Scenario-based Requirements Elicitation for User-Centric Explainable AI

A Case in Fraud Detection

Douglas Cirqueira[1[0000-0002-1283-0453]], Dietmar Nedbal[2[0000-0002-7596-0917]] , Markus Helfert[3[0000-0001-6546-6408]], Marija Bezbradica[1[0000-0001-9366-5113]]

[1] Dublin City University, Dublin, Ireland
douglas.darochacirqueira2@mail.dcu.ie
[2] University of Applied Sciences Upper Austria, Steyr, Austria
[3] Maynooth University, Maynooth, Ireland

Abstract. Explainable Artificial Intelligence (XAI) develops technical explanation methods and enable interpretability for human stakeholders on why Artificial Intelligence (AI) and machine learning (ML) models provide certain predictions. However, the trust of those stakeholders into AI models and explanations is still an issue, especially domain experts, who are knowledgeable about their domain but not AI inner workings. Social and user-centric XAI research states it is essential to understand the stakeholder's requirements to provide explanations tailored to their needs, and enhance their trust in working with AI models. Scenario-based design and requirements elicitation can help bridge the gap between social and operational aspects of a stakeholder early before the adoption of information systems and identify its real problem and practices generating user requirements. Nevertheless, it is still rarely explored the adoption of scenarios in XAI, especially in the domain of fraud detection to supporting experts who are about to work with AI models. We demonstrate the usage of scenario-based requirements elicitation for XAI in a fraud detection context, and develop scenarios derived with experts in banking fraud. We discuss how those scenarios can be adopted to identify user or expert requirements for appropriate explanations in his daily operations and to make decisions on reviewing fraudulent cases in banking. The generalizability of the scenarios for further adoption is validated through a systematic literature review in domains of XAI and visual analytics for fraud detection.

Keywords: Explainable Artificial Intelligence, Requirements Elicitation, Domain Expert, Fraud Detection.

1 Introduction

Digital platforms in retail and banking have enabled customers to experience convenience through personalization and tailored technologies for shopping and performing transactions [1-4]. However, the convenience is also accompanied by the danger of frauds [5, 6]. Transaction frauds are growing every year, and organizations such as retailers and banks realized the potential of AI models for automating the fraud detection task [7].

However, organizations leveraging AI technologies are considering the importance of automating their processes and understanding the predictions made by those models [8], as users are increasingly demanding transparency from their daily software assistants [9]. This understanding is enabled through explanations provided by Explainable AI (XAI) methods [10]. The field of XAI aims to implement and develop explanation methods, enabling transparency and traceability for statistical black-box ML models, such as deep learning approaches, which are increasingly used by industry due to their potential to reveal useful insights into the Big Data present in companies businesses [11].

While in some domains automation is relevant, it is essential for others to understand AI predictions and decisions for human stakeholders [10], as explanations can impact the work of stakeholders who adopt such tools for decision-making [12]. For instance, in healthcare, doctors can adopt explanation methods to understand the diagnosis provided by AI models predictions [10]. In finance, researchers seek to leverage explanations for better decision-making of fraud experts in reviewing fraudulent applications for credit and loans [13]. Therefore, a diversity of explanation methods for AI predictions has been developed in the XAI literature [6].

In addition, while it is essential to develop those methods, researchers from the social perspective highlight XAI research tended to adopt particular notions of what is a good explanation, not considering, for instance, the usability and causability requirements of stakeholders for understanding explanations [14, 15, 16, 17]. Such requirements are essential as they enable an understanding of the quality of explanations associated with a human agent's properties and his cognitive and intelligence capabilities for working with AI models [18].

This lack of user-centric perspective in XAI is a context also observed in the domain of fraud detection. Nevertheless, fraud experts need to act on predictions provided by AI models which they do not understand or trust. However, XAI literature is rarely addressed from a user-centric perspective in fraud detection. User-centric XAI researchers highlight the importance of considering users' needs for a trustworthy relationship with AI models for decision-making [19, 20].

Aiming a user-centric view into decision-making for fraud detection, the domain of visual analytics has also been providing contributions through visualization tools and capabilities for fraud detection [21]. Indeed, some researchers have acknowledged the importance of the human-computer interaction or human-in-the-loop perspectives contributing to research in XAI, and the need to investigate new human-AI interfaces for Explainable AI [22-26]**.** Therefore, a user-centric perspective is essential for reviewing fraud cases, whether in XAI or visual analytics research, as every wrong decision made causes financial harm for customers and organizations.

In the meantime, Information Systems (IS) research has been studying, for years, the cognitive tasks of stakeholders, and how to designing information systems that can support in their decision-making processes [27, 28]. For support in decision-making, IS research states it is fundamental to identify user requirements in a problem space for developing artifacts as systems aligned with the needs of practitioners, causing a successful impact within an organization [29, 30]. This research follows an IS theoretical perspective in XAI for fraud detection, and aims to investigate the cognitive tasks of fraud experts for decision-making, and how those tasks can be adopted to identify their

requirements for explanations of AI predictions aiding in their reviewing process of fraud cases.

To uncover the cognitive tasks of fraud experts, the main goal of this study is to demonstrate the usage of a scenario-based requirements elicitation method, and to develop scenarios illustrating the process for decision-making in fraud detection. Scenarios have the potential to bridge the gap between the social and operational focus with the organizational focus of information systems development [31]. Our stakeholder is regarded as a fraud expert, which is not knowledgeable about AI inner workings, and would benefit from explanations for reviewing fraudulent transaction cases daily in a bank. That is a context seldom addressed by the employment of scenarios within XAI.

We outline the following elements as contributions of this study:

- The demonstration of the suitability of scenario-based requirements elicitation method in the context of XAI for fraud detection.
- The development and validation of fraud scenarios for XAI literature, which can be adopted for identifying fraud experts' requirements for explanations, and designing explanation methods suitable for this domain.

The rest of this paper is organized as follows: Section 2 describes related work; Section 3 discusses the scenario-based method adopted in this study; Section 4 presents the results of the method as fraud scenarios; Section 5 describes the validation of the developed fraud scenarios given existing literature; Section 6 discusses how the developed scenarios can be adopted for requirements elicitation in XAI for fraud detection; Section 7 concludes the study with final remarks and future work.

2 Related Work

The concept of explaining has been studied for a long time by research disciplines other than information systems or computer science, such as social sciences [14, 32]. Following those lenses, Miller [33] defines explanations in XAI as an answer to a question an explainee would have to an explainer, which can be a why-question such as "Why is that transaction marked as a fraud?". Researchers in the discipline of computer science and machine learning have been developing XAI methods as explainers, which provide explanations or human-AI interfaces for different stakeholders, including domain experts, who adopt them for decision-making processes [23]. Research in XAI usually classifies explanations by their scope or dependency [33-37]. The scope can be global, when explanations provide an understanding of the whole logic of an AI model, or local when explanations provide an understanding of individual predictions. Dependency can be model-specific, which enables explanations of a particular AI model, or model-agnostic, which enables post-hoc explanations independently of the underlying AI model. Each of those methods has particular features, which enable understanding of particular aspects of AI predictions.

Within XAI literature, researchers have tried to assess the impact of explanations on the decision-making of fraud experts working with AI models in domains such as intrusion detection, fraudulent warranty claims, and banking transaction frauds. In [38], the authors provide a service architecture for security experts with explanations, aiming

to introduce more context for the outlier score given to anomalous records of network flows. The work of [39] provides domain experts with shapley additive explanations (SHAP) [40] for why particular warranty claims are marked as anomalies by an ML model. In [41], the authors also work with SHAP explanations for fraud alerts, and observe through experiments that SHAP explanations impact decision-making for fraud cases. The same authors in [42] go further and provide a case-based SHAP explanation based on neighborhood, and enable experts to visualize similar instances to an observation for which a fraud alert was issued. Their goal is to increase the trust of domain experts in AI models analyzing transaction frauds in banking.

Some researchers consider the aid of visual analytics for understanding AI models, also in the fraud domain [43, 44]. In this context, [21] provides a visual analytics tool to support domain experts in their fraud detection workflow. The contribution was developed in close collaboration with fraud teams, through a user-centric iterative design process [45]. The authors make an essential contribution towards extending a fraud detection workflow with human analysis through visual analytics. However, they focus on interactive visualizations, but not on XAI methods. In [46], the authors focus on developing a visual analytics tool for supporting cyber analysts in making decisions when dealing with intrusion detection alerts. However, the authors also do not consider explanations in XAI. Their scenario is focused on network intrusion, which has different constraints than transaction fraud.

Regarding requirements elicitation in XAI, the literature is still at an early stage. Nevertheless, it was identified proposals for this elicitation in the literature. In [47], the authors provide a systematic methodology composed of five steps. Their goal is to understand requirements for XAI from multiple perspectives, assess explanation capabilities, and steer future research to industrial cases. In [48], also inspired by the requirements engineering literature, the authors propose a workflow to elucidate requirements for explanations, considering those requirements are non-functional. The methodology is assessed in a hypothetical hiring scenario. In [49], a Question-driven approach to assess explanation needs is proposed. The authors adopt a taxonomy of XAI methods mapped to user question types. They assume an explanation can be seen as an answer to a question, and represent user needs for XAI methods in terms of the questions a user might ask. In [50], the authors propose a stage-based participatory process for designing transparent interfaces incorporating perspectives of users, designers, and providers. They map requirements considering real-world needs influencing how to explain, such as company-specific style guidelines.

The work of [51] is one of the first proposals discussing the usage of scenarios in the context of XAI. Their goal is to anticipate scenarios of XAI usage to system development. They present a case study of aging-in-place monitoring, and argue that such a method can become a design resource to tackle the gaps between XAI, IS and Human-Computer Interaction communities for understanding how end users might interact with explanations capabilities and its workplace implications.

In summary, it is observed in [38, 39, 41, 42] proposals aiming for the integration of explanations in a fraud detection context. Within visual analytics literature, it is also observed studies aiming to support the decision-making of fraud experts through visualizations [21, 45, 46]. However, a social and user-centered perspective has been lacking in those works, by first understanding the needs of fraud experts for explanations

which can enhance their trust in AI models and decision-making processes. Moreover, the adoption of scenario-based elicitation in XAI is introduced by Wolf [51]. Nevertheless, the author has not presented the process in the context of fraud detection, which is complex by itself, as fraud experts need to deal with critical decisions daily, relating to financial losses of customers [52]. Therefore, it is essential to understand the needs of those experts for explanations, given their context and cognitive tasks for reviewing fraud cases.

For the reasons illustrated, we chose and demonstrate the scenario-based method to uncover the cognitive tasks of fraud experts, creating scenarios that can be further employed to identify their requirements regarding socio-technical and operational constraints in their real context, to reflect appropriate explanations for their operations and trust in AI predictions.

3 Scenario-Based Requirements Elicitation

3.1 The Method

Scenario-based elicitation is considered a problem-centered method for identifying stakeholder needs early in the development of information systems [53]. The idea is not to discuss solutions beforehand with stakeholders, but to understand their socio and operational context. Therefore, stakeholders are not asked what they want a system to provide them with, but what they want to achieve [54].

Scenarios can bridge the cognitive or psychological focus of traditional HCI methods, with the organizational focus of information systems development, creating a hybrid lens into ways in which these concerns are co-constituted in practice [30, 55]. We add to this argument, with the fact that scenarios enable the possibility to uncover the needs of stakeholders from a qualitative perspective, which is valuable for research from interpretivist and subjective philosophical lenses targeting the cognitive tasks of human decision-makers.

Therefore, scenarios can be used to analyze software requirements, such as to guide the design of user interface layouts and controls [54]. They are narratives on the sequence of events and steps performed by a stakeholder in their daily operations [56]. Scenarios consist of particular elements, including scenes with one or more actors in their settings, their goals, knowledge, and tools, providing them with capabilities to manipulate and working on their particular tasks [54].

The method is also referred to as Scenario-based task analysis, especially within the HCI community [57, 58]. Indeed, it enables an overview of human-computer interactions and tasks through stories of past or future use of a system by a human agent. This perspective intersects well with the concept adopted in this research for scenarios, given we aim to uncover the cognitive tasks and requirements of fraud experts during the decision-making of fraud cases.

Finally, given this study adopts an IS theoretical lens for XAI research, it is crucial to consider the role of the domain experts in consuming explanations, which should be tailored to follow their user requirements. We aim to develop scenarios that can be adopted for a following requirements elicitation stage in XAI for fraud detection, considering the role of the fraud expert and his socio-technical context. Figure 1 depicts

the scenario-based method, and research design adopted, inspired by [54] and [56]. In Section 6, we discuss how the scenarios obtained in this study can be used for requirements elicitation.

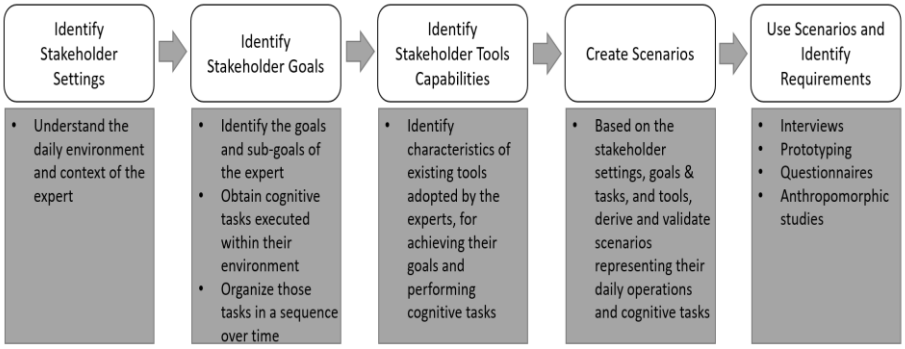

Fig. 1. Scenario-Based Requirements Elicitation Method

3.2 Fraud Detection Context

We focus on the type of fraud naming transaction fraud. In banking, transaction fraud happens when a customer card or online account balance is used to perform a transaction without the customer's consent or awareness [59]. The fraud can happen trough a shopping transaction in a retailer or money transfer between customers of an institution. Organizations have their workflows for transaction fraud detection, derived from research and fraud experts' knowledge. Those workflows, in general, contain events and processes reported as: 1) Transaction Attempt, 2) Transaction Blocking Rules, 3) Transaction Classification, and 4) Transaction Investigation [60]. In the end, there is the Transaction Investigation step, where fraud experts review fraud cases issued by a fraud detection system.

Therefore, domain experts investigate fraud cases and make the final decision if an alert represents a false or true positive for fraud. Nevertheless, it is usually tricky for fraud experts to understand how AI models work, and consequently trust the alerts issued by those models [42]. We illustrate how scenarios would work to identify fraud experts' requirements for providing them with tailored explanations to review fraud cases.

3.3 Using and Demonstrating the Method

We follow the steps depicted in Figure 1, inspired by [54] and [56], to compose the aimed fraud detection scenarios by uncovering the settings with a fraud expert as an actor, their goals and sub-goals, cognitive tasks, and tools providing them with capabilities to review fraud transaction cases.

Those steps are implemented through a problem-centered expert interview [61]. This approach emphasizes the uncovering of problems within the operational context of interviewees. Three experts in banking fraud are interviewed within an Austrian bank, to guarantee multiple perspectives for the creation of the aimed scenarios. Following [61],

the interview starts with a brief introduction into the project in which this study is being developed. Given the experts are already users of a fraud detection system, but not based on AI models, we asked them to think of their current settings and decision-making or cognitive tasks to perform their daily analyses.

In order to demonstrate the steps and the usage of the method depicted in Figure 1, Table 1 brings the interview guide designed to create the aimed fraud detection scenarios. Following the guidelines of [61], we avoided a continuous interruption with questions for the fraud experts, aiming to uncover their context. When they considered the answer was complete, we used the questions in Table 1 to continue the discussion. The questions are inspired by [49], and we tailor them to our context to uncover the elements of scenarios [54].

Table 1. Expert Interview Guide for Scenario-Based Requirements Elicitation for XAI in Fraud Detection

Step	Example
1) Introduction into the Project	The introduction of the researcher and a brief overview into the project within this study is situated.
2) Identify Stakeholder Settings	a) Can you describe a typical day of work within your department?
	b) What is the event that needs to be analyzed during your daily operations?
	c) Do you have preferences for colors and visualizations for performing your analysis?
	d) What type of data is adopted at your fraud detection system and on which you perform your analysis?
	e) How many experts do you have for analyzing outcomes of your system? Do you share tasks for the analyses?
	f) Do you conduct analysis before, during, or after receiving an output from your system?
3) Identify Stakeholder Goals	a) Can you describe what is your end goal when analyzing an output from your fraud detection system?
	b) What are the tasks you need to perform to achieve your end goal?
	c) Do you consider this analysis in a particular order?
4) Identify Stakeholder Tools Capabilities	a) What is the usual medium or channel for obtaining outputs from your fraud detection systems?
	b) Are you interacting with the interfaces for conducting your analysis?
	c) Are you aware of your fraud detection system's capabilities and limitations, and consider those when analyzing fraud cases?
	d) How long can you take to review a fraud case and make a decision during your daily operations?
	e) How many screens do you usually have for performing your analysis?
5) Short Questionnaire	a) Can you give me a summary of your professional experience? b) What is your role in this department?

4 Results: Fraud Detection Scenarios

From the interviews, it was possible to obtain detailed narratives on the daily operations of the experts. A second meeting was arranged with the experts to validate the narratives and qualitative data obtained. On this occasion, they confirmed the existence of two particular scenarios, which are described next using a fictitious name.

"Robert is a fraud expert with years of experience in reviewing fraudulent transaction cases. On a typical day in his work, he receives an alert for a case from his company's fraud detection system. Ideally, the system should deliver fraud cases based on their risk priority as a ranking, followed by the confidence level of a transaction being fraudulent. Robert has three computer screens with interfaces to analyze the fraud case. The interfaces illustrate tables, raw data, and graphical visualizations. He needs more information on the detected fraud in order to make a decision for it being a true positive, as the whole fraud case is composed of little pieces. Robert is interested in the most important pieces of information for analyzing the fraud case and no distractions. He needs to make a decision as soon as possible for the case, as there is no time to think in hours. It should be less to avoid more harm to that customer. Robert starts the analysis of the case by looking into similar cases for which fraud alerts were issued, and tries to understand that fraud by similarities. He realizes more information is needed, and then analyses the destination of that transaction, to observe if it is, for instance, a first time beneficiary. Given that it was detected as an anomalous beneficiary, he looks further into important attributes highlighted by the system to issue the alert and observes that the transaction's location is a high indicator for fraud. He finishes the analysis observing details on the customer data registered in the bank, such as his usual location for performing transactions. He observes a clear anomaly regarding the location indicator, and similar cases where this attribute was the determinant factor for considering the case as a fraud. He reports the case, and the transaction is not processed by the system".

The second scenario is described as follows.

"In similar settings, Robert receives a new alert from the fraud detection system. In this case, he finds it difficult to observe similar past cases for the current case reported. When analyzing the destination of the transaction, he finds it is a usual beneficiary. He then observes the important attributes highlighted by the system and realizes they match to the customer's data. In this scenario, Robert is unsure about the reported case, and performs more actions to investigate the incident. His next moves focus on analyzing further important attributes in the current transaction, and triggered rules by his fraud detection system. Then, he tries to observe the impact of attributes on the transaction and rules influencing the system's outcome. With those in mind, he observes past transactions of the customer to see if they have familiarity with this current behavior. Furthermore, he analyzes the transactions that happened after this alert was issued. Usually, Robert analyzes fraud cases by himself, but in such novel and more complex cases, he collaborates with colleagues to make decisions. They have to analyze it as soon as possible to understand the case, as many customers can be victims of the same scheme. After discussing with his colleagues, Robert realizes the reasons for the transaction being considered fraudulent by the system, and reports it for avoiding harm to the customer."

Consulting with the experts, we name the first scenario as “Clear Transaction Fraud”, when they are certain about the case being a fraud, but need to clarify the reasons for the diagnosis. In the second case, we label it as an “Uncertain Transaction

Fraud", as the experts need to go for more cognitive tasks to clarify the case and protect the customer.

Therefore, we depict in Figure 2 the cognitive tasks performed in both scenarios, which are executed by experts to review fraud cases in their environment and daily operations.

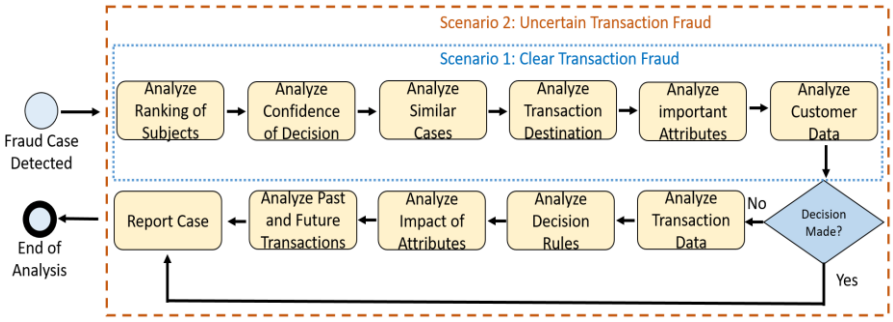

Fig. 2. Fraud Detection Cognitive Tasks Identified in Scenarios Developed with Experts in Banking Fraud

5 Validation of Fraud Scenarios

The expert interviews lasted for approximately one hour each, and the researcher facilitated the discussion. It was noticed that the experts felt comfortable and confident in giving the answers. That is the aim of the problem-centered interview methodology [61], which empowers the interviewee for the provision of real information into their context and problems [62]. Therefore, we recommend the usage of the problem-centered interview methodology for creating scenarios with domain experts.

We omit some details regarding specific attributes of datasets, which were mentioned during the interviews. That is due to privacy concerns and national regulations limiting the banking industry's sharing of fraud detection policies for the safety of their customers. However, we also aim to achieve a level of abstraction for those scenarios, which can enable their adoption for researchers working in XAI for fraud detection.

Therefore, for validation, we conducted a systematic literature review following Webster and Watson [63]. The goal was to investigate studies focused on adopting explanation methods or visual analytics for supporting fraud experts in decision-making. Indeed, it is possible to validate the scenarios and cognitive tasks uncovered when analyzing the literature in visual analytics for fraud detection, as presented in Section 2, given researchers in this domain work on providing fraud experts with visualization tools for examining and reviewing fraud cases. Such tools can be related to explanations being adopted for our current scenarios.

We started the review by identifying comprehensive surveys and references in the field of XAI, to adopt search terms within this literature. The works of [13, 33, 64, 65, 66] were selected based on these criteria. Given the intersection with visual analytics literature for decision-making in fraud, we also adopt terminology from this domain for our systematic review based on [21, 43] and [67-72]. Next, core and most cited surveys

in fraud detection were analyzed for extracting coherent keywords for our review [73-75]. Then, we defined the key terms for our review as: "("visual analytics" OR "explainable ai" OR "explainable artificial intelligence" OR "explanation" OR "interpretable machine learning") AND ("fraud" OR "anomaly" OR "fraud detection")". The databases selected were Scopus, ACM, IEEEXplore, and arXiv. Google Scholar was adopted for backward and forward searches. The filter for papers was focused on proposals adopting visual analytics or explanation methods for supporting experts in decision-making. It was identified 367 potentially relevant papers, from which 52 are deemed relevant for analysis. From those, 38 papers are added as new references in this study.

Table 2 illustrates the cognitive tasks mapped from the systematic literature review, and their association with the scenarios obtained through interviews with fraud experts. We managed to map 13 cognitive tasks. It is shown the supporting papers for each task identified, and whether they are observable from the expert interviews performed to develop fraud detection scenarios. The tasks can inform design principles for the integration of explanation methods and interfaces into fraud detection processes. Finally, a description is available for each task.

We hypothesize that the provided set of cognitive tasks and requirements can better inform the design of user-centric explanation methods and interfaces for fraud detection, promoting the trust of fraud experts for collaboration with AI models predictions. Researchers in XAI can refer to those cognitive tasks when designing explanation methods and interfaces for the domain of fraud detection.

It is noticeable that every cognitive task from fraud scenarios is identified in the XAI and visual analytics literature in fraud detection. When discussing with the experts regarding the non-presence in their scenarios of the tasks *Analyze Contrast Between*, *Analyze Cases in Clusters*, *Analyze Relationships Between Attributes*, they highlighted it is due to the available capabilities of the current fraud detection system in use. However, they highlighted that such tasks are also valuable and useful in their context.

6 Usage of Scenarios for Requirements Elicitation for Explanations

With the usage of the scenario-based method, we can establish scenarios as templates for further requirements elicitation steps. As illustrated by the scenario narratives and cognitive tasks in Sections 4 and 5, it is possible to envision an actor's real context in a scenario, the fraud expert in this study. With these scenarios, it is possible to better plan experiments deploying explanations for the usage by the expert, according to his cognitive tasks.

Table 2. Cognitive Tasks in Fraud Detection Scenarios and their Presence in the Literature of XAI and Visual Analytics for Fraud Detection

Literature Support	Total of Literature Supporting Papers	Observable in Experts Fraud Scenarios	Cognitive Task for Decision-Making in Fraud Detection	Description
[22,36,43,44,55,68,71, 72,80,88,89,92,93, 95,96,97,98, 101,102,103,104,105, 106,107]	24	Yes	Analyze Relationships Between Subjects	This task is associated with the analysis of a transaction destination. Experts observe the relationship between different subjects, which can be different customers within a network of transactions. The aim is to see, for instance, if a customer is usually performing transfers to another, or if it is a sign of an anomaly.
[21,22,27,43,55,67,68, 71,72,76,79,82,88,89, 92,93,95,106, ,107,110,112]	21	Yes	Analyze Attributes over Temporal Perspective	This task relates to the analysis of past and future transactions by experts. The aim is to analyze the values of attributes over time. For example, to analyze the number of transactions performed in a specific time frame, or the number of transfers to a destination in past and future dates.
[21,39,41,42,43,44,67, 72,78,80,81,83,88, 89,90,91,92,93,94]	19	Yes	Analyze the Importance of Attributes on Decisions	Analyze the most important attributes as reasons for a transaction being considered as a fraud by the system.
[22,72,76,80,83,84,86,8 9,90,92,99,100, 108,109,110,111]	16		Analyze Relationships Between Attributes	Observe how changes in the values of two attributes are influencing the predictions of a system for fraud.
[38,41,43,68,72,82,91, 92,93,94,95,96,97]	13	Yes	Analyze Feature Distribution	This task is associated with the analysis of current transaction data, or the common distribution of attributes, which represent the known pattern and behavior of users. That can be represented by averages, minimum and maximum thresholds for attributes.
[16,38,42,67,76, 77, 78,79,80,81,82,83]	12	Yes	Analyze Similar Cases	Analyze fraud cases which are similar to the current case detected by the fraud detection system.
[22,27,32,72,80,88,90, 101,102,110,111,113]	12	Yes	Analyze Decision Path Rules	This task is associated with the analysis of decision rules by experts. Detailed observation on the decision path made by a fraud detection system, such as rules and attributes associated with the rules to provide predictions.
[42,79,80,81,83,87,88, 94,98,99,100]	11	Yes	Analyze Impact of Attributes	Analyze what is the influence of an attribute in the prediction of a system when changing the value of attributes.
[71,72,79,85,86,87]	6		Analyze Cases in Clusters	Observe cases in groups according to the characteristics of the transactions and their attributes.
[31,41,83,92,94]	5	Yes	Analyze Confidence of Decision	Observe the confidence of the system in predicting and detecting frauds.
[79,83,84]	3		Analyze Contrast Between Cases	Detect differences between a legitimate and a fraudulent transaction.
[21,44]	2	Yes	Analyze the Ranking of Subjects	Visualize the most important transactions and attributes to be analyzed, given the time constraints fraud experts have in their scenarios.
[71,93]	2		Analyze Decision in Natural Language	Analyze rationales on the reasons for predictions, such as textual descriptions of the reasons for a transaction being classified as fraudulent.

The scenarios start by describing the settings of a fraud expert and the system he works with. Based on the narratives, it is clear that an AI model deployed in this environment should provide the riskiest transactions for a productive relationship with the

expert. It is also described by the expert the common interface he is used to operating, which can guide on the deployment of explanations aligned with such design, including tables and graphical charts. It is possible to observe non-functional requirements in the scenarios already. For instance, the experts stated they need only the most important pieces of evidence for making a decision, which is aligned with the non-functional requirement stated by Miller [33] that explanations should be selective, and not overload their users with unnecessary reasons for an AI prediction. In the context of fraud in banking, the experts also point out a decision should be made promptly, which might indicate the need to support his decision-making with explanations that do not require heavy mental workload for understandability [42]. Those constraints are vital as they can dictate which XAI methods fit, for instance, into the time an expert has to review fraudulent transactions.

From the first scenario, with a clear transaction fraud, it is noticeable the specific tasks and sequence of cognitive tasks performed by the expert. The narrative helps in defining specific explanation which can be provided in experiments. Given the expert is usually focusing on reviewing individual fraud cases, a preliminary filter for explanation methods can be already established, such as to adopt local explanations provided by post-hoc XAI methods [13]. As the expert starts comparing cases and looking into destinations of transactions, an explanation interface might be presented with a case-based and network visualization explanation for reviewing cases. Furthermore, it could be deployed a feature importance explanation [98], as fraud experts need to investigate the most critical attributes impacting the prediction, such as the location of a transaction.

In the second scenario, it is also possible to think of explanations to be adopted in experiments. The expert goes further in his analysis by examining inference rules and the impact of attributes in the outcome of the system, which can be supported by explanations showing decision rules, such as Anchors [114], and counterfactuals and what-if scenarios [115]. Besides, he analyzes the past and further transactions of a customer, which can be aided by a temporal explanation component in the sequence of customer transactions.

Therefore, a scenario enables the establishment of assumptions regarding explanation interfaces that can be deployed in experiments as prototypes for uncovering experts' requirements [54]. Questions concerning the order of steps enable the potential design of workflows for fraud detection with the support of explanation methods, as the expert details the order of steps during his analysis of fraud cases. The assumptions for explanations to deploy on scenarios are based on XAI literature describing explanation interfaces and tools [116, 117]. Figure 3 depicts the usage of the cognitive tasks in scenario 1 in an experiment with prototypes of explanations interfaces.

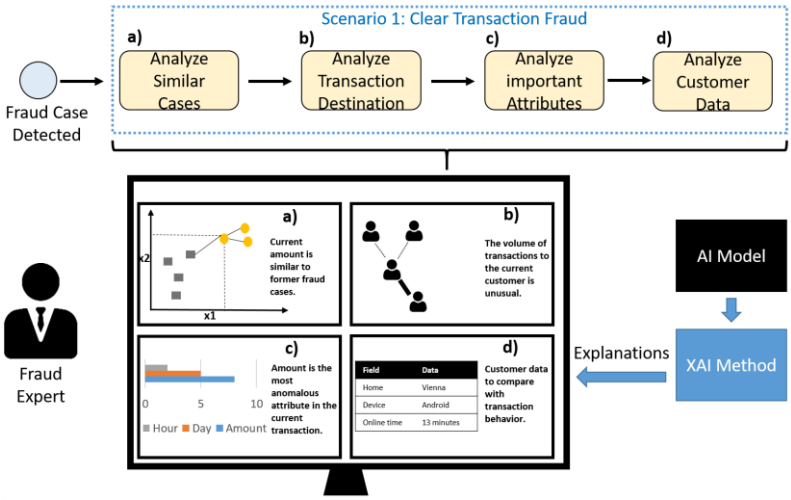

Fig. 3. Using Scenarios within an Experiment and Prototyping to Identify Requirements of Experts

7 Conclusions

This study calls for the potential of developing XAI research with an information systems theoretical lens. This research is aligned with user-centric XAI, which regards the vital role of stakeholders of explanations, their requirements, and their needs for understanding AI predictions. This study reinforces the need and benefits of understanding the socio-technical and operational environment of a stakeholder before deploying explanations to support their decision-making processes.

We demonstrate the usage of the scenario-based method for requirements elicitation, well regarded in IS and software engineering research. The method is adopted within a domain rarely addressed from a user perspective in XAI, which is fraud detection. We derived two fraud detection scenarios, discuss how they can be adopted for developing user-centric explanation methods in prototypes, and further elicit user requirements for explanations, such as having a selective set of explanations and enabling experts to perform local comparisons of fraud cases, respectively.

It is demonstrated the potential of the scenario-based method in uncovering directions and opportunities for developers of XAI methods and explanations in the early stage of their implementation. We aim to provide these scenarios for the XAI community interested in developing explanation methods tailored for the particularities of the fraud detection domain. Regarding limitations, the focus of this study was on domain experts, the users of AI predictions. Therefore, the scenarios are not focused on AI engineers who work in developing and improving AI models. Scenarios serve as a template for elicitation of requirements, so the direct relationships with specific explanations are inferred by the researcher based on previous literature defining explainability features.

As future work, the scenarios will be adopted through experiments with fraud experts and user-centric explanation prototypes. The aim is to follow the discovered tasks for

decision-making to identify user requirements for appropriate explanation methods. The goal is to detect patterns and reveal potential design principles for integrating explanations into the domain of fraud detection, from a user-centric XAI perspective.

Acknowledgements. This research was supported by the European Union Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie grant agreement No. 765395; and supported, in part, by Science Foundation Ireland grant 13/RC/2094.

References

1. Cirqueira D., Hofer M., Nedbal D., Helfert M., Bezbradica M. (2020) Customer Purchase Behavior Prediction in E-commerce: A Conceptual Framework and Research Agenda. In: Ceci M., Loglisci C., Manco G., Masciari E., Ras Z. (eds) New Frontiers in Mining Complex Patterns. NFMCP 2019. Lecture Notes in Computer Science, vol 11948. Springer, Cham
2. Bielozorov, A., Bezbradica, M. and Helfert, M., 2019, July. The role of user emotions for content personalization in e-commerce: literature review. In International Conference on Human-Computer Interaction (pp. 177-193). Springer, Cham.
3. Cakir, G., Bezbradica, M. and Helfert, M., 2019, June. The Shift from Financial to Non-financial Measures During Transition into Digital Retail–A Systematic Literature Review. In International Conference on Business Information Systems (pp. 189-200). Springer, Cham.
4. Iftikhar, R., Pourzolfaghar, Z. & Helfert, M. (2019). Omnichannel Value Chain: Mapping Digital Technologies for Channel Integration Activities. In A. Siarheyeva, C. Barry, M. Lang, H. Linger, & C. Schneider (Eds.), Information Systems Development: Information Systems Beyond 2020 (ISD2019 Proceedings). Toulon, France: ISEN Yncréa Méditerranée.
5. Cirqueira, D., Helfert, M. and Bezbradica, M., 2019, September. Towards Preprocessing Guidelines for Neural Network Embedding of Customer Behavior in Digital Retail. In Proceedings of the 2019 3rd International Symposium on Computer Science and Intelligent Control (pp. 1-6).
6. Ryman-Tubb, N.F., Krause, P. and Garn, W., 2018. How Artificial Intelligence and machine learning research impacts payment card fraud detection: A survey and industry benchmark. Engineering Applications of Artificial Intelligence, 76, pp.130-157.
7. Mohseni, S., Zarei, N., & Ragan, E.D. (2019). A Multidisciplinary Survey and Framework for Design and Evaluation of Explainable AI Systems. arXiv: Human-Computer Interaction.
8. Abdul Miller, T., 2019. " But why?" Understanding explainable artificial intelligence. XRDS: Crossroads, The ACM Magazine for Students, 25(3), pp.20-25.
9. Chazette, L. and Schneider, K., 2020. Explainability as a non-functional requirement: challenges and recommendations. Requirements Engineering, pp.1-22.
10. Holzinger, A., Biemann, C., Pattichis, C.S. and Kell, D.B., 2017. What do we need to build explainable AI systems for the medical domain?. arXiv preprint arXiv:1712.09923.
11. Samek, W., Montavon, G., Vedaldi, A., Hansen, L.K. and Müller, K.R. eds., 2019. Explainable AI: interpreting, explaining and visualizing deep learning (Vol. 11700). Springer Nature.
12. Goebel, R., Chander, A., Holzinger, K., Lecue, F., Akata, Z., Stumpf, S., Kieseberg, P. and Holzinger, A., 2018, August. Explainable AI: the new 42?. In International Cross-Domain Conference for Machine Learning and Knowledge Extraction (pp. 295-303). Springer, Cham.

13. Adadi, A. and Berrada, M., 2018. Peeking inside the black-box: A survey on Explainable Artificial Intelligence (XAI). IEEE Access, 6, pp.52138-52160.
14. Wang, D., Yang, Q., Abdul, A. and Lim, B.Y., 2019, May. Designing theory-driven user-centric explainable AI. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (pp. 1-15).
15. Miller, T., Howe, P. and Sonenberg, L., 2017. Explainable AI: Beware of inmates running the asylum or: How I learnt to stop worrying and love the social and behavioural sciences. arXiv preprint arXiv:1712.00547."
16. Moalosi, M., Hlomani, H. and Phefo, O.S., 2019. Combating credit card fraud with online behavioural targeting and device fingerprinting. International Journal of Electronic Security and Digital Forensics, 11(1), pp.46-69."
17. Holzinger, A., Langs, G., Denk, H., Zatloukal, K. and Müller, H., 2019. Causability and explainability of artificial intelligence in medicine. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 9(4), p.e1312.
18. Holzinger, A., Carrington, A. and Müller, H., 2020. Measuring the quality of explanations: the system causability scale (SCS). KI-Künstliche Intelligenz, pp.1-6.
19. Akula, A.R., Liu, C., Saba-Sadiya, S., Lu, H., Todorovic, S., Chai, J.Y. and Zhu, S.C., 2019. X-tom: Explaining with theory-of-mind for gaining justified human trust. arXiv preprint arXiv:1909.06907."
20. Delaney, B.C., Fitzmaurice, D.A., Riaz, A. and Hobbs, F.R., 1999. Can computerised decision support systems deliver improved quality in primary care?. Bmj, 319(7220), p.1281."
21. Leite, R.A., Gschwandtner, T., Miksch, S., Kriglstein, S., Pohl, M., Gstrein, E. and Kuntner, J., 2017. Eva: Visual analytics to identify fraudulent events. IEEE transactions on visualization and computer graphics, 24(1), pp.330-339."
22. Holzinger, A., 2016. Interactive machine learning for health informatics: when do we need the human-in-the-loop?. Brain Informatics, 3(2), pp.119-131.
23. Abdul, Ashraf, et al. ""Trends and trajectories for explainable, accountable and intelligible systems: An hci research agenda."" Proceedings of the 2018 CHI conference on human factors in computing systems. ACM, 2018."
24. Spinner, T., Schlegel, U., Schäfer, H. and El-Assady, M., 2019. explAIner: A visual analytics framework for interactive and explainable machine learning. IEEE transactions on visualization and computer graphics, 26(1), pp.1064-1074.
25. Chatzimparmpas, A., Martins, R.M., Jusufi, I. and Kerren, A., 2020. A survey of surveys on the use of visualization for interpreting machine learning models. Information Visualization, p.1473871620904671.
26. Chatzimparmpas, A., Martins, R.M., Jusufi, I., Kucher, K., Rossi, F. and Kerren, A., 2020. The State of the Art in Enhancing Trust in Machine Learning Models with the Use of Visualizations. In Computer graphics forum (Print).
27. Bell, S., 2013. Learning with information systems: Learning cycles in information systems development. Routledge.
28. Ostrowski, Lukasz and Helfert, Markus, "Reference Model in Design Science Research to Gather and Model Information" (2012). AMCIS 2012 Proceedings. 3.https://aisel.aisnet.org/amcis2012/proceedings/SystemsAnalysis/3
29. Browne, G.J. and Rogich, M.B., 2001. An empirical investigation of user requirements elicitation: Comparing the effectiveness of prompting techniques. Journal of Management Information Systems, 17(4), pp.223-249.
30. Carroll, J.M., 1996. Becoming social: expanding scenario-based approaches in HCI. Behaviour & Information Technology, 15(4), pp.266-275.
31. Malle, B.F., 2011. Time to give up the dogmas of attribution: An alternative theory of behavior explanation. In Advances in experimental social psychology (Vol. 44, pp. 297-352). Academic Press."

32. Preece, A., Harborne, D., Braines, D., Tomsett, R. and Chakraborty, S., 2018. Stakeholders in explainable AI. arXiv preprint arXiv:1810.00184."
33. Miller, T., 2019. Explanation in artificial intelligence: Insights from the social sciences. Artificial Intelligence, 267, pp.1-38."
34. Linsley, D., Shiebler, D., Eberhardt, S. and Serre, T., 2018. Global-and-local attention networks for visual recognition. arXiv preprint arXiv:1805.08819.
35. Seo, S., Huang, J., Yang, H. and Liu, Y., 2017, August. Interpretable convolutional neural networks with dual local and global attention for review rating prediction. In Proceedings of the eleventh ACM conference on recommender systems (pp. 297-305).
36. Doshi-Velez, Finale, and Been Kim. "Towards a rigorous science of interpretable machine learning." arXiv preprint arXiv:1702.08608 (2017).
37. Došilović, Filip Karlo, Mario Brčić, and Nikica Hlupić. "Explainable artificial intelligence: A survey." 2018 41st International convention on information and communication technology, electronics and microelectronics (MIPRO). IEEE, 2018.
38. Laughlin, Brandon, Karthik Sankaranarayanan, and Khalil El-Khatib. "A Service Architecture Using Machine Learning to Contextualize Anomaly Detection." Journal of Database Management (JDM) 31.1 (2020): 64-84.
39. Antwarg, Liat, Bracha Shapira, and Lior Rokach. "Explaining anomalies detected by autoencoders using SHAP." arXiv preprint arXiv:1903.02407 (2019).
40. Lundberg, Scott M., and Su-In Lee. "A unified approach to interpreting model predictions." Advances in neural information processing systems. 2017.
41. Weerts, Hilde JP, Werner van Ipenburg, and Mykola Pechenizkiy. "A Human-Grounded Evaluation of SHAP for Alert Processing." arXiv preprintarXiv:1907.03324 (2019).
42. Weerts, Hilde JP, Werner van Ipenburg, and Mykola Pechenizkiy. "Case-Based Reasoning for Assisting Domain Experts in Processing Fraud Alerts of Black-BoxMachine Learning Models." arXiv preprint arXiv:1907.03334 (2019).
43. Dilla, William N., and Robyn L. Raschke. ""Data visualization for fraud detection: Practice implications and a call for future research."" International Journal of Accounting Information Systems 16 (2015): 1-22.
44. Leite, R.A., Gschwandtner, T., Miksch, S., Gstrein, E. and Kuntner, J., 2018. Visual analytics for event detection: Focusing on fraud. Visual Informatics, 2(4), pp.198-212."
45. T. Munzner. A nested model for visualization design and validation.IEEE transactions on visualization and computer graphics, 15(6):921–928, 2009
46. Franklin, L., Pirrung, M., Blaha, L., Dowling, M. and Feng, M., 2017, October. Toward a visualization-supported workflow for cyber alert management using threat models and human-centered design. In 2017 IEEE Symposium on Visualization for Cyber Security (VizSec) (pp. 1-8). IEEE.
47. Hall, M., Harborne, D., Tomsett, R., Galetic, V., Quintana-Amate, S., Nottle, A. and Preece, A., 2019. A Systematic Method to Understand Requirements for Explainable AI (XAI) Systems. In Proceedings of the IJCAI Workshop on eXplainable Artificial Intelligence (XAI 2019), Macau, China.
48. Köhl, M.A., Baum, K., Langer, M., Oster, D., Speith, T. and Bohlender, D., 2019, September. Explainability as a Non-Functional Requirement. In 2019 IEEE 27th International Requirements Engineering Conference (RE) (pp. 363-368). IEEE.
49. Liao, Q.V., Gruen, D. and Miller, S., 2020. Questioning the AI: Informing Design Practices for Explainable AI User Experiences. arXiv preprint arXiv:2001.02478.
50. Eiband, M., Schneider, H., Bilandzic, M., Fazekas-Con, J., Haug, M. and Hussmann, H., 2018, March. Bringing transparency design into practice. In 23rd international conference on intelligent user interfaces (pp. 211-223).

51. Wolf, C.T., 2019, March. Explainability scenarios: towards scenario-based XAI design. In Proceedings of the 24th International Conference on Intelligent User Interfaces (pp. 252-257).
52. West, J. and Bhattacharya, M., 2016. Intelligent financial fraud detection: a comprehensive review. Computers & security, 57, pp.47-66.
53. Dick, J., Hull, E. and Jackson, K., 2017. Requirements engineering. Springer."
54. Rosson, M.B. and Carroll, J.M., 2009. Scenario-based design. In Human-computer interaction (pp. 161-180). CRC Press."
55. Maguire, M. and Bevan, N., 2002, August. User requirements analysis. In IFIP World Computer Congress, TC 13 (pp. 133-148). Springer, Boston, MA."
56. Hertzum, M., 2003. Making use of scenarios: a field study of conceptual design. International Journal of Human-Computer Studies, 58(2), pp.215-239."
57. Diaper, D. and Stanton, N. eds., 2003. The handbook of task analysis for human-computer interaction. CRC Press.
58. Go, K. and Carroll, J.M., 2003. Scenario-based task analysis. The handbook of task analysis for human-computer interaction, 117.
59. Raj, S. Benson Edwin, and A. Annie Portia. ""Analysis on credit card fraud detection methods."" 2011 International Conference on Computer, Communication and Electrical Technology (ICCCET). IEEE, 2011."
60. Dal Pozzolo, A., Boracchi, G., Caelen, O., Alippi, C. and Bontempi, G., 2017. Credit card fraud detection: a realistic modeling and a novel learning strategy. IEEE transactions on neural networks and learning systems, 29(8), pp.3784-3797."
61. Witzel, Andreas, and Herwig Reiter. The problem-centred interview. Sage, 2012."
62. Forstner, A. and Nedbal, D., 2017. A problem-centered analysis of enterprise social software projects. Procedia computer science, 121, pp.389-397."
63. Webster, J. and Watson, R.T., 2002. Analyzing the past to prepare for the future: Writing a literature review. MIS quarterly, pp.xiii-xxiii.
64. Arrieta, A.B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., García, S., Gil-López, S., Molina, D., Benjamins, R. and Chatila, R., 2020. Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. Information Fusion, 58, pp.82-115.
65. Gunning. Explainable artificial intelligence (XAI), Defense Advanced Research Projects Agency (DARPA). Accessed: Jun. 6, 2018. [Online].Available:http://www.darpa.mil/program/explainable-artificial-intelligence
66. Mueller, S.T., Hoffman, R.R., Clancey, W., Emrey, A. and Klein, G., 2019. Explanation in human-AI systems: A literature meta-review, synopsis of key ideas and publications, and bibliography for explainable AI. arXiv preprint arXiv:1902.01876.
67. Leite, R.A., Gschwandtner, T., Miksch, S., Gstrein, E. and Kuntner, J., 2015, October. Visual analytics for fraud detection and monitoring. In 2015 IEEE Conference on Visual Analytics Science and Technology (VAST) (pp. 201-202). IEEE.
68. Novikova, E., Kotenko, I. and Fedotov, E., 2014. Interactive Multi-View Visualization for Fraud Detection in Mobile Money Transfer Services. International Journal of Mobile Computing and Multimedia Communications (IJMCMC), 6(4), pp.73-97.
69. Argyriou, E.N., Symvonis, A. and Vassiliou, V., 2014, January. A fraud detection visualization system utilizing radial drawings and heat-maps. In 2014 International Conference on Information Visualization Theory and Applications (IVAPP) (pp. 153-160). IEEE.
70. Chang, R., Lee, A., Ghoniem, M., Kosara, R., Ribarsky, W., Yang, J., Suma, E., Ziemkiewicz, C., Kern, D. and Sudjianto, A., 2008. Scalable and interactive visual analysis of financial wire transactions for fraud detection. Information visualization, 7(1), pp.63-76.
71. Shi, Y., Liu, Y., Tong, H., He, J., Yan, G. and Cao, N., 2019. Visual Analytics of Anomalous User Behaviors: A Survey. arXiv preprint arXiv:1905.06720.

72. Sun, J., Zhu, Q., Liu, Z., Liu, X., Lee, J., Su, Z., Shi, L., Huang, L. and Xu, W., 2018, April. Fraudvis: Understanding unsupervised fraud detection algorithms. In 2018 IEEE Pacific Visualization Symposium (PacificVis) (pp. 170-174). IEEE
73. Ahmed, Mohiuddin, Abdun Naser Mahmood, and Md Rafiqul Islam. ""A survey of anomaly detection techniques in financial domain."" Future Generation Computer Systems 55 (2016): 278-288.
74. Phua, Clifton, et al. ""A comprehensive survey of data mining-based fraud detection research."" arXiv preprint arXiv:1009.6119 (2010).
75. Bolton, Richard J., and David J. Hand. ""Statistical fraud detection: A review."" Statistical science (2002): 235-249.
76. Interpretable machine learning as decision support for processing fraud alerts Weerts, H. J. P. (Author). 24 Jun 2019
77. Avanti Shrikumar, Peyton Greenside, and Anshul Kundaje. 2017. Learning important features through propagating activation differences.arXiv preprintarXiv:1704.02685(2017).
78. Böhmer, K. and Rinderle-Ma, S., 2019. Mining association rules for anomaly detection in dynamic process runtime behavior and explaining the root cause to users. Information Systems, p.101438.
79. Guo, S., Jin, Z., Chen, Q., Gotz, D., Zha, H. and Cao, N., 2019. Visual Anomaly Detection in Event Sequence Data. arXiv preprint arXiv:1906.10896.
80. Zhao, X., Wu, Y., Lee, D.L. and Cui, W., 2018. iforest: Interpreting random forests via visual analytics. IEEE transactions on visualization and computer graphics, 25(1), pp.407-416.
81. Mejia-Lavalle, M., 2010, September. Outlier detection with innovative explanation facility over a very large financial database. In 2010 IEEE Electronics, Robotics and Automotive Mechanics Conference (pp. 23-27). IEEE.
82. Novikova, E. and Kotenko, I., 2019. Visualization-Driven Approach to Fraud Detection in the Mobile Money Transfer Services. In Algorithms, Methods, and Applications in Mobile Computing and Communications (pp. 205-236). IGI Global.
83. Collaris, D. and van Wijk, J.J., 2020, June. ExplainExplore: Visual Exploration of Machine Learning Explanations. In 2020 IEEE Pacific Visualization Symposium (PacificVis) (pp. 26-35). IEEE.
84. Zhu, J., Liapis, A., Risi, S., Bidarra, R. and Youngblood, G.M., 2018, August. Explainable AI for designers: A human-centered perspective on mixed-initiative co-creation. In 2018 IEEE Conference on Computational Intelligence and Games (CIG) (pp. 1-8). IEEE.
85. Didimo, W., Liotta, G., Montecchiani, F. and Palladino, P., 2011, March. An advanced network visualization system for financial crime detection. In 2011 IEEE Pacific visualization symposium (pp. 203-210). IEEE.
86. Ko, S., Cho, I., Afzal, S., Yau, C., Chae, J., Malik, A., Beck, K., Jang, Y., Ribarsky, W. and Ebert, D.S., 2016, June. A survey on visual analysis approaches for financial data. In Computer Graphics Forum (Vol. 35, No. 3, pp. 599-617).
87. Olszewski, D., 2014. Fraud detection using self-organizing map visualizing the user profiles. Knowledge-Based Systems, 70, pp.324-334.
88. Perez, D.G. and Lavalle, M.M., 2011, November. Outlier detection applying an innovative user transaction modeling with automatic explanation. In 2011 IEEE Electronics, Robotics and Automotive Mechanics Conference (pp. 41-46). IEEE.
89. Huang, M.L., Liang, J. and Nguyen, Q.V., 2009, July. A visualization approach for frauds detection in financial market. In 2009 13th International Conference Information Visualisation (pp. 197-202). IEEE.
90. Collaris, D., Vink, L.M. and van Wijk, J.J., 2018. Instance-level explanations for fraud detection: a case study. arXiv preprint arXiv:1806.07129.

91. Lin, H., Gao, S., Gotz, D., Du, F., He, J. and Cao, N., 2017. Rclens: Interactive rare category exploration and identification. IEEE transactions on visualization and computer graphics, 24(7), pp.2223-2237.
92. Leite, R.A., Gschwandtner, T., Miksch, S., Gstrein, E. and Kuntner, J., 2016, June. Visual Analytics for Fraud Detection: Focusing on Profile Analysis. In EuroVis (Posters) (pp. 45-47).
93. Xie, C., Chen, W., Huang, X., Hu, Y., Barlowe, S. and Yang, J., 2014. VAET: A visual analytics approach for e-transactions time-series. IEEE transactions on visualization and computer graphics, 20(12), pp.1743-1752.
94. Gal, G., Singh, K. and Best, P., 2016. Interactive visual analysis of anomalous accounts payable transactions in SAP enterprise systems. Managerial Auditing Journal.
95. Didimo, W., Liotta, G. and Montecchiani, F., 2014. Network visualization for financial crime detection. Journal of Visual Languages & Computing, 25(4), pp.433-451.
96. Rieke, R., Zhdanova, M., Repp, J., Giot, R. and Gaber, C., 2013, September. Fraud detection in mobile payments utilizing process behavior analysis. In 2013 International Conference on Availability, Reliability and Security (pp. 662-669). IEEE.
97. Leite, R.A., Gschwandtner, T., Miksch, S., Gstrein, E. and Kuntner, J., 2018, June. Network Analysis for Financial Fraud Detection. In EuroVis (Posters) (pp. 21-23).
98. Ribeiro, M.T., Singh, S. and Guestrin, C., 2016, August. " Why should I trust you?" Explaining the predictions of any classifier. In Proceedings of the 22nd ACM SIGKDD international conference on knowledge discovery and data mining (pp. 1135-1144).
99. Gupta, N., Eswaran, D., Shah, N., Akoglu, L. and Faloutsos, C., 2018, September. Beyond outlier detection: LOOKOUT for pictorial explanation. In Joint European Conference on Machine Learning and Knowledge Discovery in Databases (pp. 122-138). Springer, Cham.
100. Vojíř, S., Zeman, V., Kuchař, J. and Kliegr, T., 2018. EasyMiner. eu: Web framework for interpretable machine learning based on rules and frequent itemsets. Knowledge-Based Systems, 150, pp.111-115.
101. Chmielewski, M. and Stąpor, P., 2018. Hidden information retrieval and evaluation method and tools utilising ontology reasoning applied for financial fraud analysis. In MATEC Web of Conferences (Vol. 210, p. 02019). EDP Sciences.
102. Vaculík, K. and Popelínský, L., 2016, October. Dgrminer: Anomaly detection and explanation in dynamic graphs. In International Symposium on Intelligent Data Analysis (pp. 308-319). Springer, Cham.
103. Kobayashi, M. and Ito, T., 2007, November. A transactional relationship visualization system in Internet auctions. In 2007 IEEE/WIC/ACM International Conference on Intelligent Agent Technology (IAT'07) (pp. 248-251). IEEE.
104. Chmielewski, Mariusz, and Piotr Stąpor. "Money Laundering Analytics Based on Contextual Analysis. Application of Problem Solving Ontologies in Financial Fraud Identification and Recognition." In Information Systems Architecture and Technology: Proceedings of 37th International Conference on Information Systems Architecture and Technology–ISAT 2016–Part I, pp. 29-39. Springer, Cham, 2017.
105. Wang, D., Lin, J., Cui, P., Jia, Q., Wang, Z., Fang, Y., Yu, Q., Zhou, J., Yang, S. and Qi, Y., 2019, November. A Semi-supervised Graph Attentive Network for Financial Fraud Detection. In 2019 IEEE International Conference on Data Mining (ICDM) (pp. 598-607). IEEE.
106. Chang, R., Ghoniem, M., Kosara, R., Ribarsky, W., Yang, J., Suma, E., Ziemkiewicz, C., Kern, D. and Sudjianto, A., 2007, October. Wirevis: Visualization of categorical, time-varying data from financial transactions. In 2007 IEEE Symposium on Visual Analytics Science and Technology (pp. 155-162). IEEE.
107. Didimo, W., Liotta, G., Montecchiani, F., Richard, P., Kraus, M., Laramee, R.S. and Braz, J., 2012. Vis4AUI: Visual Analysis of Banking Activity Networks. In GRAPP/IVAPP (pp. 799-802).

108. Mokoena, T., Lebogo, O., Dlaba, A. and Marivate, V., 2017, September. Bringing sequential feature explanations to life. In 2017 IEEE AFRICON (pp. 59-64). IEEE.
109. Hao, M.C., Dayal, U., Sharma, R.K., Keim, D.A. and Janetzko, H., 2010, January. Visual analytics of large multidimensional data using variable binned scatter plots. In Visualization and Data Analysis 2010 (Vol. 7530, p. 753006). International Society for Optics and Photonics.
110. Turner, R., 2016, September. A model explanation system. In 2016 IEEE 26th International Workshop on Machine Learning for Signal Processing (MLSP) (pp. 1-6). IEEE.
111. Dumas, M., McGuffin, M.J. and Lemieux, V.L., 2014, November. Financevis. net-a visual survey of financial data visualizations. In Poster Abstracts of IEEE Conference on Visualization (Vol. 2, p. 8).
112. Carminati, M., Caron, R., Maggi, F., Epifani, I. and Zanero, S., 2014, June. BankSealer: An online banking fraud analysis and decision support system. In IFIP International Information Security Conference (pp. 380-394). Springer, Berlin, Heidelberg.
113. Das, S., Islam, M.R., Jayakodi, N.K. and Doppa, J.R., 2019. Active Anomaly Detection via Ensembles: Insights, Algorithms, and Interpretability. arXiv preprint arXiv:1901.08930.
114. Ribeiro, M.T., Singh, S. and Guestrin, C., 2018, April. Anchors: High-precision model-agnostic explanations. In Thirty-Second AAAI Conference on Artificial Intelligence.
115. Byrne, R.M., 2019, August. Counterfactuals in Explainable Artificial Intelligence (XAI): Evidence from Human Reasoning. In IJCAI (pp. 6276-6282).
116. Du, M., Liu, N. and Hu, X., 2019. Techniques for interpretable machine learning. Communications of the ACM, 63(1), pp.68-77.
117. Molnar, C., 2019. Interpretable machine learning. Lulu. com.