I. J. Engineering and Manufacturing, **2021, 4, 1-9**
Published Online August 2021 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijem.2021.04.01

Tree-classification Algorithm to Ease User Detection of Predatory Hijacked Journals: Empirical Analysis of Journal Metrics Rankings

Arnold Adimabua Ojugo
Department of Computer Science, Federal University of Petroleum Resources Effurun, Delta State, Nigeria.
Email: ojugo.arnold@fupre.edu.ng, arnoldojugo@gmail.com, maryarnoldojugo@gmail.com

Obinna Nwankwo
Department of Computer Science, Novena University, Ogume, Delta State, Nigeria
Email: tuk2obinna@gmail.com, obinna.nwankwo@novena.edu.ng

Received: 02 May 2021; Revised: 01 June 2021; Accepted: 14 June 2021; Published: 08 August 2021

Abstract: A major challenge today in communication and over various communications medium is the wanton havoc wreaked by attackers as they continue to eavesdrop and intrude. Young and inexperienced academia are today faced with the challenge of journal houses to send cum have their articles published. The negative impact thus, of predatory and hijacked journals cannot be over-emphasized as adversaries use carefully crafted, social engineering (phishing attack) skills – to exploit unsuspecting and inexperienced academia usually for personals gains. These attacks re-direct victims to fake pages. The significance of the study is to advance a standard scheme/techniques employed by phished (predatory/hijacked) journals to scam young academia and inexperienced researchers in their quest for visibility in highly impactful indexed journals. Thus, our study advances a decision-tree algorithm that educates users by showing various indicators cum techniques advanced by predatory and hijacked journals. We explore journal phishing attacks employed by such journals, targeted at young academia to adequately differentiate also using web-page ranking. Results show the classification algorithm can effectively detect 95-percent accuracy of journal phishing based on journal metric indicators and website ranks.

Index Terms: Phishing, predatory journals, decision tree, tree algorithm, social engineering

1. Introduction

The increasing need for e-commerce and the ineffective vigilance of such transactions has often constituted a fact – that fraudsters are also often steps ahead of genuine biz owners and users of a product always. Pre-empting fraudulent transactions prior its occurrence is quite possible in traditional non-automated tasks owing to our natural intelligence. But even with the advances so far made in in computing alongside the plethora of improved methods, intelligence and tools available – we are yet to proffer techniques to completely curb fraudulent activities [1-2]. Many of such fraudulent activities are crafted via social engineering skill and techniques [3]. The consequent use of intelligent systems however, is on the rise to detect phishing activities [4]. Though, the birth of online transactions and its increased functionality has given rise to more personal comfort; But, it has also attracted malicious persons interested in handsome rewards – endangering online transactions as easy targets for crime, which therein perpetrated are only discovered weeks afterwards [5].

Successful fraudulent methods in use include: (a) copying of user private data, (b) vendors deducting more money than agreed without users' consent or awareness [6-8], and (c) when banks lose money due to fraud, users partly and entirely (where possible) pay for such loss via higher interest rates, reduced benefits and higher membership fees. Thus, both banks and user must help via user education to reduce fraud [9, 10].

Some of the problems encountered by young academia and (inexperienced) researchers in general in their quest to publish their manuscripts and articles in renowned, high-impact and indexed journals includes: (a) phishing attacks as this opens their systems to other forms of compromises and attacks, (b) the unfortunate incident of being scammed by phished journal houses that claims high-impact of their journals even the journal is just a few years old, and (c) the unavailability of studies and frameworks/schemes and/or techniques that will further equips these researchers with the means to identify and detect these phished journals from the outset [3-5, 11].

Thus, the goal of this study is advance a decision tree-classification algorithm on the journal dataset – so as to provide a decision support system that helps young academia and researchers (in general) to effectively classify between genuine high-impact, indexed journals from predatory/hijacked journals using phishing attack metrics as a basis.

2. Literature Review

A. Social Engineering with Phished Journals

Surfing the internet alongside human interaction is hinged on decisions and its associated risks therein. As we interact thus, and make decisions, a certain level of logic and risk assessment is involved. We must become more rationale in our thinking and decision making so as to end up with effective choices that are based on objective factors [11-13]. Though, [14-15] showed that our decisions are often biased and influenced by emotions among other factors, as opposed to it being purely logical. An adversary pretends to be an authentic source in a transaction and fraudulently attempts to exploit data for monetary gain of a victim. Response to socially engineered attacks is considered a decision error – if the user does not correctly estimate the risks therein. Such response is often due to certain biases and behavioural influences. Scams have thus, continued to spread because victims have continued in their quest to fill the void in their personal traits. Phishing are deception techniques used by adversaries and modelled in such fashion that they always appeal to human vulnerabilities, such as in our desire for immediate gain, our desire to help people and desire to be liked by scammers. Studies also suggests that certain victims have personality traits that exposes them and makes them more susceptible and vulnerable to scam attacks – some of whom are even preys to repeated scams. A major factor that makes it more likely for certain people to become victim – is the lack of emotional control [16-18].

The study [19] notes that victims reported inability to resist such attacks due to persuasion and indiscriminate approach to offers they responded to – and, concludes that about 20% of the population were vulnerable as some became serial victims, who fell repeatedly for scams. Another study in a bid to investigate the underlying factors that contributes to such vulnerabilities in persons – sought to examine the relations between traits and scams [20], noted that persons with high score neuroticism may not detect fraud – since they possess they are generally upset when being lied to and prefer to believe that persons they come in contact with, are basically truthful (just to avoid emotional pain). Alternately, victims with high score in premeditation [21-22] showed high correlation capability to detect fraudulent offers. This fact remain disagreeable in that [20] states clearly that for personality traits to scams – persons who are agreeable are better equipped to detect lies; While, [21] stated that such agreeable persons were found to more likely fall for scams.

B. Young Academia and Predatory/Hijacked Journals

The term ‘predatory journal’ was first used by Jeffrey Beall of the University of Colorado [24] as he observed the growing number of exploitative academic journals that employed high article processing fee without proper quality checks of the submitted and soon-to-be published articles. He noted journals exploiting inexperienced authors as their prey and luring them via quick publishing of their manuscripts for a willing charge. Thus, predatory journals (or deceptive/scamming journals) seek to exploit, often young and inexperienced researchers of their unsuspecting author article processing fee under guise of quick article publishing; while leveraging on poor academic standard and practices in their peer-review as well as editorial processes. They often claim to live-up to established quality control standards in peer-review [25].

The rise in predatory journals have been attributed to the open access movement – that suddenly saw the skyrocket in number of new (online-only) publishers. This movement though sought to leverage on the benefits of the Internet; But, however, saw the demerit therein with the proliferation of predatory journals geared and poised towards financial gains at the expense of the publishing system. A rising trend now for predatory journals have been their imminent prograde to ***hijacked*** journals – in that they mimic cum impersonate established (legitimate) journals, usually in prints [24, 26-27].

C. Study Motivation

Our study is motivated thus [23, 25-26, 28-31]:

1. Rising quest trend in universities for greater visibility using webometrics ranking includes article publications in high impact, peer-reviewed journals indexed in many globally-accepted ranked databases – have necessitated this study, as such quest has exposed academia to susceptible phishing, and article submissions to hijacked journals (attacks).
2. Phishing detection is often limited, and its reporting unwise to describe in great details over public domain. This will equip attackers with data and capabilities to evade detection.
3. The unavailability of datasets and censored results – makes such detection tedious and sometimes, shown performance non-reliability. These are attributed to noisy data, parameter selection, mismatched feats and anomalies. Eliminating noisy feats via an accurately optimized classifier will thus, foster a more efficient network fraud prediction.

Thus, study seeks to advance a decision tree-classification algorithm onto the journal dataset – so as to provide a decision support system that helps young academia and researchers (in general) to effectively classify between genuine high-impact, indexed journals from predatory and hijacked journals using socially-engineered phishing attack metrics as a basis.

3. Materials and Methods

A. Journal Phishing

The basic framework to classify a journal as predatory is via certain attack feature(s). We will seek to formalize an approach-based classifier to detect predatory journal attacks. Scammers in a bid to present themselves as authentic, forge and redirects victims to their fake websites, which mimics a genuine website so as to steal victim's records. The fake journals (with no prior relations) leverages on the credibility of valid journals; And as in phishing attack – leans on financial motivations. Thus, they forge fake website mimicked after active journals with valid names, original features and ISSN values – and lure researchers to pay high sums to publish victim articles. Thus, the process of such socially-engineered, predatory journal and phishing attack is shown in Figure 1 [23, 26].

From figure 1, phished journal (referred to herein afterwards as the scammer) can opt and decide therein to either forge a predatory journal as well as hijack genuine journals in their bid to deceive young academia cum inexperienced researchers in general – who seek to become visible in their constant quest for visibility. The unsuspecting victim is sent an spam email(s) – to which he/she is asked and directed to submit paper articles to their predatory cum hijacked journal usually via the means of email attachment sent to the Journal Editor. Then, within a period of two/three weeks, the young researcher is sent an email on the acceptance of their paper article and is further directed to pay a token (usually as article processing fee) for the journal. The victim often pays only for his/her hopes of being visible dashed when he/she further notices that the journal claims high-impact even when their journal is just too recent and that the respectable indexing databases have no trace of the said journal [23-26].

Some of the webometric indicators for ranking journal sites includes: navigation, task orientation, overall usability, form and data entry, content quality, search usability, page layout and visual design, trust and credibility, help, feedback and error handling [11-13]. Thus, common feats as classified by previous studies is as observed in Table 1.

Table 1. Common Phishing Attacks In Predatory Journals

No	Features	Journal Phishing	Phishing Attacks
1	Socially-Engineering	Very high	Average
2	Financially motivated	Yes	Yes
3	Deceptive emails	Yes	Yes
4	Use same name/domain	Yes	Yes
5	Chosen targeted victims	Yes	Yes: Spear phishing
6	Fake website with short-life design	Short life span for fake journals	Short life span for phished websites
7	Exploit network protocol weakness e.g. in TCP/IP	Yes	Yes

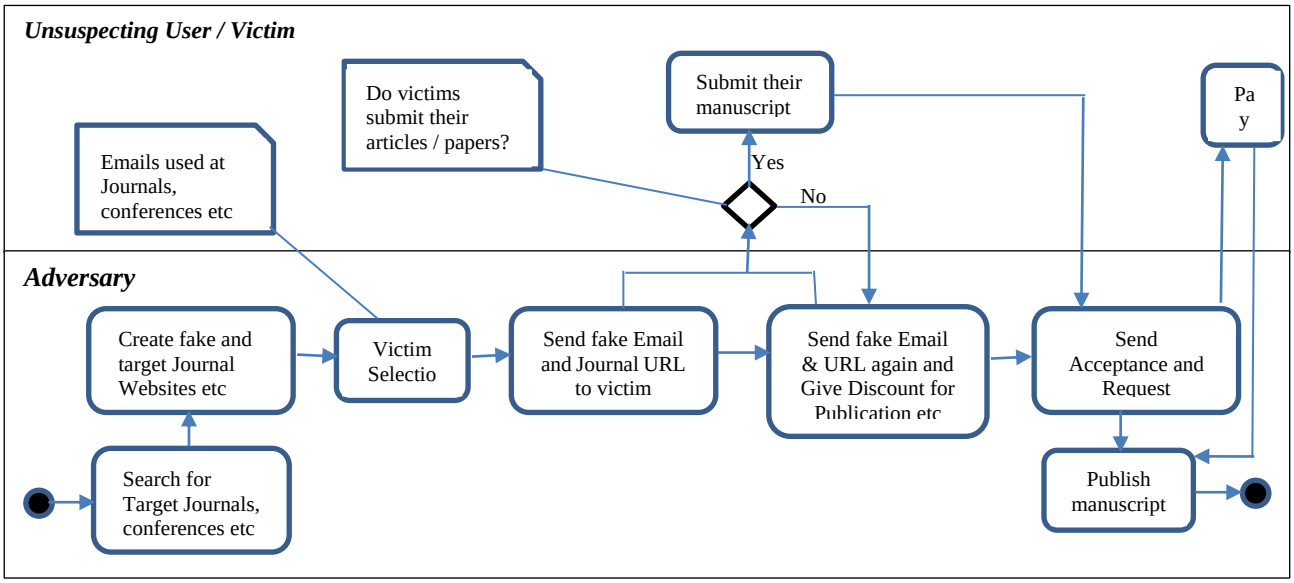

Fig. 1. The processes of a predatory/hijacked phishing journal attack on Young Academia

B. Data Gathering / Sampling

Dataset is compiled from known and unclassified indexed Journal databases. It contains about 54,803 records of known predatory hijacked journals and also genuine journals alongside their websites as its data contents. Sampled dataset is from 2016 – 2019. We seek to classify the data using process classification algorithm from Dadkhah et al [23] and Ojugo et al [29-32].

The classifying algorithm is applied thus: (a) apply selected data feats in table 2 to extract samples from dataset, and (b) use classified samples to make decision on future data, (c) compare results with benchmark algorithms C5, CHAID, QUEST, and C&R tree as supported by [23, 26]. Extracted samples are coded in tree-format [33]. To extract related journal feats, we sampled known hijacked journal(s) resources available on: (a) Beall's List (www.beallist.net / www.beallslist.weebly.com), (b) Yale University (https://guides.library.yale.edu), (c) Stop Predatory journals (www.predatoryjournals.com), and (d) ResearchGate (researchgate.net/List_of_Predatory_Journals_2019).

In furtherance of Dadkhah et al [23] – the scoring criteria for hijacked predatory journals is thus deduced from Table 2 as:

- ✓ Ranking – Predatory hijacked journals are a copy of a legal journal. Thus, if checked alongside website domain – we note they have no high ranks in search engine. For journal(s) without website, a search engine may detect a fake website instead of legal one (e.g. www.jokulljournal.com is hijacked Jokull journal). This journals has rank in Google as it has the capability to rank website based on page rank, which has a Boolean value in that if checked and website has ranking, its value is 1; Otherwise, it will be 0.
- ✓ External links checks websites codes structure. In the case that external links provide images with checked website content, the website is a suspected journal phishing because most of journal phishing use other websites copied content.
- ✓ Domain lifetime – From survey, hijacked journals phishing often register months before designing fake website. Thus, by using Whios databases, we can extract the time spent to archive journal articles and in turn, detect phishing journals. Suitable lifetime is measured by the first issue in journal.
- ✓ Indexed Journals –CiteFactor and Scopus databases is best when searching for journals to publish as most predatory, hijacked journals are now indexed in Thomson-Reuters (making it quite unsuitable for surveying).
- ✓ Sequence in search result adds to increased accuracy in detecting phishing pages. If journal title is inquired of by a search engine – it returns as its value, the website address.
- ✓ Entered countries to journal website – Studies shows known predatory hijacked journal websites target victims in certain countries like Nigeria. They can easily be detected by Alexa database (www.alexa.com) and classifying website guests based on the country.
- ✓ Archived/Previous issues – are usually not available, or just a few are. Phishers prevent user access to these archives via a login page. They also mention writers` names or paper subjects – since designing a website with previous issue requires time and because, forgers often do not have access to all the previous issues.
- ✓ Long URL – Most hijacked phishing journals use long URL to mask and hide doubtful parts on address bar. Since, there is no standard length to detecting legal URLs from illegal ones but normally, if a URL seems long this might belong to a phishing website.
- ✓ Journal aim / scope – Most phished journals accept papers with different subjects. Thus, they have general aim and scope. Thus, they use specific names that do not represent a subject area (like Walia or http://www.waliaj.com) or their subjects conclude varying research fields (like Journal of Technology).

C. Experimental Result

We use/score a 25-point 3-likert format checklist, to evaluate if journal is genuine or predatory/hijacked. The questionnaire guides experts and young inexperienced authors in considering journals to publish. A total of 100-authors (Scopus experienced authors and young authors) were chosen as participants from the ten (10) departments at the Federal University of Petroleum Resources Effurun in Delta State of Nigeria.

Table 2. Common Feats In Predatory Phishing Journals Attack

No	**Dependent Variables**	**1=Yes Agree**	**0=No Disagree**	**?=Not Clear**
Socially Engineered				
1	Very fast publication process which is often less than or between two (2) to four (4) months	78	18	4
2	No clear publication date or timeframe	56	35	9
3	Low cost of publication	94	6	-
4	Calls for article submission are done via Unsolicited/Open mails for authors to submit papers	99	1	-

5	Journals often claims high impact factor but relatively new in years of start of publishing	98	2	-
6	Transfer of Copyright is requested in some cases despite its Open Access state	56	35	1
7	Deceptive emails that also often end up in span folders	67	28	5
8	Email is non-professional or non-journal affiliated (e.g @gmail.com)	72	10	18
Journal History / Archive				
9	Has deceptive Domain Name	84	14	2
10	Journal is Rather New	92	6	2
11	Few paper from known and International authors	98	-	2
Adherence to Standard				
12	Undefined aim / scope	99	1	-
13	Article to be published are mostly submitted via mail	100	-	-
14	Published articles outside Journal scope	99	1	-
15	Very high acceptance rate	99	1	-
16	Published article with too many typos	98	1	1
17	Non-transparent policies	98	1	1
18	Publisher not member of COPE, STM, OASPA etc	99	1	-
19	Not indexed in Web of Science, CiteFactor, Scopus, PubMedCentral	100	-	-
Website Page Ranking				
20	Editor-In-Chief: same as many other journals in same publishing house	92	6	2
21	Poorly designed visuals for websites	98	2	-
22	No Address for Editorial Board/publisher	96	4	-
23	Journal listed in Beall's List and other Predatory journal	84	12	4
24	Fake website with short-life	94	6	-
25	Journal not known or read by colleagues	92	7	1

D. Discussion of Findings

Result notes that a suitable classification algorithm should be able to detect journal phishing attacks if provided the requisite (training) journal phishing dataset. This training dataset must include phishing websites in addition to legal ones to be able to detect original websites too. Thus, with our tree-classification algorithm, the key features of phishing journal and their usage possibility in detecting journal phishing attacks has been represented in Table 3. The feats with high-priorities of 1 must be selected as the tree-root. This is important as it is possible that one feat in the website cannot be measured. Thus, we can proceed to make our decision using a different feat as the tree-root. Note, that if the root feature changes, the decision tree will conversely, change.

Table 3. Priority Feats of Predatory Phished Hijacked Journals

N	Features	Kind	Measures	Priority
1	Domain Ranking	Logical	1 = Has page rank 0 = Without page rank	1
2	Use of External links	Discrete	L = External links < 2 M = External links 2< x <7 H = External links > 7	0.85
3	Domain Lifetime	Logical	0 = short lifetime 1 = long lifetime	1
4	Indexed Popular Database	Logical	1 = Indexed 0 = Not Indexed	0.997
5	Sequence in Searching Result	Discrete	L = Contained first 2 Result M = Contained 2 to 4 H = Other Results	0.96
6	Journal Website with Countries Notified	Discrete	H = Among 1 to 4 Countries M = Among 4 to 8 Countries L = More than 8 Countries NA = No information	1
7	Previous Issues Available	Logical	1 = Available 0 = Not Available	1
8	Long URL	Logical	1 = Long URL 0 = Suitable URL	0.85

9	Journal aim and scope	Logical	1 = General aim and scope 0 = Specific aim and scope	1
10	Adherence to aim and scope	Logical	1 = Yes 0 = Not Adhered to	1

E. Journal Phishing Measured Via Website Metrics

In advancing Ojugo and Eboka [11] and Ojugo and Otakore [13] – we propose the following guidelines for validating if a site is for a predatory or hijacked journal website as opposed to a genuine/original journal by scoring based on the following selected criteria namely:

a. Design Process relates to visual display and attractiveness of a site. The use of appropriate design of a website's pages, and the appropriate use of images, fonts and colors in the design of a site. It includes the aesthetic design, appropriate use of images, page design and its consistency.
b. Content refer to authentic research, employability, teaching and international outlook using author profile, citations, references to scholarly journals, the structure of sites' data content and how it is divided into logically, clear groups – with each group is associated with related information. It has simple navigation menus to aid users around its pages.
c. Navigation And Search – helps a user assess menu features. The links help facilitate effective navigation around pages of a website with no broken links and orphaned pages. A user can also request for data and safely acquire the desired data via a search option that can return the much desired data, appropriately to the user.
d. Credibility relates to data contents housed in the pages of the website being authenticated by renowned personnel.

With data obtained from both the various university website webmaster as well as the corresponding web server log data file as domiciled in these universities archive, the data therein are expressed in Figs 2 to 6 respectively.

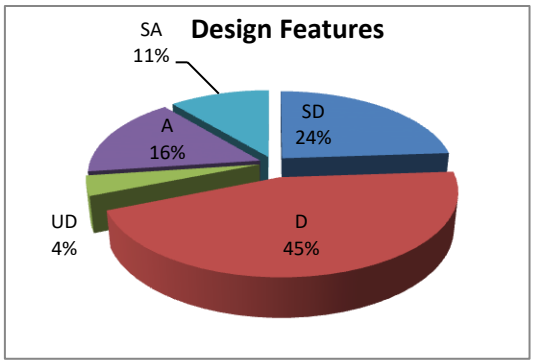

Fig. 2.Design Usability Features For Website

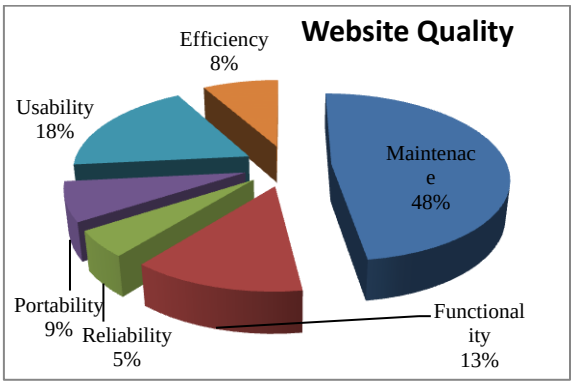

Fig. 3. Quality Features for Journals website

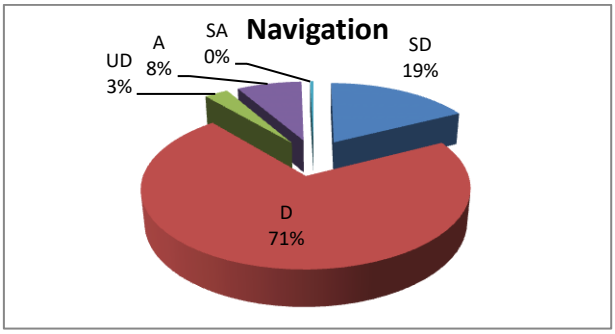

Fig. 4. Navigation Criteria

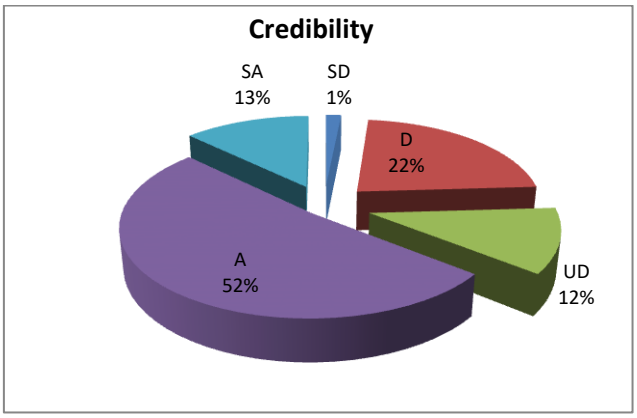

Fig. 5. Trust and Credibility of Website Usability

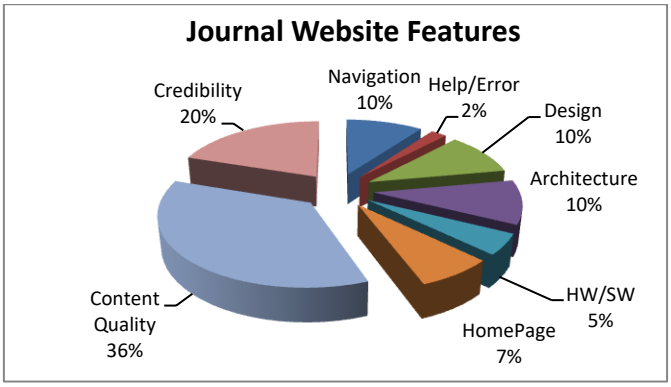

Fig. 6: Overall Website Usability for Journals in Nigeria

Websites now play prominent roles in education and training as millions of users visit them, searching for relevant data to meet their various research needs. It helps inexperienced and young researchers to interact between the various processes in trying to have their articles published. Website ranking and usability has become imperative in the qualitative assessment as it details the quality of research by the journals and its authors [33-36] – while, showcasing the online presence and footprint of authors over a period. Its primary aim is to help researchers make informed comparative choice about their various articles to be published and those that have also been consequently published. The ranking compares journals across 10-broad areas as in Table 3 alongside their respective priorities [37-41].

4. Summary and Conclusion

The ever-increasing adoption of the Internet and its usage for various transactions and online presence – has further advanced the ineffective vigilance of both researchers over such medium. Social engineering and adversaries have come to stay and they continually revise their mode of operations over time so as to seamlessly exploit unsuspecting users [34-39]. By being steps-ahead in their vigilance – adversaries will continue to leverage on social engineering methods due to human nature by default seeks to improve on their trust-level of technologies amongst other means that seek to improve their daily living. Thus, the need to protect clients via effective implementation of predictive fraud management and

prevention systems aimed at keeping at bay techniques such as phishing, vishing, keystroke logging – to mention a few [42-44].

Web presence is a trustworthy mirror, which avails us of its positive and direct relevance to a university ranking. The university that wishes to improve its position must enrich her website. This importance is seen both in university ranking criteria and website ranking, because there are both direct and indirect relevance between these two items.

References

[1] A.A. Ojugo., R.E. Yoro., Forging a deep learning neural network intrusion detection framework to curb distributed denial of service attack, Int. J. Elect. Computer Engr., Vol. 11, No. 2, pp 128-138, 2021

[2] A.A. Ojugo., A.O. Eboka., Empirical evaluation on comparative study of machine learning techniques in detection of DDoS, J. Applied Sci. Eng. Tech. & Edu., Vol. 2, No. 1, pp18–27, 2020, doi: 10.35877/454RI.asci2192

[3] L. Delamaire, H. Abdou, *Credit card fraud and detection techniques: a review*, Banks and Bank Systems, 4(2), pp57, 2009

[4] A.A. Ojugo, A.O. Eboka., R.E. Yoro., M.O. Yerokun., F.N. Efozia., Framework design for statistical fraud detection, *Mathematics and Computers in Sciences and Engineering Series*, 50: 176-182, 2015, ISBN: 976-1-61804-327-6.

[5] A.A. Ojugo., D. Allenotor et al., Comparative stochastic study for credit-card fraud detection models, African J. of Computing and ICT., 8(1-2): pp15 –24, 2015.

[6] V. Dheepa, R. Dhanapal, *Analysis of Credit Card Fraud Detection Methods*, Int. J. Recent Trends in Engr., 2(3), pp126, 2009.

[7] A.A. Ojugo., E. Ekurume., Predictive intelligence decision support model in forecasting of diabetes pandemic using a reinforcement deep learning approach, Int. J. Edu. and Mgt. Engr., 2021, 11(2), pp.40-48, doi: 10.5815/ijeme.2021.02.05

[8] S.J. Stolfo, D.W. Fan, W. Lee, A.L. Prodromidis, Credit card fraud detection using meta learning: issues and initial results, 2015, [online]: http://www.researchgate.net/publication/2282588

[9] I.P. Okobah., A.A. Ojugo., Evolutionary memetic models for malware intrusion detection: a comparative quest for computational solution and convergence, *IJCAOnline Int. J. Comp. Application*. Vol.179, No. 39. pp34–43, 2018

[10] A. Marane, Utilizing Visual Analysis for Fraud Detection, Understanding Link Analysis, 2011., [web]: linkanalysisnow.com/2011/leveraging-visual-analytics.html

[11] A.A. Ojugo., A.O. Eboka., Assessing user satisfaction and experience on academic websites: a case of selected Nigerian Universities websites, Int. J. Tech & Comp. Sci., 10(7): pp53-61, doi: 10.5815/ijitcs.2018.10.07, 2018

[12] A.A. Ojugo., D.O. Otakore., Redesigning academic website for better visibility and footprint: a case of Federal University of Petroleum Resources Effurun website, Network & Comm. Tech., 3(1): pp33–44, doi.org/10.5539/nct.v3n1p33, 2018b

[13] A.A. Ojugo., O.D. Otakore., Mitigating social engineering menace in Nigerian Universities, J. Comp. Sci. & Application, 6(2): pp64–68, doi: 10.12691/jcsa-6-2-2, 2018

[14] D. Kahneman and A. Tversky. Prospect theory: an analysis of decision under risk. *Econometrica*, March 1979.

[15] A.A. Ojugo., E. Ben-Iwhiwhu, O. Kekeje., et al., Malware propagation on social time varying networks: a comparative study of machine learning frameworks, Int. J. Modern Edu. Comp. Sci., 2014, 6(8): pp25-33, doi: 10.5815/ijmecs.2014.08.04

[16] J. Campbell, N. Greenauer, K. Macaluso, C. End. Unrealistic optimism in internet events, *Computers in Human Behaviour*, 23: pp1273–1284, 2007.

[17] B. Debatin1, J. P. Lovejoy et al., Facebook and online privacy: attitudes, behaviours, and unintended consequences. *Journal of Computer-Mediated Communication*, 15: pp83–108, 10 2009.

[18] S. Sheng, M. Holbrook, P. Kumaraguru, L. Cranor, and J. Downs. Who falls for Phish? Demographic analysis of phishing susceptibility and effectiveness of Interventions. *Proc. SIGCHI conf. on Human Factors in computing systems*, pp373–382, 2010.

[19] Univ. of Exeter School of Psychology. Psychology of scams: Provoking and committing errors of judgement. oft.gov.uk/shared_oft/reports/consumer_protection/oft1070.pdf.

[20] F. Enos, S. Benus, R. L. Cautin, M. Graciarena, J. Hirschberg, E. Shriberg. Personality factors in human deception detection: comparing human to machine performance. *INTERSPEECH - ISLP*, 2006.

[21] D. Modic., S.E. Lea. How neurotic are scam victims, really? The big five and Internet scams. *Security & Human Behaviour*, 2012.

[22] E.W. Khin, Employing Artificial Intelligence to Minimize Internet Fraud. Int. J. Cyber Society and Education, 2(1), pp.61-72, 2019

[23] M. Dadkhah., T. Sutikno, M.D. Jazi., D. Stiwan., An introduction to journal phishing and their detection approach. *Telkomnika*, 13(2), pp.373-280, doi: 10.12928/TELKOMNIKA.v13i2.1436, 2015

[24] R. Allen, The rise and rise of predatory journals. *University World News*, 19 October 2018.

[25] A.A. Ojugo., O. Nwankwo., Spectral-cluster solution for credit-card fraud detection using genetic algorithm trained modular deep neural network, Journal of Info. & Visualization, 2(1): pp , doi: 10.35877/454RI.jinav274, 2021.

[26] M. Dadkhah., G. Borchardt, Hijacked journals: an emerging challenge for scholarly publishing. *Aesthetic Surgery Journals*, 36: doi: 10.1093/asj/sjw026, 2016

[27] S. Eriksson., G. Helgesson., The false academy: predatory publishing in science and bioethics. *Medical Health Care & Philosophy*, 20: pp163, doi: 10.1007/s11019-016-9740-3, 2017

[28] A.A. Ojugo., O. Nwankwo., Forging spectral-clustering multi-agent hybrid deep learning model to predict rainfall runoff in Nigeria, Int. J. of Innovative Science, Engineering and Technology, 2021, 8(3), pp140-146

[29] A.A. Ojugo, A.O. Eboka., Comparative evaluation for high intelligent performance adaptive model for spam phishing detection, Digital Tech., 3(1): pp. 9-15, 2018

[30] A.A. Ojugo., A.O. Eboka., Signature-based malware detection using approximate Boyer Moore string matching algorithm, Int. Journal of Math. Sciences & Computing, 3(5): pp49-62, doi: 10.5815/ijmsc.2019.03.05, 2019

[31] A.A. Ojugo., O. D. Otakore., Forging optimized Bayesian network model with selected parameter for detection of Coronavirus in Delta State Nigeria, J. App. Sci. Eng. Tech. Edu., 3(1): pp37–45, 2021, doi: 10.35877/454RI.asci2163

[32] D.A. Oyemade., A.A. Ojugo., A property oriented pandemic surviving trading model, Int. J. of Advanced Trends in Comp. Sci. and Engr., 2020, 9(5): pp7397-7404
[33] R Kumar, R Verma. Classification Algorithms for Data Mining: A Survey. International Journal of Innovations in Engineering and Technology. 1(2): 7-14, 2012
[34] C. Chiu, C. Tsai, Web Services-Based Collaborative Scheme for credit card fraud detection, Proc. IEEE Int'l Conf. e-Tech, e-Commerce and e-Service, pp. 177-181, 2004
[35] C. Phua, D. Alahakoon, V. Lee, Minority Report in fraud detection: classification of skewed data, ACM SIGKDD Explorations Newsletter, 6(1), pp. 50-59, 2004
[36] C. Phua, V. Lee, K. Smith, R. Gayler, A comprehensive survey of data mining-based fraud detection research, 2007 [web]: www.bsys.monash.edu.au/people/cphua/ .
[37] A.A. Ojugo, A.O. Eboka., Memetic algorithm for short messaging service spam filter text normalization and semantic approach, Int. J. of Info. & Comm. Tech., 2020, 9(1): pp. 13 – 27, doi: 10.11591/ijict.v9i1.pp9-18
[38] R. Bolton, D. Hand, Unsupervised Profiling Methods for Fraud Detection. Credit Scoring and Credit Control VII, 2001
[39] T. Minahan, Fraud detection and prevention. 2013, [web]: nebhe.org/info/pdf/tdbank_breakfast/Fraud_Prevention_and_Detection.pdf
[40] A.A. Ojugo., R.E. Yoro., Extending three-tier constructivist learning model for alternative delivery: ahead covid-19 pandemic in Nigeria. Indonesian J. of Elect. Engr. & Comp. Sci., 21(3): pp1673-1682, doi: 10.11591/ijeecs.v21.i3.pp1673-1682
[41] A.A. Ojugo., R.E. Yoro., Empirical solution for an optimized machine learning framework for anomaly-based network intrusion detection, Tech. Report of Kansai University, TRKU-13-08-2020-10996, 2020, 62(10): pp6353-6364
[42] A.A. Ojugo, D.O. Otakore., Improved early detection of gestational diabetes via intelligent classification models: a case of Niger Delta, J. of Computer Sci. & Application, 2018, 6(2): pp. 82-90, doi: 10.12691/jcsa-6-2-5.
[43] A.A. Ojugo., A.O. Eboka., Mitigating technical challenges via redesigning campus network for greater efficiency, scalability and robustness: a logical view, Int. J. of Modern Education & Computer Sci., 6, pp29-45, 2020, doi: 10.5815/ijmecs.2020.06.03
[44] A.A. Ojugo., D.O. Otakore., Intelligent cluster connectionist recommender system using implicit graph friendship algorithm for social networks, Int. J. of Artificial Intelligence, 9(3): pp497~506, doi: 10.11591/ijai.v9.i3.pp497~506.

Authors' Profiles

Arnold Adimabua Ojugo received his BSc in 2000, MSc in 2005 and PhD in 2013 – all in Computer Science from The Imo State University in Owerri, The Nnamdi Azikiwe University in Awka, and The Ebonyi State University in Abakiliki. He currently lectures as an Associate Professor at the Department of Computer Science of the Federal University of Petroleum Resources Effurun in Delta State, Nigeria. His research interests are in: Intelligent Systems, CyberSecurity, and Graph Theory. He is also an Editor with various Journals and a member of: The Nigerian Computer Society, The Computer Professionals of Nigeria and International Association of Engineers (IAENG), Hong-Kong. He has six (6) children namely: Greg, Easterbell, Emmanuel, Eric, Elena and Elizabeth.

Obinna Nwankwo received his B.Sc in Computer Science in 2008 from the Cross River University of Technology Calabar, and M.Sc from University of Lagos, Akoka in 2011. He currently lectures with Department of Computer Science at Novena University Ogume, Delta State. His research interests are: Software Engineering. He is a member of: Nigerian Computer Society. He is married with a kid.

How to cite this paper: Arnold Adimabua Ojugo, Obinna Nwankwo, " Tree-classification Algorithm to Ease User Detection of Predatory Hijacked Journals: Empirical Analysis of Journal Metrics Rankings ", International Journal of Engineering and Manufacturing (IJEM), Vol.11, No.4, pp. 1-9, 2021. DOI: 10.5815/ijem.2021.04.01