尼日利亚银行系统中的网络安全和计算法

易卜拉欣·戈尼
尼日利亚 穆比 阿达马瓦州立大学理学院计算机科学系

摘　要：银行系统是任何国家的中枢神经系统，网络安全和计算法是银行系统的主要问题。这项研究工作的主要目的是检查尼日利亚银行系统中网络安全和计算法的效率，在这项调查中，使用了主要和次要数据，包括：本研究采用问卷调查、访谈和互联网等方法，采用相关和回归技术对数据进行分析，并使用卡方检验假设。从卡方（x^2）分布表中，显著性水平（0.05）下的自由度 3=7.815。由于计算出的 x^2 大于 x^2 统计值，即 9.389>7.815，因此否定零假设，接受替代假设。这意味着尼日利亚银行系统的网络安全法效率很高。

关键词：网络安全；计算定律；银行系统

Cyber Security and Computational Laws in Nigerian Banking System

Ibrahim Goni
Department of Computer Science, Faculty of Science Adamawa State University, Mubi, Nigeria

Abstract: Banking system is central nervous system of any nation and cyber security and computational law is a major problem of banking system. The main aim of this research work is to examine the efficiency of cyber security and computational laws in Nigerian banking system, in this survey research method were used both primary and secondary data were used which includes; questionnaire, interview and internet were used in this work the data were analyzed using correlation and regression technique and Chi-square were used to test the hypothesis. From the Chi-square (x^2) distribution table, the degree of freedom 3 under the level of significance (0.05) = 7.8 15. Since the x^2 calculated is greater than x^2 statistical value i.e. 9.389>7.815, the null hypothesis is rejected and the alternative hypothesis is accepted. This means there is an efficiency of cyber security law in the Nigerian banking system.

Keywords: Cyber security; Computational law; Banking system

1. 引言

1892 年，非洲银行合作组织（ABC）开始在拉各斯开展银行业务，一年后，英国西非银行（BBWA）在尼日利亚播下了银行体系的种子。然而，传统银行系统于 1952 年在尼日利亚开始。在银行倒闭期间，许多国家领导人主张建立尼日利亚中央银行，以监督银行，同时也是促进国家经济发展的工具。从那时起，该行业见证了《CBN 法案》和《银行法案》的大量监管和制度进步，一系列改革导致 80 家商业银行合并为 24 家实力更强的大型银行。这为该国的银行提供了一个基础，使其跻身非洲和世界上增长最快的银行联盟，预计 2004–2007 年间吸引了 34.8% 的资金流入非洲 [1]。

为了赶上全球发展，提高服务质量，尼日利亚银行无疑在技术上投入了大量资金；并广泛采用电子和电信网络来提供广泛的增值产品和服务。金融系统是每个经济体的中枢神经系统，尤其是银行业。它包括若干独立但相互关联的组成部分，所有这些都对其有效和高效运作至关重要。然而，尼日利亚银行业安全问题的后果至关重要。尼日利亚银行系统是否有计算法则？谁负责执行法律？客户知道计算法则吗？网络犯罪是一个挑战吗？尽管实施了当前应对银行欺诈的措施，以及现有的互联网银行法规，但网络欺诈在尼日利亚仍然非常普遍。这项工作的主要目的是检查尼日利亚银行系统中是否存在任何计算法，以及如何防止或更好地将尼日利亚银行的欺诈发生率降至最低。

网络安全是对数字信息及其所在基础设施的保护。最近，对与银行系统相关的计算法则和网络安全进行了大量研究，如 [2–9] 所示。[10] 认为，网络技术为特定金融机构带来了大量利润，网络攻击也对这些机构构成了严重威胁。研究建议，需要进行网络安全审计、网络安全培训、网络安全评估和加强安全。根据 [15]，2015 年网络犯罪事件的成本为 3 万亿美元，预计到 2021 将达到 6 万亿美元。在 [11] 中指出，2014 年，墨西哥是拉丁美洲网络攻击最多的国家，受害者约为 1000 万。根据 [12] 的说法，2017 年 5 月，印度银行不得不关闭 ATM，以应对勒索软件的威胁。2014 年卡塔尔国家网络安全战略报

告称，2013 年 11 月至 2014 年 3 月，中东和北非收到的短信数量位居第三（每月 17 亿条短信）。根据 [13] 的数据，2016 年，恶意网络活动使美国经济损失了 570 亿至 1090 亿美元。

在尼日利亚 [14] 发布了基于风险的网络安全框架和存款银行和支付服务提供商指南，该框架为管理网络安全风险提供了一种基于风险的方法。该文件包括六个部分：网络安全治理和监督、网络安全风险管理系统、网络韧性评估、网络安全运营韧性、网络威胁情报和度量、监测和报告。

在尼日利亚，关于计算法和网络犯罪的规定存在于以下法案中：

《经济和金融犯罪委员会成立法》（2015 年）。

1995 年《洗钱法》。

2004 年《洗钱（规定）法》。

1995 年《无提前欺诈和其他欺诈相关犯罪法》。

1994 年《破产银行（收回债务）和银行金融不良行为法》。

1991 年《银行和其他金融机构法》；以及《杂项犯罪法》。

如下图 [16] 所示，为信息系统、金融机构、企业和政府机构的可持续性提出了许多网络安全框架。

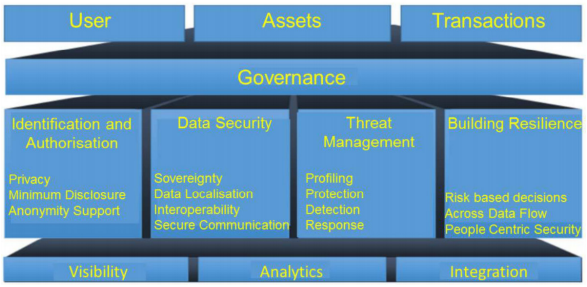

图 1. 网络安全框架。

2. 方法

众所周知的事实是，几乎在全世界，要获得研究工作的良好结果，取决于用于数据收集的仪器。因此，在这项调查研究中，使用的工具是问卷调查、口头访谈和观察。在这项研究工作中，用于分析数据的统计技术是相关性和回归分析。由于本研究变量的性质，相关性和回归分析是最佳选择。

3. 假设

无效假设（H_0）：通过尼日利亚的网络安全法，无法实现向客户提供银行服务的效率。

替代假设（H_1）：通过尼日利亚的网络安全法，实现了客户银行服务的效率。

替代假设（H_a）：尼日利亚通过使用计算法则实现了银行服务对客户的效率。

零假设（H_b）：尼日利亚通过使用计算法则实现银行服务对客户的效率。

4. 结果和讨论

本研究工作中收集的数据以表格形式呈现如下：共发放了一百二十（120）份问卷，仅有 82 份返回，将用于本研究工作。

Year	Respondents	Percentage
18-29	24	29.27%
30-39	25	30.49%
40-49	19	23.17%
50-59	9	10.98%
60 and above	5	6.09%
Total	82	100%

表 1. 受访者的年龄。

从上面的表 1 中可以看出，30 岁至 39 岁之间的受访者比例最高，其中 25 人预测的比例高达 30.49%，18 岁至 29 岁的受访者比例为 24 人，预测的比例为 29.27%，40 岁至 49 岁的受访者为 19 人，预测比例为 23.17%，而 50 岁至 59 岁的受访者中有 9 人预测的比率为 10.98%，60 岁及以上的受访者中，有 5 人预测的百分比为 6.09，如下图所示。

Year	Respondents	Percentage
Banker	20	24.39%
Civil servant	34	41.46%
Military/Paramilitary	15	18.29%
Others	13	15.85%
Total	82	100%

表 2. 受访者的职业。

从上表 2 可以看出，公务员的回答比例最高，为 34 人，占 41.46%；银行家为 20 人，占 24.39%；军事 / 准军事人员为 15 人，占 18.29%；其他受访者为 13 人，占 15.58%。

4.1 相关性和回归分析

使用由字母“r”表示的皮尔逊积矩相关性对数据进行分析，该相关性测量收集数据中两个变量之间的线性关系。从收集的数据来看，Yes 变量用 X 表示，No 变量用 Y 表示。以下是所使用的人员乘积公式：

$$r=\frac{n\Sigma xy-\Sigma x\Sigma y}{\sqrt{(n\Sigma x^2-(\Sigma x)^2(n\Sigma y^2-(\Sigma y)^2}} \quad (1)$$

其中：n= 值对的数量。

r= 皮尔逊相关系数。

0	324
0	324
0	324
65	25
0	324
0	324

X	Y	XY	X^2	Y^2
18	0	0	324	0
18	0	0	324	0
206	28	110	3598	394

表 3. 尼日利亚银行系统中网络安全和计算法的效率。

从上表 3 中可以看出，尼日利亚银行系统中的网络

安全和计算法是自变量（x），而尼日利亚银行系统的安全和计算法则的效率是因变量（y）。

根据上述等式（1）：

$$r=\frac{13\times110\times-206\times28}{\sqrt{(13\times3598-42436)(13\times394-784)}}$$

$$r=\frac{14030-5768}{\sqrt{(4338)(4338)}}$$

$$r=\frac{-4338}{\sqrt{18818244}}$$

$$r=\frac{-4338}{4338}$$

$$r=-1$$

4.2 调查结果的解释

银行系统中的安全和计算法与尼日利亚银行系统中安全和计算法律的效率之间存在着强烈的负面关系，这意味着尼日利亚银行系统对网络安全和计算法则的使用有所增加。

4.3. 假设测试和结果

使用卡方检验假设。使用了区间估计，它指定了一个范围内的值，在该范围内，可以通过某种度量来确定所估计的值位于何处。此值范围称为置信区间。

显著使用水平为 5% 0.05。

4.4. 假设一的检验

第一个假设如下：

无效假设（H_a）：在尼日利亚，通过使用网络安全法无法实现银行服务对客户的效率。

备选假设（H_b）：通过尼日利亚的网络安全法，实现了银行服务对客户的效率。

在测试这一假设时，研究使用了问题 1 至 6 的答案。六个问题中有四个是随机选择的，用于检验假设。

Variables	Q1	Q4	Q2	Q7	Total
Yes	18	18	15	18	69
No	0	0	3	0	3
Total	18	18	18	18	72

表 4. 尼日利亚银行系统的网络安全效率。

从上表 4 中，自由度为：d.f=（r－1）（c－1）。

其中：r= 原始数量。

C= 列数。

使用的公式是?

$$X2-text=\frac{\Sigma(0-E)^2}{E} \qquad (2)$$

其中：0= 观测频率。

E= 预期频率。

因此，d.f=（4－1）（2－1）=（3）（1）。

预期频率

期望频率（E）通过将总列乘以总原始值并除以总观测值来计算。

“是”的（E）计算为：

E=18 × 69=1242/72=17.25

对于“否”是：

E=18 × 3/72=54/72=0.75

X	Y	XY	X^2	Y^2
18	17.25	0.75	0.5265	0.333
18	17.25	0.75	0.5265	0.033
15	17.25	-2.25	5.0625	0.293
18	17.25	0.75	0.5625	0.033
0	0.75	-0.75	0.5625	0.75
0	0.75	-0.75	0.5625	0.75
3	0.75	2.25	5.0625	0.75
0	0.75	-0.75	0.5625	0.75

表 5. 预期的频率分布表。

上表 5 显示了 x^2=9.389 的计算值。从卡方（x^2）分布表中，显著性水平（0.05）下的自由度 3=7.815。由于计算出的 x^2 大于 x^2 统计值，即 9.389>7.815，因此否定零假设，接受替代假设。这意味着尼日利亚银行系统的网络安全法效率很高。

4.5. 假设二的检验

第二个假设是：

零假设（H_0）：在尼日利亚，银行服务对客户的效率不是通过使用计算法则实现的。

替代假设（H_1）：尼日利亚通过使用计算法则实现银行服务对客户的效率。

该假设的目的是通过在尼日利亚银行系统中使用计算法则，建立对客户的成就或非成就高效服务之间的差异。在测试这一假设时，研究使用了问题 7、6、13、9 和 11 的答案。

卡方技术被用来检验这个假设。

公式为：

$$x^2-test \qquad (3)$$

其中：0= 观测频率。

E= 预期频率。

确定自由度（d.f）时，使用以下公式：

$$d.f=(r-1)(C-1)$$

其中：r= 原始数量。

c= 列数。

尼日利亚通过使用计算法则实现了对客户的银行服务效率的假设。

Variables	Q7	Q8	Q9	Q11	Q13	Total
Yes	18	18	5	18	18	77
No	0	0	13	0	0	13
Total	18	18	18	18	18	

表 6. 尼日利亚银行系统的网络安全效率。

根据上表 6，自由度为：

$$d.f=(r-1)(c-1)=(4)(1)=4(4)$$

显著水平为 5%=0.05。

预期频率

预期频率（E）计算如下：

对于“是”：

E=18 × 77/90=15.4

“是”的预期频率为 15.4。

对于“否”=18 × 13/90=234/90=2.6。

“否”的预期频率为 2.6。

使用 x^2 - 测试计算如下：；

X	Y	XY	X^2	Y^2
18	15.4	2.6	6.76	0.439
18	15.4	2.6	6.76	0.439
5	15.4	-10.4	108.16	7.023
18	15.4	2.6	6.76	0.439
18	15.4	2.6	6.76	0.439
0	2.6	-2.6	6.76	2.6
0	2.6	-2.6	6.76	2.6
13	2.6	10.4	108.16	41.6
0	2.6	-2.6	6.76	2.6
0	2.6	-2.6	6.76	2.6

表 7. 尼日利亚银行系统的网络安全效率。

上表 7 显示了 x^2=60.78 的计算值。

从卡方（x^2）分布表中，d·f 4 下的显著水平（0.05）=9.488。

5. 结论

第一个假设试图测试银行向客户提供的服务的效率，是通过尼日利亚的使用安全法或其他方式实现的；第二个假设是通过尼日利亚或其他方式使用计算法实现银行向客户提供服务的效率。在仔细分析问题并以 5% 的显著性水平进行测试后，两个假设都接受了替代假设。这些数据表明，通过尼日利亚的使用安全和计算法，可以提高银行服务对客户的效率。尼日利亚银行系统的安全和计算法效率很高。研究表明，尼日利亚银行系统中存在计算法，EFCC 的引入有助于减少尼日利亚银行系统的网络犯罪。

致谢

我要感谢阿达马瓦州立大学木比分校为研究提供了指导环境。

参考文献

[1] F. Olubisi O., “History and evolution of banking in Nigeria”. academ arena Vol. 7 (1): pp. 9–14. 2015.

[2] O. Fadare A. “Impact of ICT tools for combating cybercrime in Nigeria online banking: A conceptual review” International Journal of Trade, Economics and Finance, Vol. 6 (5) 2015.

[3] S. Imran S. M. and R. Sana “Impact of Electronic crime in Indian Banking Sector - An Overview” International Journal Business Information Technology Vol. 1 (2). 2013.

[4] U. Basil “Dealing with the Challenge of Cybercrime in Nigeria under the new Cybercrime Act” The Lagos Chamber of Commerce & Industry 2015 Seminar of the Financial Services Group September 3, 2015.

[5] M. Usman and M. Irfan, “Information security risk assessment for banking sector–A Case study of Pakistani banks” Global Journal of Computer Science and Technology Vol. 10 (1) pp. 44. 2010.

[6] G. Marco, “Understanding cybercrime: Phenomena, challenges and legal response; ITU Telecommunication sector” 2012.

[7] B. Anah B., D. Funmi D. and M. Julius, “Cybercrime in Nigeria: causes, effects and the way out, ARPN Journal of Science and Technology VOL. 2, NO. 7, 2012.

[8] M. Aaron M., “A Case Study on E-Banking Security - WhenSecurity Becomes Too Sophisticated for the User to Access Their Information” Journal of Internet Banking and Commerce, Vol. 17 (2). 2012.

[9] O. Maitanmi O., S. Ogunlere, S. Ayinde, and Y. Adekunle.” Cybercrimes and cyber laws in Nigeria” The International journal of engineering and science (IJES) Vol. 2 (4) pp. 19–25. 2013.

[10] N. Tariq, “Impact of cyber–attacks on financial Institutions” Journal of Internet Banking and Commerce vol. 23 (2). Pp. 1–11. 2018.

[11] P. Luisa K., “The state of cyber security in Mexico: An overview. Wilson center Mexico institute pp. 1–23. 2017.

[12] Indian Bank Association, “Banking of the future: embracing technologies. EY Building a better working world”. 2018.

[13] The Council of Economic Advisers. “The Cost of Malicious Cyber Activity to the U.S. Economy CEA”. 2018.

[14] CBN, “Risk–Based Cyber security Framework and Guidelines” 2018.

[15] Cyber security ventures. “Hackerpocalypse: A cybercrime revelation” 2016.

[16] Y. Abdullahi S. “Emerging issues in cyber–crime: causes, implications and effects for the legal profession” Journal of social sciences research. Vol. 3 (7), pp. 169–180. 2014.