Data Min Knowl Disc manuscript No.
(will be inserted by the editor)

Detecção de Fraudes: Uma Revisão Sistemática

Jean Avila Rangel · Maria Claudia Figueiredo Pereira Emer · Adolfo Gustavo Serra Seca Neto

Received: date / Accepted: date

Resumo Insert your abstract here. Include keywords, PACS and mathematical subject classification numbers as needed.

Keywords Fraud detection · Anomaly detection · Deception detection · Standard deviation detection · Detecção de fraude · Detecção de anomalia · Detecção de engano · Detecção de desvio padrão

1 Introdução

A detecção de fraudes é utilizada para resolver problemas variados, sendo geralmente utilizada para reduzir falhas de segurança em sistemas onde há gasto de recursos com usuários mal intencionados.

O controle organizacional de uma empresa ou setor pode garantir a sua boa estabilidade. Soluções para detectar, prevenir e evitar fraudes podem se tornar uma ferramenta para auxiliar a economia de recursos [Chan et al, 1999].

Em todo contexto organizacional, cada ambiente possui um tipo de tratamento e armazenamento de dados. Portanto, ambientes podem possuir dados organizados de maneira estável por induzirem normativas e tecnologias padronizadas ou fazer exatamente o contrário, possuindo dados desorganizados com

Jean Avila Rangel
Federal University of Technology - Paraná, 3165 Sete de Setembro Avenue, Curitiba, PR 80230-901, BRA

Maria Claudia Figueiredo Pereira Emer · Adolfo Gustavo Serra Seca Neto
Academic Department of Informatics, Federal University of Technology - Paraná, 3165 Sete de Setembro Avenue, Curitiba, PR 80230-901, BRA
E-mail: mciemer@gmail.com

Adolfo Gustavo Serra Seca Neto
E-mail: adolfo@dainf.ct.utfpr.edu.br

poucas conexões lógicas. Desta maneira, este estudo visa conhecer abordagens gerais e adaptáveis em detecção de fraudes.

A detecção de fraudes vem sendo utilizada há muito tempo para controle organizacional e econômico [Seyedhossein and Hashemi, 2010]. Em estudos realizados no estado da arte, houve uma grande apresentação sobre algoritmos para detectar fraudes em sistemas financeiros ou de cartão de crédito [Chan et al, 1999], [Chandola et al, 2009] e [**?**].

O objetivo geral deste trabalho é realizar uma revisão sistemática em estudos relacionados à detecção de fraudes. Desta forma, sistemas desenvolvidos para inspecionar desvio de padrões, comportamentos indevidos ou fraudes serão identificados, categorizados e agrupados conforme as técnicas e áreas abordadas.

Como objetivos específicos, este trabalho visa examinar se os estudos realizados em detecção de fraudes possuem abertura para áreas pouco ou não abordadas. Caso haja necessidade, categorizar possíveis trabalhos futuros em lacunas no assunto.

Além disso, este trabalho conta como objetivo específico categorizar as técnicas mais utilizadas para detectar fraudes e as áreas mais abordadas. Espera-se realizar uma revisão sistemática considerando os trabalhos publicados após a elaboração das ultimas revisões sistemáticas do Estado da Arte.

Após realizar a revisão da literatura, este artigo se propõe a elencar como os autores descreveram e categorizaram as áreas de detecção de fraudes e quais são tecnologias as mais utilizadas para cada contexto.

A realização da revisão sistemática proposta por este trabalho obtém motivação devido à crescente expansão do Estado da Arte no assunto. Em pesquisas realizadas em bases de dados por trabalhos realizados na área de detecção de fraude, notou-se a produção de muito material anteriormente ao ano de 2010, porém com um significativo aumento na porcentagem de publicações posteriores a 2010. Este fator indica o crescimento do interesse da comunidade científica em pesquisar o assunto.

Junto com a importância do assunto verificada após os estudos, grande parte dos autores destacaram que o problema computacional ocorrido em todos os casos é a não detecção de todos os falsos negativos (onde ações fraudulentas não são detectadas), bem como a classificação equivocada de falsos positivos (ações legítimas caracterizadas, erroneamente, como fraudulentas). Desta forma, novas abordagens são necessárias para a continuidade do tema.

Idealmente, o custo para detectar uma fraude deve ser menor do que o gasto gerado por ela. Para ilustrar, uma empresa fictícia que contem um milhão de dados em um arquivo pode possuir 1% de falsos alarmes. Esta quantia representará para a equipe responsável em avaliar fraudes cerca de 10.000 avisos. Alocar funcionários para verificar estas informações terá um custo considerável para a empresa. É importante ressaltar que a maioria dos estudos indicou que a verificação final se algum dado representa ou não uma fraude é uma tarefa recomendada para um ser humano, que pode ser auxiliado por uma ferramenta computacional, como um algoritmo.

Embora cartões de crédito e sistemas de telecomunicações tenham sido criados há décadas, ainda estão em crescimento de utilização, resultando no aumento de possíveis fraudes e valores podendo gerar prejuízos Abdallah et al [2016]. No início dos anos 2000, as palavra chave *fraud detection* já contava com mais de 80 patentes registradas Bolton et al [2002].

Acrescentando à motivação e justificativa, em trabalhos futuros após este artigo, pretende-se estudar e desenvolver (ou utilizar) uma ferramenta ou técnica para rastrear fraudes em setores públicos. Com isto, técnicas de detecção de fraudes seriam aplicadas para descobrir problemas em dados de auditoria e controle em órgãos públicos.

A seguir será descrito o referencial teórico que situará genericamente o assunto abordado. Na sequência, a metodologia utilizada para realizar esta revisão sistemática será apresentada e discutida. Por fim, os trabalhos encontrados serão elencados, analisados e discutidos para o fechamento desta revisão sistemática.

2 Referencial Teórico

A área de detecção de fraudes obteve início em pesquisas nas áreas da estatística e da matemática. No âmbito computacional, Fawcett and Provost [1997] realizaram uma das primeiras e principais abordagens encontradas na literatura. Em seus estudos, analisaram e criaram um sistema para detecção de fraudes em sistemas de telecomunicação. Em seus estudos, constaram que indivíduos fraudadores estão constantemente mudando suas táticas para burlar sistemas, que devem adaptáveis às novas situações.

Posteriormente, utilizando dados reais fornecidos por companhias bancárias, Chan et al [1999] realizaram um trabalho em detecção de fraude em cartões de crédito e obtiveram um aumento nos seus resultados em comparação com técnicas de detecções de fraudes utilizadas anteriormente. Em suas constatações, indicaram que os métodos mais potentes para detectar fraudes são utilizados em cartões de crédito, porém as organizações não costumam revelar suas tecnologias de forma aberta, pois possíveis fraudadores podem se aproveitar do conhecimento e utilizar sistemas com má fé.

Segundo Fawcett and Provost [1997], há muitas técnicas para detecção de fraudes. As mais difundidas e utilizadas são as que produzem detecções por meio de regras pré estabelecidas e as que realizam a comparação entre valores de dados. Estas classificações geraram duas ramificações iniciais em pesquisas da área.

Uma das ramificações, a detecção de fraude por meio de regras, determina que uma fraude será detectada devido ao conhecimento que a equipe adquiriu observando fraudes recorrentes em outrora. A vantagem nesta técnica está em preditar como a fraude ocorre. A desvantagem está na possibilidade de descobrir somente fraudes já conhecidas.

O outro ramo na detecção de fraudes ocorre por meio de cálculos e comparação de valores. Como principal exemplo, um desvio no padrão comporta-

mental de alguma variável pode ser identificado comparando seus dados com dados anteriores ou de outras variáveis similares. Sua principal vantagem é a utilização de algoritmos já conhecidos na literatura [Fawcett and Provost, 1997]. O problema apresentado pela técnica é a possibilidade do indivíduo fraudador conhecer e inserir dados fraudulentos de maneira em que o sistema não consiga o identificar como um usuário malicioso.

Provost, ao comentar sobre o trabalho de Bolton et al [2002], indica que é importante não visualizar a detecção de fraudes somente como uma área, mas desmembrá-la em sub-áreas para promover a interdisciplinariedade. Com isto, constata-se que a detecção de fraudes não possui uma técnica universal, pois ela contem diversas abordagens.

3 Metodologia

Ao primeiro momento do trabalho de revisão sistemática, o planejamento da estratégia de pesquisa norteia a pesquisa em publicações na área abordada.

A revisão da literatura foi baseada no trabalho apresentado por Kitchenham and Charters [2007], onde os elementos de pesquisa são definidos para realizar e relatar a revisão.

Foram selecionadas as bibliotecas digitais abaixo para realizar a pesquisa. O motivo da escolha foi a grande quantidade de material publicado com relevância científica.

- ACM Digital Library[1]
- IEEE Xplore Digital Library[2]
- ScienceDirect[3]
- SpringerLink[4]

A tarefa para selecionar os artigos pode ser visualizada no diagrama da Figura 1, onde as etapas foram divididas em início, desenvolvimento e conclusão. Na parte inicial, o tema é definido e publicações naquele tema são pesquisadas. Posteriormente, se após a busca por artigos a base de referências não estiver sólida para um bom estudo, a etapa de busca é refeita até obter uma boa base do Estado da Arte na área. Por fim, os artigos selecionados são estudados.

Como critérios de seleção e ordenação para a pesquisa, a revisão escolheu os artigos com maior número de citações e relevância para a área.

O principal critério de seleção foi a proximidade com o tema destacado na introdução deste trabalho, onde a detecção de fraudes deveria ser a principal abordagem do artigo encontrado.

Realizando uma exceção, os principais artigos que tratam do tema de detecção de fraudes foram inclusos no estudo para serem utilizados, principal-

[1] http://dl.acm.org/
[2] http://ieeexplore.ieee.org/
[3] http://www.sciencedirect.com/
[4] http://link.springer.com/

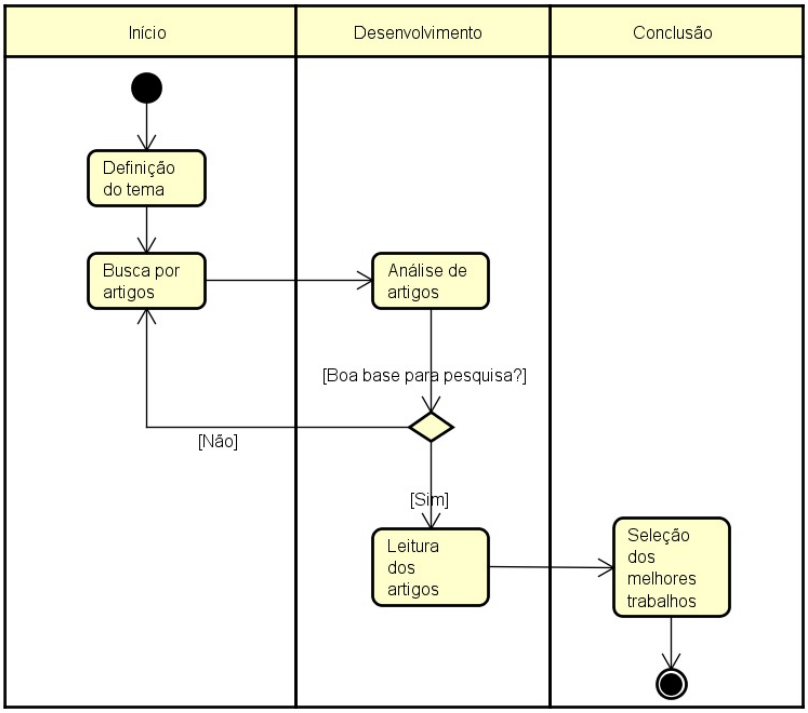

Figura 1 Diagrama de sequência indicando as etapas de seleção de artigos para a pesquisa.

mente, na seção do referencial teórico, pois eram encontrados como referência na maioria dos trabalhos atuais.

Foram excluídos da revisão os artigos que fugiam do tema proposto, não possuíam citações ou relevância nas bases de dados ou eram anteriores ao ano de 2006. Os critérios de exclusão estão elencados abaixo. Foram excluídos da seleção os artigos contendo assuntos relacionados a detecção de fraudes em:

- Imagens, vídeos ou impressões físicas;
- Contextos biológicos, como análises de DNA e moléculas;
- Componentes eletrônicos;
- Dispositivos de segurança eletrônica relacionados a vírus, *firewalls* e *cyber* ataques.

Para esta revisão sistemática, obteve-se foco em detecção de fraudes em dados computacionais como números e informações em tabelas, arquivos de texto, planilhas eletrônicas, etc. Isso justifica a exclusão de artigos tratando de áreas como processamento de imagens, biologia, eletrônica e segurança de redes de computadores.

Para a busca de publicações, foram considerados somente trabalhos que realizaram uma revisão no Estado da Arte em detecção de fraude, na língua inglesa e publicados no período entre 2006 e 2016. As palavras chave *fraud detection survey* foram utilizadas para a busca, que obteve artigos selecionados

Tabela 1 Please write your table caption here

first	second	third
number	number	number
number	number	number

com a leitura na respectiva ordem: título, resumo e artigo completo. Foram considerados somente trabalhos em que nenhum novo método era apresentado ou testado. Portanto, somente revisões sistemáticas na literatura da área foram inclusas.

Na primeira fase da pesquisa, foi considerada a utilização da combinação das palavras chave a seguir, que foram eliminadas da metodologia:

- *fraud detection AND state of art OR systematic review OR meta analysis*;
- *anomaly detection AND survey OR state of art OR systematic review OR meta analysis*;
- *outlier detection AND survey OR state of art OR systematic review OR meta analysis*;
- *deception detection AND survey OR state of art OR systematic review OR meta analysis.*

Os resultados contendo os temas *anomaly, outlier* e *deception detection* juntamente com *survey* retornaram trabalhos duplicados a pesquisa com as palavras chave *fraud detection survey* ou fora do escopo da pesquisa, onde a grande parte foram eliminados da seleção através dos métodos de exclusão citados anteriormente. Por esta razão, as palavras chave não foram consideradas para a pesquisa de artigos.

Outras palavras que podem significar revisões sistemáticas na língua inglesa são *state of art, systematic review* ou *meta analysis*. Contudo, a utilização dessas palavras chave também se mostrou obsoleta em comparação à palavra *survey*, pois trouxeram muitos resultados duplicados ou em áreas indesejadas para esta revisão sistemática, como processamento de imagens, biologia, eletrônica e segurança de redes de computadores.

No início da revisão sistemática, foram encontrados 101 artigos com potencial para estruturar este trabalho. Destes, dois não estavam disponíveis para consulta. Após a leitura do título dos 99 artigos restantes, 49 foram excluídos. Posteriormente, seguindo os critérios de exclusão, foi realizada a leitura do resumo dos artigos. Destes, 22 trabalhos foram selecionados para realizar a revisão sistemática proposta por este trabalho.

4 Estado da Arte

5 Discussão

O principal desafio apontado pela maioria dos autores diz respeito à evolução das técnicas utilizadas pelos fraudadores para burlar os sistemas. Em estudos

realizados por corporações bancárias Bolton et al [2002], o comportamento esperado por fraudadores demonstrou uma mutação quando os criminosos entenderam as técnicas para detectá-los. Indivíduos que em outrora utilizavam cartões de crédito somente para realizar compras com a intenção de não pagá-las, perceberam que poderiam pagar as compras iniciais para serem classificados como usuários comuns, e assim possuir maior margem para fraudar no futuro.

Entendendo o problema da mutação nas técnicas criminosas, constata-se que a engenharia de software tradicional possui um processo de produção padrão, onde ocorre etapas de análise, projeto, codificação, implementação e testes Sommerville [2011]. Dessa maneira, a constante evolução das características de usuários fraudulentos pode se tornar um desafio para englobar um modelo de desenvolvimento tradicional de software.

6 Conclusão

Em trabalhos futuros, almeja-se continuar a pesquisa em detecção de fraudes, aplicando técnicas para auxiliar a auditoria e controle de órgãos públicos a descobrir irregularidades em dados.

Na finalização da revisão sistemática, espera-se a publicação dos resultados obtidos na revista Data Mining and Knowledge Discovery, a qual possui a classificação de qualidade Qualis B1, elencada pela CAPES em sua última análise.

Referências

Abdallah A, Maarof MA, Zainal A (2016) Fraud detection system: A survey. Journal of Network and Computer Applications 68:90–113, DOI 10.1016/j.jnca.2016.04.007

Bolton RJ, Hand DJ, Provost F, Breiman L, Bolton RJ, Hand DJ (2002) Statistical Fraud Detection: A Review. Statistical Science 17(3):235–255, DOI 10.1214/ss/1042727940

Chan PK, Fan W, Prodromidis AL, Stolfo SJ (1999) Distributed data mining in credit card fraud detection. IEEE Intelligent Systems and their Applications 14(6):67–74, DOI 10.1109/5254.809570

Chandola V, Banerjee A, Kumar V (2009) Anomaly Detection: A Survey. ACM Comput Surv 41(3):15:1—-15:58, DOI 10.1145/1541880.1541882, URL http://doi.acm.org/10.1145/1541880.1541882

Fawcett T, Provost F (1997) Adaptive Fraud Detection. Data Mining and Knowledge Discovery 1(3):291–316, DOI 10.1023/A:1009700419189, URL http://dx.doi.org/10.1023/A:1009700419189

Kitchenham B, Charters S (2007) Guidelines for performing Systematic Literature Reviews in Software Engineering

Seyedhossein L, Hashemi MR (2010) Mining information from credit card time series for timelier fraud detection. In: Telecommunications (IST), 2010 5th International Symposium on, pp 619–624, DOI 10.1109/ISTEL.2010.5734099

Sommerville I (2011) Engenharia de Software, 9th edn. Pearson Brasil

Appendices

Conforme visto na Figura 2, o escopo do trabalho foi delimitado pelas tarefas: Definir tema; Definir objetivos, justificativa e motivação; Escolher o local para publicação; Elaborar o método de pesquisa; Revisar a literatura e selecionar trabalhos; Produzir artigo científico; e Publicar o artigo finalizado.

As tarefas foram divididas entre os meses de junho a setembro e receberam a classificação: Concluída ("OK", em verde); Em andamento ("Andam.", em amarelo); e Não iniciada ("Não Inic.", em vermelho).

Mês / Tarefa	Jun	Jul	Ago	Set
Definir tema.	OK			
Definir objetivos, justificativa e motivação.	OK			
Escolher o local para publicação.	Ok			
Elaborar o método de pesquisa.	OK			
Revisar a literatura e selecionar trabalhos.		Andam.	Andam.	
Produzir artigo científico.		Andam.	Andam.	Não Inic.
Publicar artigo finalizado.				Não Inic.

Figura 2 Cronograma do planejamento do projeto.