analytical engine actually set the stage for sophisticated and new generation computers which suddenly became instruments of sabotage in the cyberspace. Joseph - Marie Jacquard, a textile manufacturer from France was at the center of activities that led to the act of first cybercrime, when he produced a device capable of performing all the duties of fellow employees in fabrics weaving. Other employees whose source of income was almost cut-off committed acts of sabotage to stop Jacquard from application of the new technology. This was the first recorded cybercrime (Parker, 2011)

Another dimension of the history of cybercrime holds that cybercrime first emerged in Russia and Eastern Europe where a significant number of students are good in mathematics, physics and computing (Ogwezzy 2012). Today, cybercrime has spread to every nooks and crannies of the world. Information and communication technology has become so indispensable in human life because of its numerous benefits, and ability to perform divers forms of work, thus providing comfort and convenience for mankind. But, all these benefits are marred by the attendant ills accompanying ICT inventions. Cybercrime is an evil capable of destroying the world when everything is fully automated.

In Nigeria, Ogwezzy (2012) holds that cybercrime which has become so prevalent in the country started as a small local fraud, where fraudsters on internet send email letters to their targets. These targets often become victims as the contents of such letters are usually too attractive to ignore. The Advanced Fee Fraud of today is similar to a much older scam known as the 'Spanish Prisoner Scam' in which the trickster informs the victim that a wealthy Prisoner promised to share treasure with the victim in exchange for money to bribe Prison Guards. An older version of this scam existed by the end of 18th Century and is called "the letter from Jerusalem" by Eugene Francois Vidocq in his memoirs. But what really made the Nigerian version of this trick as old as a major industry was the advent of the Internet. The modern technology of telecommunications and Internet cost-effective software collection, offers the potential for mass email. Over the past twenty years, the Nigerian fraudsters have grown from a small local fraud scheme, to one of the largest industries in Nigeria and all over the world. This trick in itself, is actually much older than it is expressed, dating back at least 300years (Ogwezzy, 2012)

Researchers have identified different types of cybercrimes to include among others:- **Auction fraud:** This is the misrepresentation of a product advertised for sale through an internet auction site, or the non-delivery of the products purchased through an internet auction site. The seller posts the auction as if he resides in the United States, then responds to victims with a congratulatory email stating he is outside the United States for business reasons, family emergency etc. They often post the auction under one name, and ask for the funds to be transferred to another individual or directly to him via Western Union, Money Gram or bank to bank wire transfer. By using these services, the money is virtually unrecoverable with no recourse for the victim.

Piracy: This is the act of illegally making access to people's soft copies such as, books, games, movies and CDs or DVDs, etc and make copies of same to disseminate for some gains which is usually financial gains.

Hacking: This is the act of cracking firewalls or security codes with the use of computers, laptops and sophisticated phones in order to gain access to people bank accounts, data or any other profitable information.

Ponzi/pyramid: This is a kind of money doubling scam. It is usually initiated as an investment for never to be received profits. Because it a bogus and attractive investment proposal, desperate individuals often fall victim. The victims of these scams neither receives dividends nor their initial capital

Credit card fraud: This involves illegal or unauthorised use of people's credit/debit cards to steal their money. Out of carelessness or negligence, victims usually compromise their credit/debit cards numbers to fraudsters, who actually get same from close observation or outright theft, sometimes on gun point. In Nigeria, such numbers are obtained in ATM withdrawal terminals or robbery at any location and pins are obtained on gun point.

Identity theft: This is the act of impersonation for the purpose of committing theft. Fraudsters usually fake the identity of individuals, organisations or governments to dupe persons who have legitimate businesses or transactions with such bodies. Victims are fooled through internet or other social networks such as Facebook, Skype, Whatsapp, blackberry pinging, etc.

Cyber terrorism: This is the process of launching computer based attack against computers, phones, networks and the information stored on them. Cyber terrorism is an act of terrorism committed through the use of Cyberspace or computer resources.

Internet time thefts: This is the act of manipulating or circumventing servers of network service providers in order to hack their passwords and gain login access. Fraudsters usually steal airtime from Internet Service Providers or GSM service providers, like the case that affected MTN Nigeria sometime in February 2009.

Web jacking: This is the process of fraudulently gaining access into individual's, corporate organisation or government websites or e-mails and completely taking charge or control of it. This is done by breaking through the passwords and other unique features, and editing same whereby the original owner may not be able to gain access again.

Phone phishing: Phishing attack also extends to phones such that messages claimed to come from a bank may tell users to dial a phone number regarding problems with their bank accounts, once the number (owned by the phisher, and provided by a voice over IP Service) has been dialled, prompts would tell users to enter their account numbers and Personal Identification Number (PIN) which the Phisher would use in defrauding the victim.

Sale of illegal articles: This is the process of selling contrabands or illegal products such as hard drugs or weapons of mass destruction through the use of internet websites, e-mails, short message services and other means of digital communication. .

Employment/business opportunity fraud: On the Internet different websites and most often 'pop-ups' on web pages have been design to advertise lucrative employment opportunities and businesses with the aim of defrauding unemployed persons.

Forgery: This is the act of counterfeiting an original document, made possible and easy by the emergence of information and communication technology. It is the act of faking an original money note or coin, or any other document to make it look similar or almost the same as the legal or original one. In Nigeria, there are a lot of forged certificates and naira notes.

Artificial Intelligence Powered System

Artificial intelligence is credited with transforming the field of cyber security and has taken it to another level by using superior skills to find incidents before they happen, including detecting, preventing, or responding to online menaces (Sarker, Janicke and Maglaras 2024).
With the help of artificial intelligence, cyber security systems can be used to recognize anomalies and doubtful activities immediately, thus enabling institutions to take first-hand measures to defend themselves against online fraud. Equally, significant historical information helps predict future risks that need to be dealt with in advance by organizations (Sarker et al., 2024).

Humans use conventional methods to recognize and mitigate threats. However, these tactics can be swamped by the magnitude and sophistication of cyber-attacks. Through real-time data analysis at a large scale, Artificial Intelligence (AI) may quickly identify suspicious trends, computer viruses, or traces that might indicate an imminent harmful intrusion into information systems (Kaur, Gabrijelčič and Klobučar, 2023). AI examine past information regarding cyber offenses and delicate areas to come up with future risks while ensuring there are areas with fewer security measures (Kaur et al., 2023) Systems with artificial intelligence can perform some parts of incidence response operations automatically, including isolating compromised machines, separating threats from other data, and alerting security agencies. As a result, the amount of time taken for containment is also reduced, making it easier for the victims' organizations to deal with potential loss (high level).

Roles of Machine learning (ML) Algorithms in Combating Cybercrime

Bharadiya (2023) asserts that the cyber world is growing fast and is playing an important role in daily life. It has become the centre of information in the modern world. This information needs to be protected from cyber-attacks through cyber security. As attack strategies to invade a network to steal or corrupt data are rapidly diversifying, traditional cyber security technologies like firewalls, etc are becoming obsolete. Hence, ML algorithms are being widely used instead to tackle cyber security issues due to their ability to adapt (Bharadiya, 2023).

Machine Learning is a progressive field of computational methods designed to emulate human intelligence by learning from the surrounding environment (Wolf, 2022), ML is the core of online safety and cyber security for the future. Its robust algorithms efficiently and consistently detect threats that are rendered blind by older security systems. The primary algorithms of ML are Graph Neural Networks (GNN), reinforcement learning, adversarial learning, and federated learning algorithms. All of these key ML subsets play crucial roles in ensuring the security of multiple applications; for example, federated learning algorithms are used in fraud detection, spam and phishing attacks, and intrusion detection systems. The wide functionality and security of the algorithms make ML greatly useful in businesses as it prevents the threat of personal data from being stolen from ransom ware gangs, saving companies and organisations billions of dollars every year (Wolf, 2022).

Roytman (2024) highlighted that the solid integration of machine learning algorithms inside the cyber security field enhances the ability to detect malware threats, analyse the behaviour, and respond to the threat in time. In addition, we can see that machine learning algorithms are improving the resilience of cyber security frameworks, such as improving the architecture process of building the software, and extending the capabilities of data protection to enhance the response behaviour. Roytman (2024), confirms that the integration of machine learning

algorithms will add value to the security framework to accurately address the nature and dynamic of cyber threats.

Use of Two-factor Authentication in Preventing Cybercrime

According to the study of Ritik Shivras, (2023), two-factor authentication (2FA) is a security process that requires users to provide two different types of information to access their account or device. This method provides an extra layer of protection beyond a simple username and password combination, making it more difficult for hackers or cybercriminals to gain unauthorized access to a user's account. The two factors used in 2FA typically include something the user knows, such as a password or PIN, and something the user has, such as a mobile device or security token. When a user logs in to their account, they will be prompted to provide their password or PIN as usual, and then they will be required to provide the second factor of authentication, such as a one-time code sent to their mobile device or generated by a security token. 2FA can help prevent cyber-attacks by adding a layer of security that is much more difficult for hackers to bypass. Even if a hacker manages to obtain a user's password, they will still need the second factor of authentication to gain access to the account. This extra layer of protection can be particularly important for sensitive accounts, such as those containing financial or personal information. Ritik and Shivras (2023), outlined some the benefits of Two-factor authentication (2FA) to include; Enhanced security, Protection against password theft, Easy to use, Compatible with multiple devices, Reduced fraud and unauthorized access to sensitive data.

Methodology

This study was conducted in Ebonyi State University (EBSU), EBSU is a multi-disciplinary University established by Ebonyi state government under (Ebonyi state university law no 7 (1999) in 14th January 2000. The design of the study was a descriptive survey. The population of the study comprised of 5,259 four hundred level undergraduate students of Ebonyi State University, Abakalii. A sample size of 100 students that are in 400 level in the department of computer science was drawn through a simple random sampling technique and used for the study. The instrument used for data collection was a structured questionnaire designed by the researchers. The questionnaire was structured in four point rating scale of Strongly Agree, Agree, Disagree and Strongly Disagree.To ensure the validity of the instrument used in the study. The researchers subjected the instrument to face validation involving three experts from Ebonyi State University Abakaliki. Their corrections were used to modify the instrument before the production of the final copies that was administered to respondents. Data were analyzed using mean score.

Results

Research Question 1;

How will artificial intelligence powered systems be effectively used to detect and prevent cybercrime in Nigeria tertiary institutions?

Table 1: The mean responses on how artificial intelligence powered systems will be effectively used to detect and prevent cybercrime in Nigeria tertiary institutions.

SN	Items	SA	A	D	SD	X	Remark
1	Identification of Unusual patterns that may indicate a cyber-attack.	35	25	22	18	2.8	Agree
2	Automatic incidence response to reduce the impact of cyber-attack.	40	30	18	12	3.0	Agree

3	Providing real-time alert and notifications to security team to enable them respond quickly to cyber attack	33	39	13	15	2.9	Agree
4	Discovering threat data from various sources.	35	34	17	14	2.9	Agree
5	Analyse user behaviour such as login attempts and access patterns to identify potential security threat.	32	20	26	22	2.6	Agree
	Grand mean					2.8	

From the result presented in table 1 above, respondents from item 1-5 had a grand mean of 2.8 which is above the mark of 2.5 and it shows that the respondents agreed on the listed ways artificial intelligence powered systems will be effectively used to detect and prevent cybercrime in Nigeria tertiary institutions.

Research Question 2;
What are the roles machine learning algorithms plays in combating cybercrimes in Nigeria tertiary institutions?

Table 2: The mean responses on the roles machine learning algorithms plays in combating cybercrimes in Nigeria tertiary institutions

SN	Items	SA	A	D	SD	X	Remark
1	Identification and prevention of malware infections.	39	33	16	12	3.0	Agree
2	Categorizing threats into different types for easy identification.	35	32	15	18	2.8	Agree
3	Providing recommendations for cybercrimes remedy and mitigation.	31	40	15	14	2.9	Agree
4	Detecting insider threats, such as staff or student with malicious intent.	30	33	16	21	2.7	Agree
5	Detects and prevents Unauthorized access to systems and networks.	39	27	18	16	2.9	Agree
	Grand Mean					**2.9**	

From the results presented in table 2 above, Respondents in items 1 -5 with the grand mean of 2.9 which is above the mark of 2.5 and it shows that respondents agreed on the listed roles machine learning algorithms plays in combating cybercrimes in Nigeria tertiary institutions.

Research Question 3
What are the roles of two-factor authentication in preventing cybercrimes in Nigeria tertiary institutions?

Table 3: The mean response on the roles of two-factor authentication in preventing cybercrimes in Nigeria tertiary institutions

SN	Items	SA	A	D	SD	X	Remark
1	Denying attacker's unauthorized access using only password.	40	30	16	14	3.0	Agree
2	Prevention of any attack that relies on stolen password.	37	34	15	14	2.9	Agree
3	Reduces the risk of identity theft.	33	37	17	13	2.9	Agree

4	Protects sensitive information such as financial data, personal identifiable information.	30	31	20	19	2.7	Agree
5	Reduces the risk of data breaches, which can result in significant financial losses.	28	32	17	23	2.6	Agree
	Grand mean					2.8	

From the result presented in table 3 above, it could be seen the table 3 had a grand mean of 2.8 which is above the mark of 2.5 and it show that the respondents agreed on the listed roles of two-factor authentication in preventing cybercrimes in Nigeria tertiary institutions.

Discussion of findings

Findings in table 1 revealed that identification of unusual patterns that may indicate a cyber-attack, Automatic incidence response to reduce the impact of cyber-attack, Providing real-time alert and notifications to security team to enable them respond quickly to cyber-attack, Discovering threat data from various sources, Analyse user behaviour such as login attempt and access patterns to identify potential security threat, are how artificial intelligence powered systems will be effectively used to detect and prevent cybercrime in Nigeria tertiary institutions. The findings agreed with the findings of Sarker et al. (2024), who stated that with the help of artificial intelligence, cyber security systems can be used to recognize anomalies and doubtful activities immediately, thus enabling institutions to take first-hand measures to defend themselves against online fraud. Equally, significant historical information helps predict future risks that need to be dealt with in advance by organizations

Findings in table 2 revealed that identification and prevention of malware infections, categorizing threats into different types for easy identification, providing recommendations for cybercrimes remedy and mitigation, detecting insider threats such as staff or student with malicious intent and detecting and preventing unauthorized access to systems and networks are the roles machine learning algorithms plays in combating cybercrimes in Nigeria tertiary institutions. The findings are in line with the findings of Roytman, M., (2024) who stated that the solid integration of machine learning algorithms inside the cyber security field enhances the ability to detect malware threats, analyse the behaviour, and respond to the threat in time.

Findings in table 3 revealed that denying attackers unauthorized access using only password, reducing any attack that relies on stolen password, reducing the risks of identity theft, protecting sensitive information such as financial data, personal identifiable information and reducing the risk of data breaches which can result in significant financial losses are the roles of two-factor authentication in preventing cybercrimes in Nigeria tertiary institutions.
The findings agree with the finding of Ritik Shivras (2023) who stated that two-factor authentication provides an additional layer of security beyond a simple username and password combination, making it much more difficult for hackers or cybercriminals to gain unauthorized access to a user's account or device.

Conclusion

Based on the findings of the study, the researcher concluded that inclusion of digital technologies such as artificial intelligence, machine learning algorithms, two-factor authentication to the traditional cyber security measures will help to drastically reduce the looming cybercrime activities in Nigerian tertiary institutions.

Educational implications

The study has the following Educational implications:

1. Cybercrimes in tertiary institutions can be drastically combated through the application of digital technologies such as Artificial intelligence, machine learning algorithms, two-factor authentication.
2. Both the staff and students of tertiary institutions in Nigeria need more knowledge of digital technology and the application to combat cybercrime.
3. The campaign against cybercrime in Nigerian tertiary institutions can only succeed if the use of digital technologies is added as part of cyber security measures.

Recommendations

In line with the findings of this study, the following recommendations are made to help combat cybercrimes in Nigeria tertiary institutions.

1. Cyber fraud prevention courses such as Artificial Intelligence, Machine Learning algorithms, two-factor authentication etc should be made compulsory in all tertiary institutions in Nigeria to educate students on how to identify cyber fraudsters and as well prevent their attacks on innocent citizens.
2. There should be collaboration between ICT departments and cyber-security experts for smooth integration and maximising of digital technologies in tertiary institutions in Nigeria; while ICT department of every tertiary institution in Nigeria should be properly equipped with computers and other necessary equipment that will enable the cyber security team function effectively.
3. Government should employ more digital technology experts into all the tertiary institutions to serve as cyber security team that will be actively checking and preventing any occurrence of cybercrime.

References

Bharadiya, J. (2023). Machine Learning in Cyber security: Techniques and Challenges. *European Journal of Technology*, [online] 7 (2), 1–14. doi: https://doi.org/10.47672/ejt.1486.

Chioma, C. O. (2017). Proliferation of cyber insecurity in Nigeria: A root cause of analysis. *International Journal of Science and Technology* (STECH), 6 (2). 14-55.

Egoeze, F., Misra, S., Maskeliūnas, R., & Damaševičius, R. (2018). Impact of ICT on universities administrative services and management of students' records: *International Journal of Human Capital and Information Technology Professionals*, 9 (2), 1-15. https://doi. org/10.4018/IJHCI

Grynyshyna, M., Boiko, T., Boklan, M., Husakova, N., & Pozniak, A. (2023). Comparative analysis of ways to integrate Microsoft Teams, Zoom, Google Meet into the educational process of higher education institutions of Ukraine. *Journal of Higher Education Theory and Practice*, 23 (2), 42-51. https://doi.org/10.33423/jhetp.v23i2. 5806

Haripriya, P., Chakravarthy, N. S., & Siva Reddy, I. V. (2019). Knowledge management practices in technical educational institutions using ICT tools of Rayalaseema Region in Andhra Pradesh. *International Journal of Recent Technology and Engineering*, 8(2S3), 1083- 1090. https://doi.org/10.35940/ ijrte.b1203.0782s319

Hassan, A. B., Lass, F. D., & Makinde, J. (2012). Cyber- crime in Nigeria: Causes, effects and way out. *International Journal of Science and Technology*. 2 (7), 626- 631 http://www.silicon.com, 2013)

Hussaini, I., Ibrahim, S., Wali, B., Libata, I. A., & Musa, U. A. (2020). Effectiveness of Google Classroom as a digital tool in teaching and learning: Students' perceptions. *International Journal of Research and Innovation in Social Science*, 4(4), 51-54. Retrieved from https:// www.rsisinternational.org/jour- nals/ijriss/Digital-Library/volume- 4-issue-4/51-54.pdf

Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023, September). Artificial intelligence for cyber security: Literature review and future research directions. *Information Fusion*, 97, 101804. https://www.sciencedirect.com/science/article/pii/S1566253523001136

Keser, H., & Semerci, A. (2019). Technology trends, education 4.0 and beyond. *Contemporary Educational Researches Journal*, 9(3), 39-49. https://doi.org/10.18844/ cerj.v9i3.4269

Lucero, H. R., Victoriano, J. M., Carpio, J. T., & Fernado, P. G. J. (2021). Assessment of e-learning readiness of faculty members and students in the government and private higher education institutions in the Philippines. *International Journal of Computing Sciences Research*, 5(1), 398-406. https://doi.org/10.25147/ ijcsr.2017.001.1.48

M. A., & Camilleri, A. C. (2017). Digital learning resources and ubiquitous technologies in education. *Technology, Knowledge and Learning*, 22, 65-82. https://doi.org/10.1007/s10758- 016-9287-7

Martin, F., & Borup, J. (2022). Online learner engagement: Conceptual definitions, research themes, and supportive practices. *Educational Psychologist*, 57(3), 162-177. https://doi.org/10.1080/0

Ogwezzy, M. C. (2012). Cybercrime and the proliferation of yahoo addicts in Nigeria. *International Journal of Juridical Sciences, No. 1 PP 86-102.* Available online at htpp://www.jurdicaljournal.univagora.ro. Visited 12thMarch, 2013.

Omodubbi, B. A., Esan, A. & Olaniya, O. (2016). Cyber- crime in Nigeria: Analysis, Detection and Prevention. *International Journal of Engineering and Technology*, 1 (1), p 38

Pohekar, D. (2018). Role of ICT on universities administrative services and management. *International Research Journal of Engineering and Technology*, 5(11), 266-271. Retrieved from https:// www.irjet.net/archives/V5/i11/ IRJET-V5I1149.pdf

Raman, Sairi, I., Zizi, N. A. M., & Khalid, F. (2020). The importance of cyber security education in school. *International Journal of Information and Education Technology*, 10(5), 378-382.

Ritik Shivras (2023) Cyber security professionals/5+YOE/Experts in threat detection, incident Response, Pen testing, Network security & vulnerability Assessment/ CEH, CNDA, CCNA-Security/ Python, Burp Suit, SIEM. Published March 2 2023.

Roytman, M ,(2024). The Future of AI and ML in Cyber security. Available at: https://www.forbes.com/sites/forbestechcouncil/2024/03/05/the-future-of-ai-and-ml-in-cybersecurity/ [Accessed on 20 Jun. 2024].

Santiago, C., Ulanday, M. L., Centeno, Z. J., Bayla, M. C., & Cal- lanta, J. S. (2021). Flexible learning adaptabilities in the new normal: E-learning resources, digital meeting platforms, online learning systems and learning engagement. *Asian Journal of Distance Education*, 16(2), 38-56. Retrieved from https://asianjde.com/ojs/index.php/AsianJDE/article/view/580

Sarker, I. H., Janicke, H., Mohsin, A., Gill, A., & Maglaras, L. (2024, August). Explainable AI for cybersecurity automation, intelligence and trustworthiness in digital twin: Methods, taxonomy, challenges and prospects. ICT Express.https://www.sciencedirect.com/science /article/pii/S2405959524000572

Wolf, A. (2022). *History of Cybercrime*. [Online] Arctic Wolf. Available https://arcticwolf.com/resources/blog/decadeofcybercrime/#:~:text=Technically%2C%20the%20first%20cyber%20attack [Accessed 19 Jun. 2024].