The Challenge of Quality Evaluation in Fraud Detection

John Puentes, Pedro Merino Laso, David Brosset

The Challenge of Quality Evaluation in Fraud Detection

JOHN PUENTES, IMT Atlantique
PEDRO MERINO LASO, Chair of Naval Cybersecurity
DAVID BROSSET, Naval Academy Research Institute

CCS Concepts: • **Security and privacy → Intrusion/anomaly detection and malware mitigation**; • **Information systems → Decision support systems**; *Data analytics*;

Additional Key Words and Phrases: Quality meta-analysis, context, cumulative indicators, fraud life cycle

1 INTRODUCTION

A system is considered to be safety-critical when its failure may lead to unacceptable consequences [17]. One failure of particular interest in safety-critical systems is fraud, understood as abusing a position of trust to get illegal advantage and/or cause losses by false suggestions or suppression of the truth. Although some safety-critical systems are protected by design against known threats, innovative exploitation of latent vulnerabilities remains a possibility. Fraud has multiple consequences on provision of services, management of organizations, and operational infrastructure, causing damage to human lives, production processes, and the natural environment.

Paradoxically, in fraud situations, compliance to fitness for use seems to be appropriate, while conformity to procedures is cleverly bypassed. Also, even if automatic procedures continuously check for potential fraud, legitimate users may commit fraud inside organizations or maliciously manipulated applications can have significant unknown repercussions on a system. Besides, voluminous heterogeneous data and information are exchanged in and between systems. For these reasons, quality evaluation in fraud situations is very complex. The automobile industry [14], banks [7], health institutions [21], and government [2] are some examples of organizations affected by frauds. Taking into account that the quality assessment of procedures and processes is still an open problem [1] [5], this proposal focuses on data and information quality within those procedures. This article discusses why quality assessment in fraud contexts is a challenging problem and argues for a longitudinal quality meta-analysis, relying on contextual cumulative indicators.

This work is supported by the Chair of Naval Cybersecurity, funded by École Navale, IMT Atlantique, Thales and Naval Group.
Authors' addresses: J. Puentes, IMT Atlantique, Lab-STICC UMR CNRS 6285 Équipe DECIDE - CS 83818 F29238, Brest Cedex 3, France; email: john.puentes@imt-atlantique.fr; P. M. Laso, École Navale - CC 600 F29240 Brest Cedex 9, France; email: pedro.merino@ecole-navale.fr; D. Brosset, École Navale - CC 600 F29240 Brest Cedex 9, France; email: david.brosset@ecole-navale.fr.

2 CHALLENGE

A unique unexplored quality research challenge stems from the dynamics of fraud. We hypothesize that fraudulent transactions can be detected examining their quality differences, inconsistent timeliness, inherent coherence, partial regularity, and questionable believability. All these characteristics are strongly related to the context on which operations are carried out. We consider that the combination of these multiple weak indicators though time might make fraud evidence emerge. As a result, frauds could be detected by identifying known patterns of variability among these indicators.

The general research challenge is therefore enounced as: *How can quality evaluation and analysis reveal pertinent contextual cumulative indicators of fraud life cycle in an information system?*

Numerous research implications arise from this comprehensive challenge. Our proposal is focused on contextual quality meta-analysis through time. Context ubiquity [6]—prior, historical, relative, behavioral, operational, applicative—is fundamental to determine the validity of rich evolving aspects like the limits of trust and credibility, as well as the pertinence of concerned quality dimensions. Moreover, longitudinal evaluation deployment entails tracking activities through time to identify anomalies in operational patterns, making use of variable observation time windows [23]. Meta-analysis consists of detecting relevant activity indicators in traced fingerprints of individuals and groups, according to the acceptance of quality variability depending on context [16].

3 RESEARCH DIRECTIONS

Among multiple possible research directions that derive from investigating quality evaluation in fraud situations, the definition of suitable quality dimensions, acceptable quality variability, and understanding of the fraud cycle seem to be fundamental to address this challenge.

3.1 Quality Dimensions

The evaluation of quality dimensions is considered essential in data fusion [11] and decision support [9] [5]. Yet, current definitions of quality dimensions do not meet fraud detection needs. Two objective dimensions, timeliness and coherence, may provide some of the answers.

Timeliness: Refers to the chronological patterns of transactions commonly observed in data and information exchanges between subsystems [18]. The contextual analysis of these quality patterns might prove helpful to address the differences between incompatible timeliness generated by doubtful transaction sequences and system malfunctions [10].

Coherence: Examines the agreement of relationships between information streams [15]. Research about the quality coherence of fraudulent operations components—e.g., type of anomalies and errors, unusual high or low scores, recursive modifications of steps, data fabrication, sudden decision changes, involved system nodes, differences with respect to working standards, and degree of similarity—should be conducted to differentiate these operations from normal ones.

Conversely, subjective quality measurements carried out by humans are often useful because of the evaluator's experience, and should be therefore adapted to fraud detection. Man-machine collaboration can take, in this case, the form of active learning to provide complementary significant operational observations [20]. Dimensions that contribute to represent evaluations done by humans are believability, consistency, and interpretability.

Believability: Serves to complete the understanding of gathered evidence to decide if further inquiries are appropriate. It is required to assess, for instance, the complexity and pertinence of transactions, omissions, misrepresentation, over and under statements, fictitious claims, and compliance with regulations [24].

Consistency: Examines the global regularity of activities, their types, media formats, sequences of actions, interactions, contacts, preferences, and volume of operations, among others. Group and individual descriptions can be built integrating these elements to define activity summaries associated to roles and responsibilities [3].

Interpretability: Represents the explanation of system traces left by operators' activities. It permits us to explain the pertinence of suspect imbalances, which appear when one or various transaction elements are disregarded, or when anomalous traces are found [12].

3.2 Quality Variability

Most of data quality analysis has been circumscribed to fitness for use. However, in fraud scenarios, data are likely to be of sufficient quality to meet this requirement and pass undetected through controls. Hence, one possible way to detect fraud is to determine acceptable variable quality states [4], in agreement with actual contextual representative quality of data and information. To this end, context provided by metadata (e.g., operator, location, time stamps, transaction type, file or stream size, transmission changeability, involved system modules, etc.) and indicators like operator status (e.g., hire, resign, laid off, promotion, assignments, vacations, etc.) can serve to outline the appropriate quality variability [8]. Not being totally available to the fraudster, context could permit us to identify potentially conflicting elements of quality evaluation.

3.3 Fraud Cycle

Single anomalies do not expose unambiguously a fraud situation. Globally, it takes more than one year to detect a fraud, after the first consequences are noticed and the respective modus operandi deciphered [13]. Fraud cycles are composed of multiple indicators, which could be estimated according to variable quality and described dimensions to elicit irregularities. Hence, continuous metadata collection can be synthesized as fingerprints of relevant activities, to be analyzed by means of quality measurements during time periods of variable length. Such analysis considers that each operator and group have a metadata profile related to specific contexts, for which variations in the quality pattern can be identified in the form of anomalies. Besides, depending on the severity of anomalies, quality variations propagate through a system with different impacts on subsystems [22]. Collected quality indicators also represent cumulative behavior patterns of multiple procedures and individuals, at different spatial and temporal resolutions. Repetitive or articulated quality anomalies through time could thus represent questionable differences to be examined [19], implying that, if identified, the analysis should be further adjusted to detected fraud characteristics.

4 CONCLUSION

To recognize risk patterns, fraud detection in information systems should examine numerous quality-related potential warning signs. The global approach requires us to consider contextual quality variability and propagation, according to objective and subjective dimensions. Open research issues concern the definition and articulation of multi-dimensional context-based quality measures, relying on temporal profiling meta-analysis.

REFERENCES

[1] Isel Moreno-Montes de Oca, Monique Snoeck, Hajo A. Reijers, and Abel Rodríguez-Morffi. 2015. A systematic literature review of studies on business process modeling quality. *Information and Software Technology* 58 (2015), 187–205.

[2] Ratbek Dzhumashev. 2014. The two-way relationship between government spending and corruption and its effects on economic growth. *Contemporary Economic Policy* 32, 2 (2014), 403–419.

[3] Álvaro García-Recuero, Sérgio Esteves, and Luís Veiga. 2014. Towards quality-of-service driven consistency for big data management. *International Journal of Big Data Intelligence* 1, 1–2 (2014), 74–88.

[4] Stephen L. George and Marc Buyse. 2015. Data fraud in clinical trials. *Clinical Investigation* 5, 2 (2015), 161.

[5] Pola Hahlweg, Sarah Didi, Levente Kriston, Martin Härter, Yvonne Nestoriuc, and Isabelle Scholl. 2017. Process quality of decision-making in multidisciplinary cancer team meetings: A structured observational study. *BMC Cancer* 17, 1 (2017), 772.

[6] Joseph M. Hellerstein, Vikram Sreekanti, Joseph E. Gonzalez, James Dalton, Akon Dey, Sreyashi Nag, Krishna Ramachandran, Sudhanshu Arora, Arka Bhattacharyya, Shirshanka Das, and others. 2017. Ground: A data context service. In *8th Conference on Innovative Data Systems Research*.

[7] Matthew Hollow. 2014. Money, morals and motives: An exploratory study into why bank managers and employees commit fraud at work. *Journal of Financial Crime* 21, 2 (2014), 174–190.

[8] Steven A. Israel and Erik Blasch. 2016. Context assumptions for threat assessment systems. In *Context-Enhanced Information Fusion*. Springer, 99–124.

[9] Marijn Janssen, Haiko van der Voort, and Agung Wahyudi. 2017. Factors influencing big data decision-making quality. *Journal of Business Research* 70 (2017), 338–345.

[10] Andreas Lanz, Barbara Weber, and Manfred Reichert. 2014. Time patterns for process-aware information systems. *Requirements Engineering* 19, 2 (2014), 113–141.

[11] Didier G. Leibovici, Julian F. Rosser, Crona Hodges, Barry Evans, Michael J. Jackson, and Chris I. Higgins. 2017. On data quality assurance and conflation entanglement in crowdsourcing for environmental studies. *ISPRS International Journal of Geo-Information* 6, 3 (2017), 78.

[12] Saurabh Nagrecha, Reid A. Johnson, and Nitesh V. Chawla. 2018. FraudBuster: Reducing fraud in an auto insurance market. *Big Data* 6, 1 (2018), 3–12.

[13] Association of Certified Fraud Examiners. 2018. Report to the Nations on Occupational Fraud and Abuse. Global Fraud Study. Retrieved May 12, 2018 from https://s3-us-west-2.amazonaws.com/acfepublic/2018-report-to-the-nations.pdf.

[14] Rik Oldenkamp, Rosalie van Zelm, and Mark A. J. Huijbregts. 2016. Valuing the human health damage caused by the fraud of volkswagen. *Environmental Pollution* 212 (2016), 121–127.

[15] Duc-Son Pham, Svetha Venkatesh, Mihai Lazarescu, and Saha Budhaditya. 2014. Anomaly detection in large-scale data stream networks. *Data Mining and Knowledge Discovery* 28, 1 (2014), 145–189.

[16] Darren Quick and Kim-Kwang Raymond Choo. 2018. Digital forensic intelligence: Data subsets and open source intelligence (DFINT+ OSINT): A timely and cohesive mix. *Future Generation Computer Systems* 78 (2018), 558–567.

[17] Marvin Rausand. 2014. *Reliability of Safety-Critical Systems: Theory and Applications*. John Wiley & Sons.

[18] Rafael Ramos Regis Barbosa, Ramin Sadre, and Aiko Pras. 2016. Exploiting traffic periodicity in industrial control networks. *International Journal of Critical Infrastructure Protection* 13 (2016), 52–62.

[19] Ian Ross. 2015. *Exposing Fraud: Skills, Process and Practicalities*. John Wiley & Sons.

[20] Manali Sharma, Kamalika Das, Mustafa Bilgic, Bryan Matthews, David Nielsen, and Nikunj Oza. 2016. Active learning with rationales for identifying operationally significant anomalies in aviation. In *Joint European Conference on Machine Learning and Knowledge Discovery in Databases*. Springer, 209–225.

[21] Dallas Thornton, Michel Brinkhuis, Chintan Amrit, and Robin Aly. 2015. Categorizing and describing the types of fraud in healthcare. *Procedia Computer Science* 64 (2015), 713–720.

[22] Ion-George Todoran, Laurent Lecornu, Ali Khenchaf, and Jean-Marc Le Caillec. 2015. A methodology to evaluate important dimensions of information quality in systems. *Journal of Data and Information Quality* 6, 2–3, Article 11 (2015), 23 pages.

[23] Véronique Van Vlasselaer, Cristián Bravo, Olivier Caelen, Tina Eliassi-Rad, Leman Akoglu, Monique Snoeck, and Bart Baesens. 2015. APATE: A novel approach for automated credit card transaction fraud detection using network-based extensions. *Decision Support Systems* 75 (2015), 38–48.

[24] Amrapali Zaveri, Anisa Rula, Andrea Maurino, Ricardo Pietrobon, Jens Lehmann, and Sören Auer. 2016. Quality assessment for linked data: A survey. *Semantic Web* 7, 1 (2016), 63–93.