

A BIBLIOMETRIC ANALYSIS AND VISUALIZATION OF ACCOUNTING FRAUD DETECTION USING MACHINE LEARNING RESEARCH

Totok Dewayanto *)

Abstract

Background: Machine Learning technology used in the field of accounting has been widely studied by scholars all over the world. But there is little research on Accounting Fraud Detection Using Machine Learning (AFDUM) from the perspectives of bibliometrics and visualization, and the research topics and development trends in this field are still unclear.

Methods: This paper has applied bibliometric visualization software tools, R-Biblioshiny Package, to study the citation characteristics, international cooperation, author cooperation, and geographical distribution of the Accounting Fraud Detection Using Machine Learning (AFDUM).

Finding:

The literature data involved in this study are retrieved from the core collection of SCOPUS. A total 320 documents are obtained, and the most frequent document type is article of Business Management & Accounting subject area (181), Computer Science subject area (144), Economics, Econometrics and Finance (103), Decision Science (78), Social Sciences (47).

The bibliometric results reveal in terms of science mapping that the publications over the last 6 years (2015-2022) can be summarized to be focused in five research streams (1) financial system, (2) blockchain, (3) crime, (4) deep learning, (5) learning systems, (6) machine learning, (7) anomaly detection, (8) artificial intelligence, (9) risk assessment, (10) data mining.

Practical Implications:

The paper will identify the leading trends in the journal in terms of papers, authors,

*) *Accounting Department, Economic & Business Faculty, Diponegoro University*

institutions, countries, journals, topics and keywords. This study will enable readers achieve full understanding of the journal.

The hot topics in accounting fraud detection there is 3 frontier topics are learning system, financial system, and crime, and would be the foci of future research

Conclusion:

The present study provides a panoramic view of data mining methods applied in accounting fraud detection by visualization and bibliometrics. Analysis of authors, journals, institutions, and countries could provide reference for researchers who are fresh to the field in different ways. Researchers may also consider the emerging trends when deciding the direction of their study.

Originality/Value:

The study provides objective evaluation of the journal progress through a decade of its operation; it highlights the achievement and discusses the progress and contribution of the journal to the scientific research.

Keywords: **bibliometric analysis, bibliometrix, medical data mining, visualization, R-Biblioshiny**

Introduction

Not to mention some cooperate accounting scandals happened in home country or abroad, the misreporting of financial information (so-called “falsification of financial statements”) is a serious economic event that should be avoided from practical point of view. The misreporting of listed firms’ financial information, in particular, distorts the

decision-making of various economic entities involved in financial transactions such as stock, bond trading as well as bank lending, resulting in inefficient resource allocation.

In real business relationships, such misreporting may also result in excessive risk-taking that neither the customer nor the supplier recognizes. As a result, when this risk becomes apparent, unintended stagnation of economic activities may occur. Even more serious, when such misreporting is intentional (so-called “accounting fraud”) and occurs frequently, financial activities and real economic activities could not be properly initiated from the outset (i.e., market breakdown).

These problems caused by accounting fraud are not necessarily limited to business activities but, rather, extends to policy management. Corporate financial information is referenced in various policy interventions such as the provision of subsidy to small and medium size enterprises. If a company's information observed from outside does not represent the reality, its intended policy may not be implemented correctly.

Accounting fraud is a worldwide problem. If not detected and prevented on a timely

basis, it can cause significant harm to the stakeholders of fraudulent firms (e.g., Enron and WorldCom) as well as the stakeholders of many nonfraudulent firms indirectly (Gleason, Jenkins, and Johnson [2008], Goldman, Peyer, and Stefanescu [2012], Hung, Wong, and Zhang [2015]). Unfortunately, accounting fraud is difficult to detect. Moreover, even if it is detected, serious damage has usually already been done (Dyck,

Morse, and Zingales [2010]). Hence, efficient and effective methods of corporate accounting fraud detection would offer significant value to regulators, auditors, and investors.

The objective of this study is to develop a new accounting fraud prediction model out of sample by using readily available financial statement data from publicly traded U.S. firms. Following Cecchini et al. [2010], and Dechow et al. [2011], we use the detected material accounting misstatements disclosed in the SEC's Accounting and Auditing Enforcement Releases (AAERs) as our accounting fraud sample. Although there are useful nonfinancial predictors of accounting fraud (e.g., an executive's personal behavior), we use only readily available financial data for two reasons.

First, fraud prediction models based on publicly available financial data can be applied to any publicly traded firm at low cost. Second, most of the fraud prediction models in the existing accounting literature also rely on publicly available financial data (e.g., Green and Choi [1997], Summers and Sweeney [1998], Beneish [1999], Cecchini et al. [2010], Dechow et al. [2011]). By limiting the predictors to financial data only, the performance of our fraud prediction models can be compared with the performance of

such existing models.

There is a fairly large accounting literature on the determinants of accounting fraud (e.g., Entwistle and Lindsay [1994], Beasley [1996], Dechow, Sloan, and Sweeney [1996], Beneish [1997, 1999], Summers and Sweeney [1998], Efendi, Srivastava, and Swanson [2007], Brazel, Jones, and Zimbelman [2009], Dechow et al. [2011], Schrand and Zechman [2012]), but the primary objective of most studies is to explain fraud within sample and often emphasize causal inference. Our objective is different: We wish to develop a model that can accurately predict accounting fraud out of sample (i.e., a prediction problem). Shmueli [2010] shows that the problems of causal inference and prediction, although related, are fundamentally different. Specifically, the objective of causal inference modeling is to minimize the bias resulting from model misspecification to obtain the most accurate

representation of the underlying theory. In contrast, the objective of predictive modeling seeks to minimize out-of-sample prediction error, that is, the combination of the bias and estimation variance that results from using a sample to estimate model parameters. Although causal inference represents the main stream of existing social science research, Kleinberg et al. [2015] show that there are many interesting prediction problems that are neglected in the extant business and economics literatures.

We use two types of fraud prediction models from the extant literature as benchmarks. The first is ratio-based logistic regression, commonly used in the accounting literature (e.g., Beneish [1997, 1999], Summers and Sweeney [1998], Dechow et al. [2011]). Such models typically use financial ratios as predictors; the ratios are often identified by human experts based on theories (e.g., the motivation-ability-opportunity framework from the criminology literature). Among these models, the model in Dechow et al. [2011] is generally regarded as the most comprehensive fraud prediction model in accounting literature. Accordingly, we adopt a similar logistic regression model as our first benchmark model (referred to as the Dechow et al. model). The second benchmark model is a fraud prediction model developed by Cecchini et al. [2010] based on a more advanced machine learning method (hereafter referred to as the Cecchini et al. model).

Rather than using the financial ratios identified by human experts alone, Cecchini et al. [2010] develop a new fraud prediction model based on support vector machines (SVM) with a financial kernel that maps raw financial data into a broader set of ratios within the same year and changes in ratios across different years. Cecchini et al. [2010] find that the SVM with a financial kernel outperforms the traditional fraud prediction models in accounting, including the Dechow et al. model.

Our proposed fraud prediction model differs from both of these benchmark models in two key ways.

First, we use ensemble learning, a state-of-the-art machine learning paradigm, to predict fraud. Most prior fraud prediction research in accounting uses the logistic regression (see Dechow et al. [2011] for a review). Although ensemble learning has been successfully applied in many other fields (see Zhou [2012] for a review), ours is the first study to apply the method to an accounting setting with a severe class imbalance problem (i.e., the rarity of fraud). Fernandez-Delgado et al. [2014] show that there is no universally best model across all data settings; hence, it is an empirical question whether the ensemble learning method can outperform the traditional fraud prediction methods in our special setting.

Second, our proposed model uses raw financial data items, taken directly from financial statements, as fraud predictors. Because raw financial data items are the most fundamental building blocks of the accounting system, it is interesting to explore whether they can be directly used in fraud prediction.

Ex ante, it is unclear whether fraud prediction models based on raw financial data can outperform fraud prediction models based on human expert-identified financial ratios. On the one hand, fraud prediction models based on financial ratios could be more powerful because the ratios identified by human experts are often grounded in theories that offer sharp prediction on when corporate managers have incentives to engage in fraud. Because fraud prediction models based on raw financial data are not directly linked to theory, they may be less powerful. On the other hand, existing theories about the drivers of accounting fraud may well be incomplete, as accounting fraud is, by definition, conducted in secrecy and designed to be difficult to detect. Accordingly, converting raw accounting data into a limited number of financial ratios based on potentially incomplete behavioral theories could mean the loss of useful predictive information.

In contrast, fraud prediction models that make use of raw financial data could be more powerful because they do not impose any ex ante structure on the raw data, instead letting them “speak for themselves.” In addition, with the rapid advance of machine learning methods in computer science, fraud prediction models based on raw data can take on more flexible and complex functional forms. As a result, such fraud prediction models may be able to extract more useful information from raw data. Because of these conflicting trade-offs, we believe it is an empirical question on whether our proposed ensemble learning model based on raw data can outperform the two benchmark models based on financial ratios.

Machine Learning is a branch of Artificial Intelligence (AI) where computer algorithms improve and “learn” automatically through the use of training data. These models can then be used to make predictions or decisions about new datasets.

Machine learning for fraud detection works by analyzing consumers’ current patterns and transaction methods. It can analyze these behaviors faster and more efficient than any human analysis and as a result, it can quickly identify if there is a deviation from normal behavior. This allows for opportunities in real-time approval by the user before a transaction can be complete.

Machine learning also has the benefit of increased accuracy since human error in recording or analyzing data is eliminated from the equation. Furthermore, better predictions can be achieved since machine learning models are able to process massive amounts of data. The more data supplied to a model the more the model has to learn from and can create even better predictions.

Finally, machine learning is a fairly cost-effective detection technique for companies. Data can be analyzed in milliseconds and team members aren't burdened with manual review and checks every time new data is acquired.

Bibliometrics is the cross-disciplinary science of quantitative analysis of all knowledge carried by mathematical and statistical methods. In light of bibliometric methods, the latest advances, leading topics, current gaps in a certain field of research discipline can be drawn vividly as well as geographically, and it is becoming an import research method for assessing national and international research productivity, international cooperation, citation analysis, research trends, and development of specific fields. At present, many bibliometric analysis methods and tools like CiteSpace and VOSviewer have been developed to help researchers in different field construct knowledge maps, evaluate the collective state of thought about a subject, and identify hotspots in a research field.

In this paper, we use free available R-Biblioshiny Package to carry out the visualized map, and to generate diagrams and calculate the betweenness centrality score. The literature on the application of machine learning technology in the accounting fraud detection field from the SCOPUS database has analyzed to provide a macroscopic overview on the main characteristics of AFDUM publication. And clear informative pictures presented in this paper demonstrate the research achievements in the domain of the AFDUM, which could help researchers and practitioners identify the underlying impacts from authors, journals, countries, institution, references, and research topics. Although this work is not structured as an exhaustive analysis of AFDUM-related literature, it does illustrate the utility of bibliometric techniques for exploring hidden knowledge spaces.

The goal of the current study was to review the extant literature on machine learning technology in the accounting fraud detection field Thus, the following research questions were established:

RQ1. What research has been done in the field of accounting fraud detection in the context of using machine learning, in terms of the definitions, theories, research themes, research methodologies and settings?

RQ2. What are the future research agendas in the accounting fraud detection field?

Data and methods

Data collection

The literature data involved in this study are retrieved from the core collection of SCOPUS.[5] The SCOPUS is one of the most comprehensive bibliographic sources available, and provides users an online access port to a number of resources, including massive citation databases, but not all journals or articles are indexed.[6]

For the purpose of this paper, we are interested in exploring the knowledge domain associated with “accounting fraud detection using machine learning,” and use “accounting fraud detection using machine learning” as the search term in the SCOPUS database, the literature type is defined as “all types.” For assuring the quality of data, a manual review on search results is adopted in Mendeley to remove the unrelated papers[7] is used to identify and correct all duplicate values in the databases.

The decision was to find the suitable field (i.e. title, abstract and full-text) to apply the search string on. In our experience, searching in the ‘title’ alone does not always provide us with all relevant publications. Thus, ‘abstract’ or ‘full-text’ of publications should potentially be included. On the other hand, since the search on the full-text of studies results in many irrelevant publications, we chose to apply the search query additionally on the ‘abstract’ of the studies. This means a study is selected as a candidate study if its title or abstract contains the keywords defined in the search string.

Accounting AND fraud AND detection AND using AND machine AND learning AND (EXCLUDE (EXACTSRCTITLE, "Pervasivehealth Pervasive Computing Technologies For Healthcare") OR EXCLUDE (EXACTSRCTITLE, "Betriebswirtschaftliche Forschung Und Praxis") OR EXCLUDE (EXACTSRCTITLE, "International Journal Of Emerging Technology And Advanced Engineering")) AND (EXCLUDE (PUBYEAR, 2014) OR EXCLUDE (PUBYEAR, 2013) OR EXCLUDE (PUBYEAR, 2012) OR EXCLUDE (PUBYEAR, 2011) OR EXCLUDE (PUBYEAR, 2010) OR EXCLUDE (PUBYEAR, 2009) OR EXCLUDE (PUBYEAR, 2008) OR EXCLUDE (PUBYEAR, 2007) OR EXCLUDE (PUBYEAR, 2006) OR EXCLUDE (PUBYEAR, 2005) OR EXCLUDE (PUBYEAR, 2004) OR EXCLUDE (PUBYEAR, 2003) OR EXCLUDE (PUBYEAR, 2002) OR EXCLUDE (PUBYEAR, 2001) OR EXCLUDE (PUBYEAR, 2000) OR EXCLUDE (PUBYEAR, 1999) OR EXCLUDE (PUBYEAR, 1996) OR EXCLUDE (PUBYEAR, 1995) OR EXCLUDE (PUBYEAR,1993) OR EXCLUDE (PUBYEAR, 1992) OR EXCLUDE (PUBYEAR, 1991)) AND (EXCLUDE (DOCTYPE, "cp") OR EXCLUDE (DOCTYPE, "bk") OR EXCLUDE (DOCTYPE, "re") OR EXCLUDE (DOCTYPE, "ch") OR EXCLUDE (DOCTYPE, "ed") OR EXCLUDE (DOCTYPE, "cr") OR EXCLUDE (DOCTYPE, "no") OR EXCLUDE (DOCTYPE, "le") OR EXCLUDE (DOCTYPE, "Undefined")) AND (EXCLUDE (SUBJAREA, "ENGI") OR EXCLUDE (SUBJAREA, "MATH") OR EXCLUDE

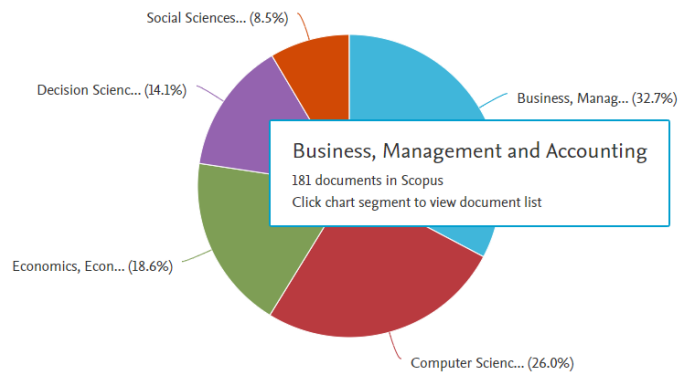
(SUBJAREA, "MATE") OR EXCLUDE (SUBJAREA, "PSYC") OR EXCLUDE (SUBJAREA, "MEDI") OR EXCLUDE (SUBJAREA, "ENER") OR EXCLUDE (SUBJAREA, "ARTS") OR EXCLUDE (SUBJAREA, "ENVI") OR EXCLUDE (SUBJAREA, "PHYS") OR EXCLUDE (SUBJAREA, "AGRI") OR EXCLUDE (SUBJAREA, "BIOC") OR EXCLUDE (SUBJAREA, "MULT") OR EXCLUDE (SUBJAREA, "CENG") OR EXCLUDE (SUBJAREA, "NEUR") OR EXCLUDE (SUBJAREA, "EART") OR EXCLUDE (SUBJAREA, "CHEM") OR EXCLUDE (SUBJAREA, "HEAL") OR EXCLUDE (SUBJAREA, "PHAR") OR EXCLUDE (SUBJAREA, "IMMU") OR EXCLUDE (SUBJAREA, "NURS")) AND (EXCLUDE (LANGUAGE, "Chinese") OR EXCLUDE (LANGUAGE, "Portuguese") OR EXCLUDE (LANGUAGE, "Spanish") OR EXCLUDE (LANGUAGE, "German") OR EXCLUDE (LANGUAGE, "French") OR EXCLUDE (LANGUAGE, "Hungarian") OR EXCLUDE (LANGUAGE, "Turkish")) AND (EXCLUDE (SRCTYPE, "p") OR EXCLUDE (SRCTYPE, "b") OR EXCLUDE (SRCTYPE, "k") OR EXCLUDE (SRCTYPE, "d"))

Finally, 320 documents are saved as “Plain Text” with “Full Record and Cited References.” And the timespan is from January 1, 2015 to January 1, 2022, which including information on title, author, keywords, abstract, journal, and year. These records are then exported to R-Biblioshiny for subsequent analysis, and 5 document types are found.

A total 320 document are obtained, and the most frequent document type is article of Business Management & Accounting subject area (181).

Subject area ↓	Documents ↓
Business, Management and Accounting	181
Computer Science	144
Economics, Econometrics and Finance	103
Decision Sciences	78
Social Sciences	47

Documents by subject area



Description	Results
MAIN INFORMATION ABOUT DATA	
Timespan	2015:2022
Sources (Journals, Books, etc)	101
Documents	181
Average years from publication	1.81
Average citations per documents	14.46
Average citations per year per doc	4.039
References	1
DOCUMENT TYPES	
article	181
DOCUMENT CONTENTS	
Keywords Plus (ID)	370
Author's Keywords (DE)	690
AUTHORS	
Authors	524
Author Appearances	565
Authors of single-authored documents	17
Authors of multi-authored documents	507
AUTHORS COLLABORATION	
Single-authored documents	18
Documents per Author	0.345
Authors per Document	2.9
Co-Authors per Documents	3.12
Collaboration Index	3.11

Sources	Articles
INTELLIGENT SYSTEMS IN ACCOUNTING FINANCE AND MANAGEMENT	10
INTERNATIONAL JOURNAL OF ACCOUNTING INFORMATION SYSTEMS	9
ACCOUNTING HORIZONS	7
INTERNATIONAL JOURNAL OF DIGITAL ACCOUNTING RESEARCH	7
JOURNAL OF MANAGEMENT INFORMATION SYSTEMS	7
JOURNAL OF INFORMATION SYSTEMS	5
JOURNAL OF INFORMATION TECHNOLOGY	5
KNOWLEDGE-BASED SYSTEMS	5
REVIEW OF ACCOUNTING STUDIES	5
ELECTRONIC COMMERCE RESEARCH AND APPLICATIONS	4
INFORMATION SYSTEMS RESEARCH	4
FINANCIAL INNOVATION	3
INTERNATIONAL JOURNAL OF FINANCE AND ECONOMICS	3
JOURNAL OF ACCOUNTING RESEARCH	3
JOURNAL OF BUSINESS RESEARCH	3
JOURNAL OF EMERGING TECHNOLOGIES IN ACCOUNTING	3
ACCOUNTING AND BUSINESS RESEARCH	2
ACCOUNTING AND FINANCE	2
BANKS AND BANK SYSTEMS	2
BIG DATA AND COGNITIVE COMPUTING	2

Analysis methods

According to (Pritchard, 1969) bibliometrics is the application of statistical methods to the study of bibliographic data. It is beneficial to screen the intellectual structure of any scientific field using quantitative methods (Hota, Subramanian and Narayanamurthy, 2019), It is the most widely used method for constructing a broad overview of a journal (Bar-Ilan, 2008). Bibliometrics help to explore, organize and analyze large amounts of data (Lezama-Nicolás et al., 2018), through this technique it is possible to know the past, understand the presence and propose directions for the future.

Likewise, (Cobo, M.J., López-Herrera, A.G., Herrera-Viedma, E., Herrera, 2011) notes that bibliometrics usually includes two procedures: Performance analysis and science mapping analysis. The first analysis focuses on performing evaluation of scientific activities and the second one focuses on showing the structural and dynamic patterns of scientific research. In summary, bibliometric enables to establish a complete profile of a specific field of study, institution or journal.

Bibliometric analysis offers additional data statistics including author, affiliation, and keywords. In this context, the items of analysis used in the study are detailed like co-authorship, journal analysis, citing, keyword analysis, geo/location collaboration, co-occurrence, and betweenness centrality score.

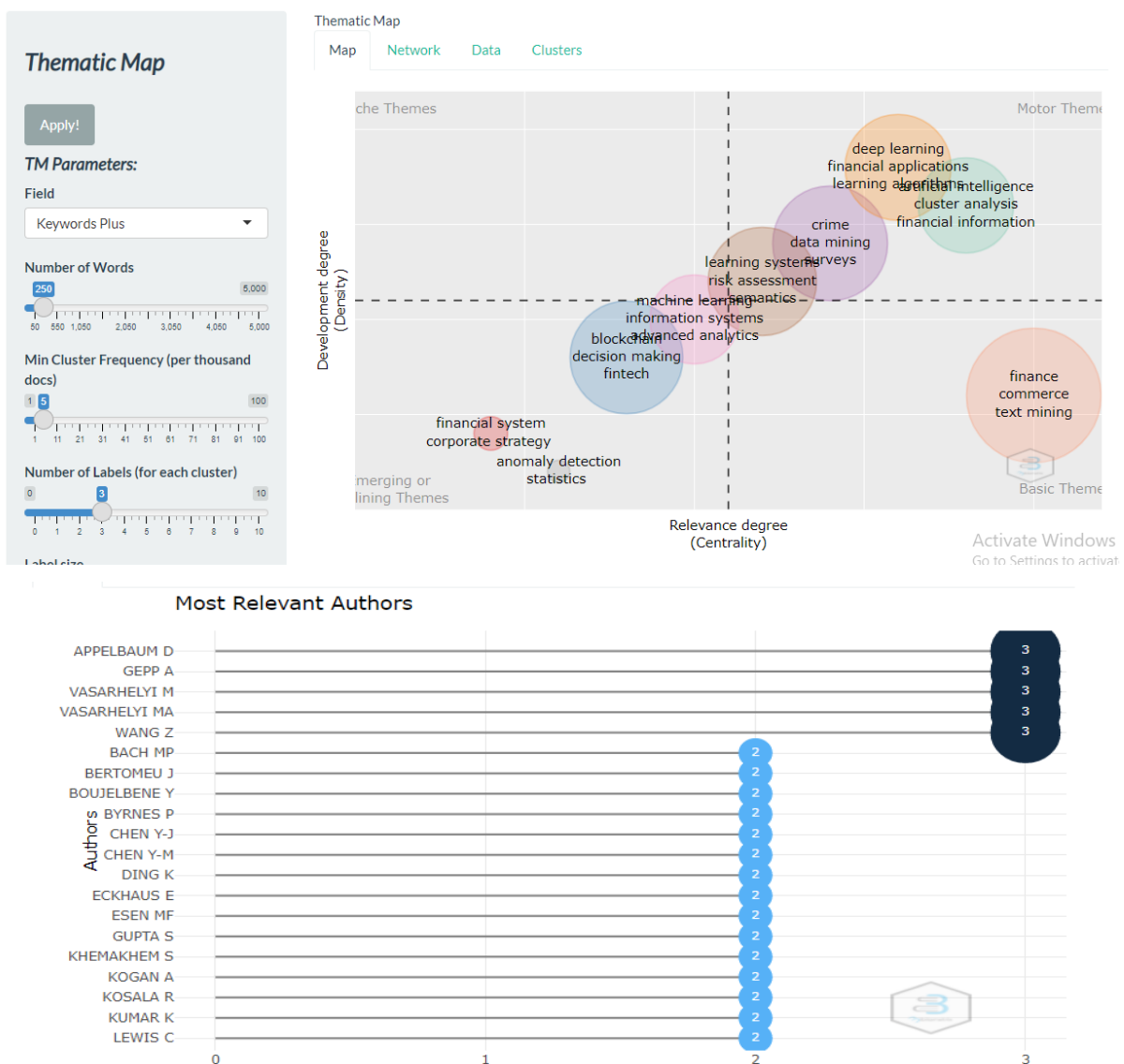
We obtained full bibliographical data from Scopus, collecting 320 articles only, Scopus is well known in social science as a common source of scholarly literature, researchers worldwide use this database for numerical analysis (Durán-Sánchez et al., 2019). To perform our analysis, we used RStudio, VOSviewer and Excel all which are famous and widely used tools to conduct bibliometric (Cortés-Sánchez, 2020) and scientometrics studies (Cortés-Sánchez, 2019).

By filtering the data with help of these tools we were able to generate the most relevant countries, institutions, journals and authors, using same technique we also generated most cited countries, institution, sources, authors, documents, and references. Scopus provided us with extra insights of Ranking and metrics. By using Biblioshiny, we were able to conduct a co-citation network, bibliographical coupling and co-occurrence analysis to generate main themes and clusters of the journal publications. Biblioshiny is a famous tool for mapping and networking analysis also it is quite helpful in conducting content analysis.

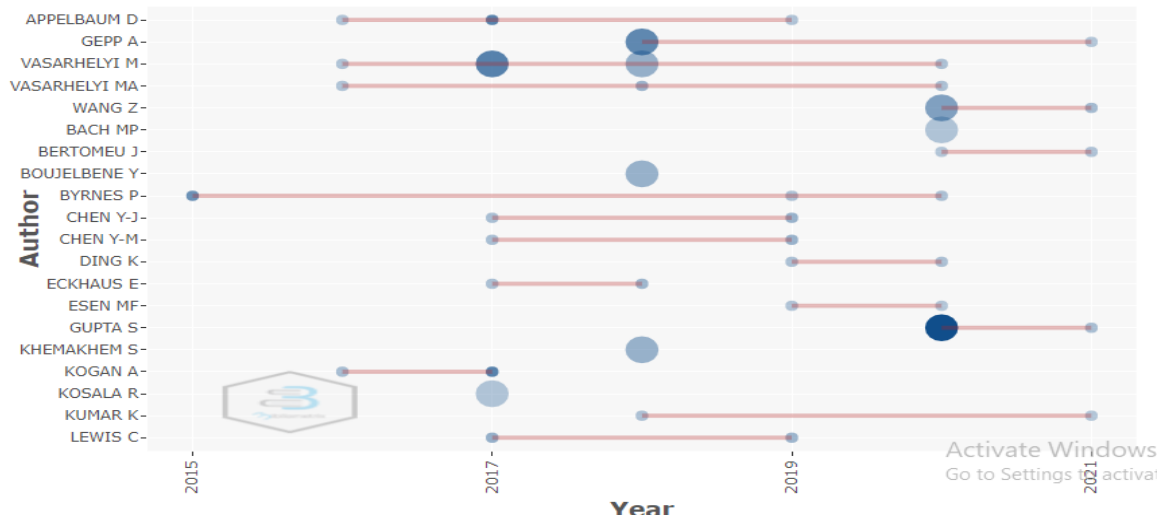
Discussions and conclusions

Findings and discussions

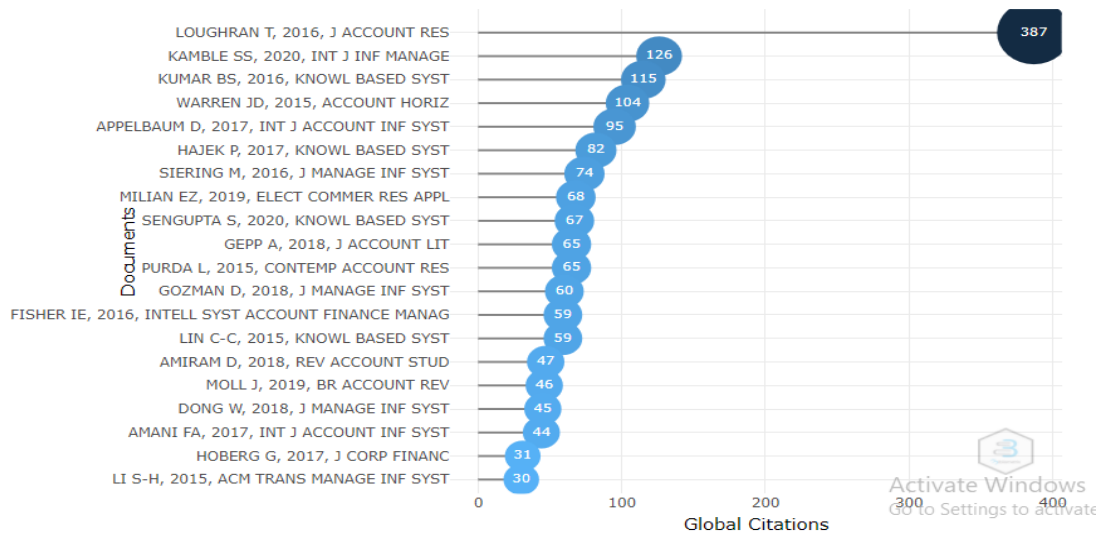
The knowledge map of AFDUM was visualized by information visualization software R-BIBLIOSHINY based on the literature retrieved from SCOPUS for 2015 to 2022 years. Through the author analysis, journal analysis, country analysis, institution analysis, co-cited references network analysis, co-occurrence keywords network analysis and burst keywords analysis, the research achievements, and potential impacts of AFDUM have been identified in a multipurpose and comprehensive way. Some interesting results concerning the AFDUM-related publications can be summarized as follows:



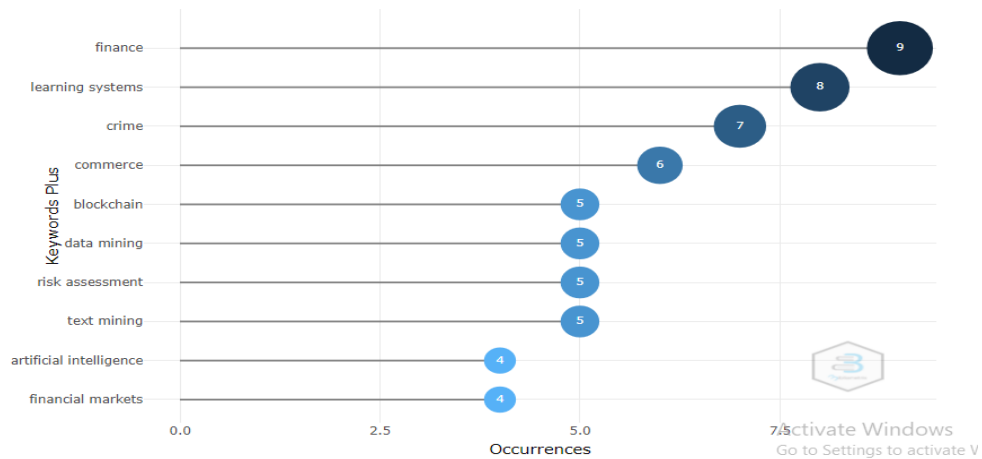
Top-Authors' Production over the Time



Most Global Cited Documents

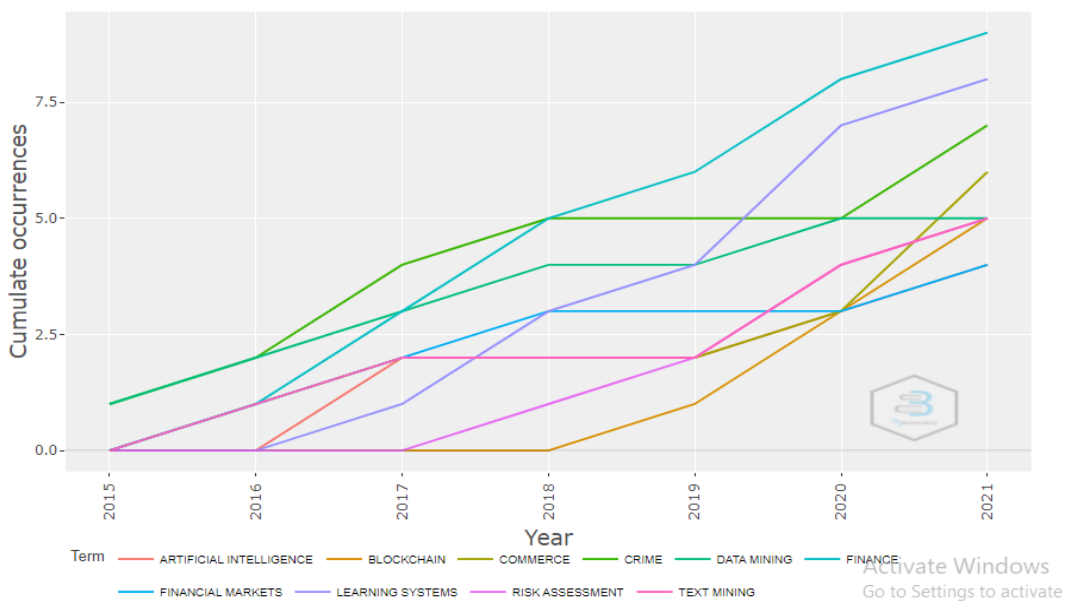


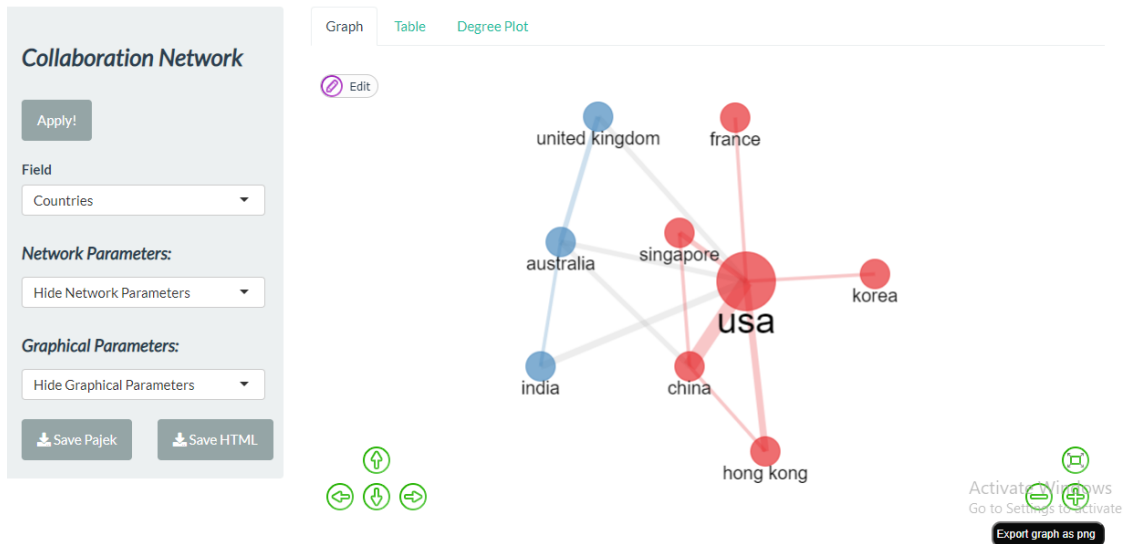
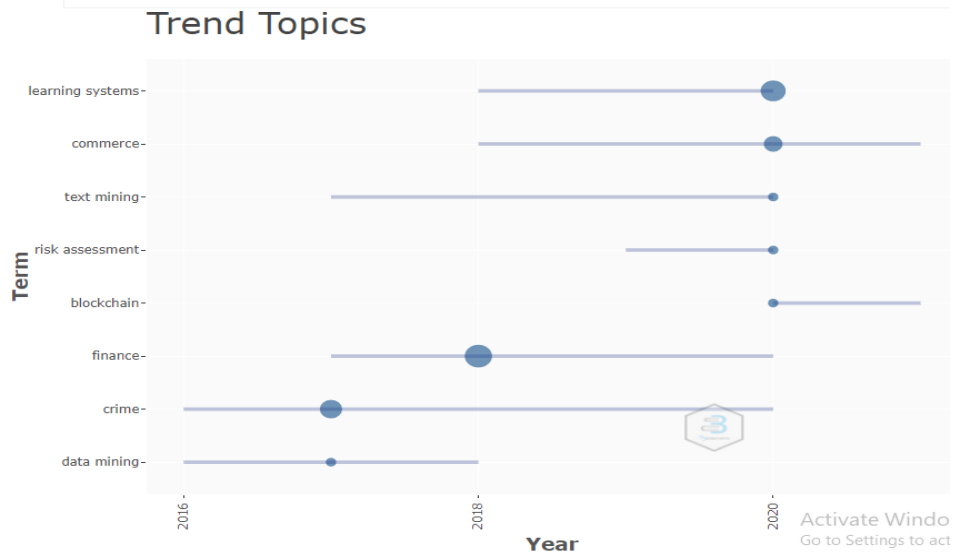
Most Relevant Words



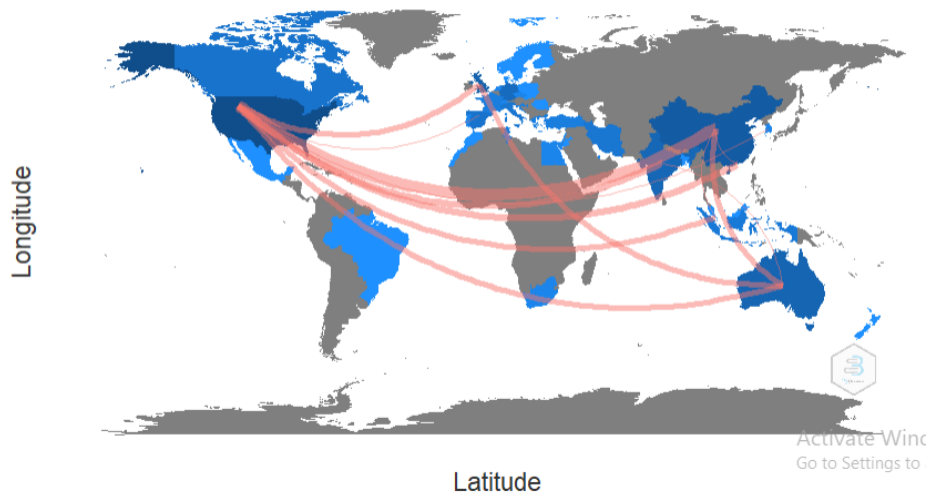


Word Growth





Country Collaboration Map



Reference

- Aisha Abdallah, Mohd Aizaini Maarof and Anazida Zainal, Fraud Detection System: A survey, *Journal of Network and Computer Applications*, <http://dx.doi.org/10.1016/j.jnca.2016.04.007>
- A. Sorin. 2012, "Survey of Clustering based Financial Fraud Detection Research". In: *Informatica Economica* 16.1, pp. 110–123.
- C. Classifier, J. Kim, K. Choi, G. Kim, and Y. Suh, "Expert Systems with Applications Classification cost : An empirical comparison among traditional classifier," *Expert Syst. Appl.*, vol. 39, no. 4, pp. 4013–4019, 2012.
- Clifton Phua, Vincent Lee, Kate Smith, and Ross Gayler. 2005. *A Comprehensive Survey of Data Mining-based Fraud Detection Research*. (2005).
- Dechow, P. M., Ge, W., Larson, C. R. and R. G. Sloan. Predicting Material Accounting Misstatements. *Contemporary Accounting Research* 28 (1): 17-82. 2011.
- Dechow, P. M., Ge, W., and C. Schrand. Understanding Earnings Quality: A Review of the Proxies, their Determinants and their Consequences. *Journal of Accounting and Economics* 50 (2)(3): 344-401. 2010.
- Dechow, P. M., R. G. Sloan, and A. P. Sweeney. Causes and Consequences of Earnings Manipulation: An Analysis of Firms Subject to Enforcement Actions by the SEC. *Contemporary Accounting Research* 13 (1): 1-36. 1996.
- E. E. Ngai et al. 2011, "The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature". In: *Decision Support Systems* 50.3, pp. 559–569.
- E Kirkos, C Spathis, and Y Manolopoulos. 2007. "Data Mining techniques for the detection of fraudulent financial statements". In: *Expert Systems with Applications* 32.4, pp. 995–1003.
- F. Louzada and A. Ara, "Expert Systems with Applications Bagging k-dependence probabilistic networks : An alternative powerful fraud detection tool," *Expert Syst. Appl.*, vol. 39, no. 14, pp. 11583–11592, 2012.
- Han Tao, Liu Zhixin, and Song Xiaodong. 2012. Insurance fraud identification research based on fuzzy support vector machine with dual membership. *2012 Int. Conf. Inf. Manag. Innov. Manag. Ind. Eng.* (October 2012), 457–460. DOI:<http://dx.doi.org/10.1109/ICIIE.2012.6340016>
- J. P. Linda Delamaire, Hussein Abdou , "Credit card fraud and detection techniques : a review," *Banks Bank Syst.*, vol. 4, no. 2, 2009.

- J. West and M. Bhattacharya. 2015, "Intelligent financial fraud detection: a comprehensive review". In: *Computers & Security* 57, pp. 47–66.
- K. Ramakalyani and D. Umadevi, "Fraud Detection of Credit Card Payment System by Genetic Algorithm," *International Journal of Scientific & Engineering Research*, vol. 3, no. 7, pp. 1–6, 2012.
- Linda Delamaire, Hussein Abdou, and John Pointon. 2009. Credit card fraud and detection techniques : a review. 4, 2 (2009).
- Li. Bermudez, J.M. Perez, M. Ayuso, E. Gomez, and F.J. Vazquez. 2008. A Bayesian dichotomous model with asymmetric link for fraud in insurance. *Insur. Math. Econ.* 42, 2 (April 2008), 779–786. DOI:<http://dx.doi.org/10.1016/j.insmatheco.2007.08.002>
- Miguel Pironet San-bento Almeida. 2009. Classification for Fraud Detection with Social Network Analysis. Dissertation for the obtaining of a Masters Degree in Engenharia Informatica e de Computadores Juri. (2009).
- Mirjana Pejic-Bach. 2010. Invited Paper: Profiling Intelligent Systems Applications in Fraud Detection and Prevention: Survey of Research Articles. In 2010 International Conference on Intelligent Systems, Modelling and Simulation. IEEE, 80–85. DOI:<http://dx.doi.org/10.1109/ISMS.2010.26>
- Mohammad Behdad, Luigi Barone, Mohammed Bennamoun, and Tim French. 2012. Nature-Inspired Techniques in the Context of Fraud Detection. *IEEE Trans. Syst.Man, Cybern. Part C (Applications Rev.* 42, 6 (November 2012), 1273–1290. DOI:<http://dx.doi.org/10.1109/TSMCC.2012.2215851>
- Panos Alexopoulos, Kostas Kafentzis, Xanthi Benetou, and Tassos Tagaris. 2007. TOWARDS A GENERIC FRAUD ONTOLOGY IN E- GOVERNMENT DETECTION .(2007).
- Peter Travaille, Dallas Thornton, and Roland M. Muller. 2011. Electronic Fraud Detection in the U . S . Medicaid Healthcare Program : Lessons Learned from other Industries. (2011), 1–10.
- Perols, J. "Financial Statement Fraud Detection: An Analysis of Statistical and Machine Learning Algorithms," *Auditing: A Journal of Practice & Theory* 30(2): 19-50. 2011.
- Perols, J., Bowen, B., and C. Zimmerman. "Finding Needles in a Haystack: Using Data Analytics to Improve Fraud Forecast," *Accounting Review* 92(2): 221-245. 2017.

- S. Benson Edwin Raj and A. Annie Portia. 2011, "Analysis on credit card fraud detection methods. In: nternational Conference on Computer, Communication and Electrical Technology (ICCCET). IEEE, pp. 152–156.
- S. Benson Edwin Raj, A. Annie Portia, and Assistant Sg. 2011. Analysis on Credit Card Fraud Detection Methods. (2011), 152–156.
- Song Survey and Research on Early Detection of Improper Accounting in Response to Recent Changes in the Economic Environment. FSA Institute Discussion Paper Series, DP 2017-6. 2018.
- Song, M., N. Oshiro, and A. Shuto. Predicting Accounting Fraud: Evidence from Japan. *The Japanese Accounting Review* 6: pp. 17-63. 2016.
- Tareq Allan, Justin Zhan, and South Dako. Towards Fraud Detection Methodologies e. (2010).
- T. Tian, J. Zhu, F. Xia, X. Zhuang, and T. Zhang, "Crowd Fraud Detection in Internet Advertising," International World Wide Web Conference Committee, 2015.
- West, J. and M. Bhattacharya. "Intelligent Financial Fraud Detection: A Comprehensive Review," *Computer & Security* 57: 47-66. 2016.
- Yacine Rebahi, Mohamed Nassar, Thomas Magedanz, and Olivier Festor. 2011. A survey on fraud and service misuse in voice over IP (VoIP) networks. *Inf. Secur. Tech.Rep.* 16, 1 (February 2011), 12–19. DOI:<http://dx.doi.org/10.1016/j.istr.2010.10.012>.