Previsão de fraudes bancárias por SMS ou voz, a partir da análise de dados de telefones celulares: Uma Revisão Sistemática de Literatura

Prediction of bank frauds by SMS or voice, from cell phone data analysis: A Systematic Literature Review

Osvaldo Fernando Cossa[1]
[1]Departamento de Engenharias,
Universidade de Trás-os-Montes e Alto Douro
Vila Real, Portugal
ofcossa@gmail.com

Nuno Sousa[2]
[2]Departamento de Ciências e Tecnologia,
Universidade Aberta
Lisboa, Portugal
nuno.sousa@uab.pt

Ramiro Gonçalves[1,3,5], José Martins[3,4], Frederico Branco[1,5]
[3]AquaValor – Centro de Valorização e Transferência de Tecnologia da Água,
Chaves, Portugal
[4]Instituto Politécnico de Bragança,
Bragança, Portugal
[5]Instituto de Engenharia de Sistemas e Computadores, Tecnologia e Ciência,
Porto, Portugal
ramiro@utad.pt,
jose.martins@aquavalor.pt,
fbranco@utad.pt

***Resumo* – Nos últimos anos registou-se um crescimento acentuado de fraudes bancárias cometidas por SMS (*Short Messaging System*) e voz. Um dos fatores que contribui para o aumento de casos de fraudes por SMS é o baixo custo de aquisição de grandes volumes de mensagens, a confiabilidade (a mensagem chegará ao destinatário) e o fato de não precisar de Internet para chegar até a vítima. Em relação as fraudes financeiras por voz, estas podem ser usadas para persuadir as vítimas a efetuarem transferências bancárias para as contas dos fraudulentos, com a promessa de receber avultadas somas em prémios. A deteção destes tipos de fraudes não é uma tarefa trivial, pois exige a aplicação de técnicas e métodos apropriados dependendo da sua natureza. Assim, neste artigo é apresentada uma Revisão Sistemática de Literatura (RSL) de 2015 a 2020, com o intuito de analisar o estado da arte sobre fraudes bancárias cometidas por SMS ou voz. A RSL permitiu identificar os tipos mais comuns de fraudes bancárias por SMS ou voz, e as respetivas técnicas de deteção.**

Palavras Chave – Fraudes financeiras por SMS; fraudes no dinheiro móvel; Análise de CDR.

Abstract **— In recent years there has been a marked increase in bank fraud by SMS (Short Messaging System) and voice. One of the factors contributing to increase in cases of SMS fraud is the low cost of acquiring large volumes of messages, the reliability (the message will reach the recipient) and the fact that it does not need the Internet to reach the victim. In relation to financial fraud by voice, these can be used to persuade victims to make bank transfers to fraudulent accounts, with the promise of receiving large sums in prizes. The prevention of these types of fraud is not a trivial task, as it requires the application of appropriate techniques and methods depending on their nature. This article presents a Systematic Literature Review (SLR) from 2015 to 2020, with the aim of analyzing the state of the art on bank frauds committed by SMS or voice. The SLR allowed the identification of the most common types of bank fraud by SMS or voice, and the respective detection techniques.**

Keywords - SMS financial fraud; Mobile Money fraud; CDR Analysis.

I. INTRODUÇÃO

A crescente utilização de tecnologias móveis nos diversos serviços financeiros tem proporcionado novas oportunidades para o sector financeiro. As tecnologias baseadas no telefone celular permitem o rápido acesso aos serviços financeiros a

2021 16th Iberian Conference on Information Systems and Technologies (CISTI)
23 – 26 June 2021, Chaves, Portugal
ISBN: 978-989-54659-1-0

partir de qualquer lugar, desde que se tenha acesso aos serviços de telecomunicações [1].

As facilidades proporcionadas pelos telefones celulares fizeram com que se tornassem numa ferramenta indispensável para a realização de atividades rotineiras do ser humano, como é o caso da realização de transações bancárias. Os telefones celulares permitem o rápido acesso a diversos serviços financeiros tais como: consulta de saldo, transferência de dinheiro, pagamento de serviços, notificações, entre outros [2]. Além disso, os operadores de serviço telefónico móvel armazenam e utilizam informações básicas de seus utilizadores para diversas análises e posterior tomada de decisão [3]. Essas informações incluem o IMEI (*International Mobile Equipment Identifier*), número do cartão SIM, número de célula de quem efetua a chamada, horário de início da chamada, duração da chamada, número de celular dos intervenientes, entre outras informações, e são armazenadas em um ficheiro denominado CDR (*Call Detail Record*), o qual contém todos os detalhes da chamada [4].

A análise de CDR pode prover informações valiosas para a planificação, instalação e localização de serviços básicos para a população, o planeamento do sistema de transporte público e a predição do estado de tráfego automobilístico de uma determinada cidade [5]. A análise de CDR permite também, a identificação e posterior análise de padrões de movimento de indivíduos e comunidades em grande escala [6]. Além disso, a análise de CDR pode ser utilizada para detetar e prevenir fraudes realizadas a partir do telefone celular.

A ocorrência de fraudes sempre foi um "pesadelo" para as instituições financeiras, e a sua mitigação tornou-se prioridade. Nos últimos anos, muitos estudos foram realizados utilizando *machine learning* para investigar novas técnicas de deteção de fraudes e vários algoritmos foram desenvolvidos para bloquear transações fraudulentas [7]. Portanto, o principal desafio do processo de deteção de fraudes é o desenvolvimento de mecanismos eficientes para distinguir transações fraudulentas das honestas [8].

Nesse contexto, no presente estudo faz-se uma Revisão Sistemática de Literatura (RSL) de 2015 a 2020, com o objetivo de investigar o estado da arte sobre a ocorrência de fraudes bancárias por SMS ou voz. Assim, fez-se uma pesquisa em bibliotecas eletrónicas de artigos científicos com o objetivo de efetuar o levantamento de estudos que definam um mecanismo para a realização de um estudo empírico sobre a deteção de fraudes financeiras realizadas a partir do telefone celular e foram excluídos todos estudos que descrevam outros tipos de fraudes.

As principais contribuições deste trabalho são:

- a elicitação dos tipos mais comuns de fraudes bancárias cometidas por SMS ou voz;
- a elicitação de técnicas utilizadas para identificar fraudes bancárias cometidas por SMS, a partir da análise de CDR;

Este artigo está estruturado da seguinte forma: Na Secção 2 faz-se uma breve discussão sobre os estudos relacionados. Na secção 3 descreve-se o processo de condução da revisão sistemática da literatura realizada. Na secção 4 apresenta-se os resultados e a sua respetiva discussão. Na secção 5 apresenta-se as ameaças à validade da RSL. Na secção 6 conclui-se o estudo.

II. Trabalhos Relacionados

No estudo de [25] os autores conduziram uma revisão sistemática de literatura (2008-2017) com o objetivo de analisar o estado da arte das metodologias envolvidas na classificação de *spam* de SMS. A triagem inicial permitiu identificar cerca de 1198 artigos, e após a sua leitura completa, 83 estudos foram considerados relevantes. Uma das métricas analisadas na revisão é o conjunto de métodos ou técnicas usadas para classificar fraudes do tipo *spam* de SMS. Os autores categorizaram as técnicas em: algoritmos de *Machine Learning*, Análises Estatísticas e Algoritmos Evolutivos.

Os métodos de *Machine Learning* são amplamente utilizados na classificação de texto e envolvem o uso de paradigmas de aprendizagem e validação experimental com foco na geração de expressões de classificação, fornecendo assim, uma visão de processos de decisão. Alguns dos métodos mais utilizados desta categoria são: *Support Vector Machine* [23], *Naive Bayes* [21], *Decision Table* [24], *Nearest Neighbour* [22].

Os métodos da categoria de Análises Estatísticas baseiam-se em modelos matemáticos como a aplicação da análise fatorial, uso de probabilidade explicita no seu desenvolvimento e o funcionamento não requer intervenção humana. Algumas das técnicas categorizadas como métodos estatísticos incluem a análise de comportamento [26].

Por fim, a categoria de Algoritmos Evolutivos, os quais são caracterizados pelo uso de técnicas evolutivas ou bioinspiradas, tais como: Sistema Imunológico Artificial (AIS), Algoritmo de Células Dendríticas (DCA), SLAVE, etc. [19].

No estudo de [27] os autores conduziram uma revisão sistemática de literatura (2006-2016) para identificar técnicas de deteção de *spam* de SMS. A triagem realizada em 11 bibliotecas de artigos científicos permitiu identificar 17 estudos relevantes para a pesquisa. Em relação às técnicas de deteção de fraudes de *spam* de SMS, os autores destacaram o fato da maioria dos estudos relevantes utilizarem a abordagem de filtragem baseada no conteúdo para identificar mensagens fraudulentas e para a classificação utilizarem algoritmos de *Machine Learning*, com maior destaque para *Naive Bayes* [21] e *Support Vector Machine* [23].

No estudo de [3] os autores utilizaram dados de telefones celulares para prever a próxima localização e o horário de mudança de localização de subscritores de serviços telefónico móvel. Além disso, a análise de dados de telefones celulares permitiu a [3] prever a próxima ação (chamada, envio de mensagens) de um determinado grupo de subscritores. A análise de CDR tem grande potencial para a resolução de vários problemas do dia-a-dia. A ref.ª [5] aponta para o estudo da mobilidade urbana como uma das suas grandes aplicações. Analisando apenas dados de CDR, é possível extrair padrões de mobilidade humana e consequentemente prever as necessidades do transporte público em uma determinada região. Em [9] dados anonimizados de CDR foram utilizados para determinar o tempo de viagem de veículos em vias públicas e identificar obstruções de ruas em tempo real. Em [10] a mobilidade urbana foi estudada e otimizou-se o transporte público utilizando dados telefónicos.

ISBN: 978-989-54659-1-0

III. MÉTODO DE INVESTIGAÇÃO

A Revisão Sistemática de Literatura (RSL) foi escolhida como método de pesquisa porque esta tenta reunir todas as evidências empíricas que se enquadram nos critérios de elegibilidade pré-especificados para responder a um determinado problema. A RSL utiliza métodos específicos e sistemáticos que são selecionados com o objetivo de minimizar o preconceito, fornecendo resultados mais confiáveis a partir dos quais se podem tirar conclusões e tomar decisões [12].

[13] apontam 3 razões para a realização de uma RSL: Primeiro, para agregar e sintetizar o conhecimento existente sobre um determinado tópico de pesquisa; Segundo, para identificar lacunas de pesquisas anteriores e; Terceiro, para fornecer informações básicas para começar a investigar um novo tópico de pesquisa. Assim, nas subseções subsequentes, apresenta-se as etapas seguidas para a realização da presente RSL, seguindo as diretrizes de [13].

A. Formulação das questões de investigação

Para a formulação das questões de investigação teve-se como base 4 elementos, conhecidos como PICO (População, Intervenção, Comparação e Resultados) conforme as recomendações de [12]. A Tabela 1 ilustra a População, Intervenção, Comparação e Resultados do presente estudo.

TABELA 1. RESUMO DO PICO

População	Estudos relacionados à elicitação e deteção de fraudes bancárias por SMS ou voz. Devem ser considerados estudos publicados entre os anos 2015 e 2020, por forma a garantir o levantamento de estudos atuais.
Intervenção	Estudar características de fraudes bancárias cometidas por SMS ou voz; Estudar técnicas de deteção de fraudes cometidas por SMS ou voz.
Comparação	Estudos que comparem técnicas de deteção de fraudes.
Resultados	Estudos que citem previsões, tipos e padrões de fraudes bancárias realizadas a partir do telefone celular;

Com recurso aos 4 elementos especificados por [12] formulou-se as seguintes questões de investigação:

Questão 1 - Quais os tipos mais comuns de fraudes bancárias cometidas por SMS ou voz?

Questão 2 – Como identificar fraudes bancárias cometidas por SMS ou voz?

B. Identificação da Literatura Relevante

Com base nas recomendações de [13], a identificação de estudos relevantes pode ser feita a partir da realização de uma pesquisa em bibliotecas eletrónicas, precedida por uma pesquisa complementar baseada em citações ou a partir de uma pesquisa manual.

1) Busca em bibliotecas electrónicas

Para formular os termos de pesquisa foram extraídas palavras-chave derivadas da análise PICO (com sinónimos e palavras alternativas). Assim, a *string* de pesquisa completa derivada é:

((Title: (Mobile Money fraud) OR Title: (SMS Financial Fraud*) OR Title: (CDR Analysis*)) AND Publication Date: (01/01/2015 TO 09/30/2021))*

Com recurso à *string* definida, fez-se uma pesquisa em 4 bibliotecas eletrónicas que consistem em artigos da área de ciência da computação e engenharia de software: ACM, IEEE Explore, Springer e ScienceDirect.

2) Pesquisa complementar baseada em citações

Este processo consistiu na consulta dos estudos citados nos artigos selecionados na pesquisa eletrónica. A pesquisa por estes estudos foi realizada na biblioteca Google Scholar.

C. Seleção de estudos

Visto que as pesquisas iniciais podem trazer grandes quantidades de artigos, definiu-se critérios de inclusão e exclusão, conforme seguem.

1) Critérios de Inclusão

- Estudos que definam um mecanismo para a realização de um estudo empírico sobre a identificação e prevenção de fraudes bancárias cometidas por SMS ou voz;
- estudos que elicitem os tipos mais comuns de fraudes bancárias cometidas por SMS ou voz;
- estudos que proponham métodos de deteção de fraudes cometidas por SMS ou voz;
- estudos que proponham técnicas de análise de dados de CDR;
- estudos publicados em inglês.

2) Critérios de Exclusão

- Estudos relacionados a fraudes bancárias que não sejam cometidas por SMS ou voz;
- estudos que tenham sido publicados antes do ano 2015;
- estudos incompletos;
- estudos que não contenham as palavras-chave no título;
- no caso de estudos duplicados (publicados mais de uma vez), será considerado o mais atual e completo;
- estudos que não estejam disponíveis na Internet;
- estudos irrelevantes para a pesquisa, ou seja, aqueles que não definem mecanismo algum para guiar um estudo empírico;
- estudos que não respondam satisfatoriamente às questões de pesquisa;

IV. RESULTADOS

A. Pesquisa em bibliotecas eletrónicas

A pesquisa eletrónica de estudos foi efetuada em 3 etapas, sendo a primeira, a aplicação da *string* de pesquisa nas bibliotecas eletrónicas: ACM, IEE Explore, Springer e ScienceDirect. Esta procura retornou 1001 artigos conforme apresenta a Tabela 2.

ISBN: 978-989-54659-1-0

A segunda etapa consistiu na leitura dos *abstracts* dos estudos pré-selecionados na primeira etapa, o que permitiu apurar 56 estudos para a etapa seguinte.

TABELA 2. PESQUISA ELETRÓNICA DE ARTIGOS

Biblioteca	*string* de pesquisa	Leitura do *abstract*	Leitura completa
ACM	320	26	6
IEE Explore	30	21	6
Springer	373	5	3
ScienceDirect	278	4	2
Total	**1.001**	**56**	**17**

A terceira e última etapa consistiu na leitura completa dos artigos e aplicação dos restantes critérios de inclusão e exclusão, o que culminou com a identificação de 17 artigos relevantes resultantes da busca eletrónica.

B. Pesquisa complementar baseada em citações

A aplicação desta técnica permitiu identificar 3 estudos relevantes (extraídos da Google Scholar).

Assim, a condução da presente revisão sistemática de literatura permitiu identificar 20 estudos relevantes para o estudo, sendo 17 resultantes da pesquisa eletrónica e 3 da pesquisa baseada em citações.

V. DISCUSSÃO

Nesta seção apresenta-se as respostas para as questões de investigação definidas na seção III.

Questão 1 - Quais os tipos mais comuns de fraudes bancárias cometidas por SMS ou voz?

Para responder a esta questão, fez-se uma leitura completa dos estudos selecionados, e deles extraiu-se os tipos mais comuns de fraudes bancárias cometidas por SMS ou voz. O primeiro tipo de fraude identificado é o *spam* de SMS, que consiste no envio de várias mensagens comerciais para vários números de uma só vez [14]. Embora o *spam* por SMS não seja tão comum quanto o *spam* por e-mail [17], nos últimos anos tem vindo a aumentar devido à facilidade de envio de mensagens para vários subscritores de uma só vez. Além disso, [16] alerta para a existência de outros fatores que contribuem para o crescimento de *spam* de SMS, como a inexistência de filtros bem implementados nos operadores de telecomunicações e nos aplicativos de SMS; o serviço de SMS não depende da conexão à Internet, o que garante que o *spam* chegue ao telemóvel do subscritor com maior facilidade e; a disponibilidade de pacotes baratos de SMS para envio em massa.

De acordo com [16], os diversos fatores associados ao rápido crescimento das fraudes de *spam* de SMS, obrigaram a Autoridade de Serviços Financeiros da Indonésia a lançar plataformas de denúncias de fraudes, por forma a identificar e responsabilizar os praticantes destes tipos de crimes. Os resultados desta ação não tardaram a chegar, tendo sido registadas cerca de 14000 denúncias de SMS de fraudes financeiras, em menos de um mês, após o lançamento de serviços de denúncia.

O *spam* pode ser também, de chamadas telefónicas, e consiste na distribuição de chamadas automatizadas em massa, vulgarmente conhecidas por chamadas de robô [14]. Ao efetuar essas chamadas, os infratores procuram convencer as suas vítimas a efetuar transferências bancárias em seu benefício, ou a facultarem dados de suas contas bancárias. Neste tipo de fraude, os fraudadores invadem sistemas telefónicos e manipulam-nos para produzir chamadas telefónicas de elevado valor às custas do operador ou do subscritor [28], causando grandes prejuízos financeiros às suas vítimas.

TABELA 3. TIPOS DE FRAUDES

Tipo de Fraude	Características
spam telefónico de SMS	Várias mensagens comerciais para vários números de uma só vez.
spam telefónico de chamadas	Várias chamadas realizadas em massa num curto período de tempo (segundos).
phishing	Mensagem comercial contendo *link* malicioso, na qual o invasor solicita o subscritor para visitar uma determinada página.
fraude de loteria	Mensagens enviadas a partir de um número diferente do curto; Contém palavras de congratulação; Contém palavras de recebimento de algum prémio.
fraude de recibo	Mensagens enviadas a partir de um número diferente do curto; Contém palavras de confirmação de transferências de dinheiro;

No estudo realizado por [11], os autores propuseram um método para investigar fraudes realizadas a partir do telefone celular, através do envio de SMS. Como metodologia, foi coletado um número significante de SMS fraudulentas por meio de um aplicativo Android desenvolvido para o efeito. Além disso, foram entrevistadas pessoas expostas as fraudes de SMS e representantes de operadores de redes móveis no Paquistão. De seguida analisou-se o conteúdo das mensagens coletadas e apurou-se 2 tipos de fraudes bastante comuns em países em via de desenvolvimento: fraude de loteria e fraude de recibo.

A fraude de loteria consiste no envio de uma mensagem informando ao destinatário que ele ganhou algum dinheiro, e que deve entrar em contacto com um determinado número para recebê-lo. Assim, a vítima liga de volta e o fraudador convence a vítima para que esta pague uma taxa para obter o prêmio em

ISBN: 978-989-54659-1-0

dinheiro. O pagamento é feito por algum mecanismo, mas o prêmio em dinheiro nunca é entregue [11].

A fraude de recibo consiste no envio de um recibo falso por SMS em nome de um determinado subscritor, em alguns casos, com o nome e endereço da vítima no conteúdo da mensagem. De seguida, o fraudador liga para o subscritor para pedir o "seu" dinheiro de volta, informando que foi acidentalmente enviado para a carteira móvel do subscritor. Este tipo de fraude, é um ataque direto aos indivíduos, ao contrário da fraude de loteria, que depende do envio de um grande número de mensagens para coletar respostas [11].

Outro tipo de fraude que pode ser cometida por SMS é o *phishing*. Esta fraude consiste no envio de um *link* malicioso por SMS no qual o invasor pede à vítima para visitar uma determinada página por forma a roubar informações confidenciais do dispositivo móvel da vítima [18]. Estas informações podem conter dados bancários e senhas do subscritor.

A Tabela 3 apresenta os diferentes tipos de fraudes identificados nos estudos analisados e as respetivas características.

Questão 2 – Como identificar fraudes bancárias cometidas por SMS ou voz?

O rápido crescimento deste tipo de fraudes demanda o desenvolvimento de novas técnicas para a sua deteção. Em [18], os autores propuseram uma técnica de filtragem de *spam* de SMS utilizando cinco algoritmos de *Machine Learning,* conforme apresenta a Tabela 4. Para classificar as mensagens em *spam*, os autores propuseram a análise de 10 características no texto, descritas em [18]: presença de símbolos matemáticos, presença de URLs, presença de pontos, presença de símbolos especiais, presença de emoções, palavras minúsculas, palavras maiúsculas, presença de número de telefone, palavras-chave específicas e comprimento do texto. Para testar o modelo proposto, utilizou-se cerca de 2608 mensagens de *spam*, das quais 2408 foram extraídas da base de dados pública de SMS de *spam,* disponível em [20] e as restantes 200 recolhidas manualmente de subscritores que tenham sido vítimas deste tipo de fraude. Para apurar a precisão da técnica, o conjunto de dados extraído foi testado na ferramenta WEKA utilizando os 5 algoritmos de *Machine Learning* descritos na Tabela 4.

TABELA 4. ALGORITMOS DE DETEÇÃO DE FRAUDE DE SMS

Algoritmo	descrição
Naive Bayes	Este algoritmo é baseado no teorema de Bayes [21]. Em Naive Bayes, as suposições entre os preditores são independentes.
Logistic Regression	A regressão logística é um algoritmo de aprendizagem de máquina, no qual a variável dependente é categórica e mede a sua relação com a varável independente usando a função logística
J48	Usa dados de treinamento de amostras já classificadas. Este algoritmo basicamente constrói uma árvore de decisão, onde cada característica é representada pelo nó.
Decision Table	A tabela de decisão é um algoritmo de aprendizado de máquina que se baseia na divisão de dados em grupos homogéneos. Pode ser utilizada em cenários de classificação ou regressão.
Random Forest	O algoritmo de floresta aleatória é o ideal para um grande número de dados. Basicamente, ele constrói um conjunto de árvores de decisão na fase de treinamento, e em seguida, cada árvore cada árvore opera em atributos escolhidos aleatoriamente.

Após comparar os resultados alcançados pelos 5 algoritmos, o *Random Forest* apresentou os melhores resultados de classificação com alta precisão, com cerca de 96.5% de taxa de verdadeiro positivo e 1,02% de falso positivo, contra 96% de verdadeiro positivo e 1,33% de falso positivo, do algoritmo *Decision Table,* segundo melhor classificado. O algoritmo de classificação *Random Forest* foi também usado em [17], onde apresentou melhores resultados (98% de precisão) após ser comparado com outros 4 algoritmos de classificação (*Naive Bayes* [21], *K-Nearest Neighbor* [22], *Support Vector Machine* [23], *Decision Table* [24]).

Para identificar fraudes de loteria e de recibo, [11] analisaram um conjunto de mensagens fraudulentas coletadas a partir de um aplicativo Android e de questionários feitos a subscritores que já tenham sido vítimas deste tipo de fraudes. Para classificar as mensagens em fraudes de loteria ou recibo, os autores identificaram os seguintes padrões: Mensagens fraudulentas nunca são enviadas a partir de um número curto; Mensagens fraudulentas contém palavras de congratulação (*Congratulations, Mubarak*, etc.); Mensagens fraudulentas contém palavras de recebimento de algum prémio (*won, awarded, nikla*, *dólar*, etc.).

De seguida, [11] exploraram várias heurísticas com base nos padrões identificados, sendo a *fx NxORMxANDCxORRxORLx,* a que se mostrou mais eficaz (99,2% de eficácia) para detetar fraudes, onde N, M, C, R e L, são funções que retornam verdadeiro, se o número de telefone, moeda, palavras de congratulação, palavras de recebimento ou palavras relacionadas ao sorteio estiverem presentes.

[28] propuseram a utilização de algoritmos de *Machine Learning* não supervisionado para a deteção de fraudes de spam de chamadas com recurso à análise de CDR. Os autores começaram por definir algumas variáveis de análise: o número de quem efetua a chamada, o número do destinatário, a duração da chamada, o custo da chamada e a cidade de destino, num universo de 11418 milhões de chamadas efetuadas entre 01 a 31 de maio de 2018. Após a extração de dados, os autores aplicaram os algoritmos de K-Means [29] e DBSCAN (Density-Based Spatial Clustering of Applications with Noise) [30] para avaliar os resultados do aprendizado, por forma a determinar a sua precisão. Nos resultados apresentados, os autores apontaram para o algoritmo K-Means como sendo aquele que alcançou o

ISBN: 978-989-54659-1-0

melhor valor de precisão, recomendando-o como sendo ideal para detetar fraudes em CDR.

VI. Ameaças à validade

De acordo com [15], durante o processo de desenvolvimento de qualquer tipo de estudo, por mais cuidado que se tenha, a possibilidade de existência de ameaças à sua validade não pode ser descartada, e é da responsabilidade do investigador identificá-las e definir ações de controle para mitigá-las.

Neste estudo, a primeira grande limitação pode ser encontrada na construção da *string* de pesquisa, devido à existência de muito material sobre fraudes bancárias na Internet, e na sua maioria irrelevante para o presente estudo. Então, construir uma *string* de pesquisa que retornasse apenas os artigos relevantes para a esta, tornou-se um desafio e fez com que no processo de seleção preliminar, se optasse por procurar artigos que tivessem as palavras-chave no título, ignorando a sua ocorrência no *abstract* e introdução. De certa forma, essa validação pode ter feito com que alguns artigos relevantes para a pesquisa não fossem retornados, comprometendo desse jeito os resultados do estudo.

A segunda ameaça à validade do estudo, é o fato das pesquisas terem sido realizadas em inglês, o que pode ter contribuído para a exclusão de estudos escritos em outros idiomas e potencialmente relevantes para a presente investigação.

Outra importante ameaça à validade do estudo, é o fato de terem sido procurados e analisados artigos num curto espaço temporal (i.e., 2015 a 2020), pois, podem existir estudos mais antigos que possivelmente contenham informação útil para o presente trabalho. Além disso, constitui ameaça à validade do estudo, o facto de terem sido consultadas apenas 4 bibliotecas eletrónicas.

Diante disso, buscou-se minimizar qualquer ameaça à validade do estudo, sobretudo no processo de seleção e extração.

VII. Conclusões

Neste estudo realizou-se uma RSL com o objetivo de analisar o estado da arte sobre fraudes bancárias realizadas por SMS e voz para o telefone celular da vítima. O processo de seleção de estudos permitiu identificar 20 artigos relevantes para o tema da pesquisa. O método de pesquisa consistiu na definição de uma *string* de investigação e realizaram-se pesquisas em bibliotecas eletrónicas de artigos científicos de referência. Além disso, realizou-se uma busca complementar baseada em citações no Google Scholar.

A análise dos estudos considerados relevantes permitiu identificar alguns dos principais tipos de fraudes bancárias por SMS e voz, e as respetivas técnicas de deteção. Constatou-se que um dos principais tipos de fraudes de SMS é o *spam* e a sua deteção pode ser feita por meio de métodos de filtragem de mensagens e da aplicação de algoritmos de classificação de *Machine Learning*. Outra importante constatação é que as fraudes bancárias por SMS ou voz, nunca são realizadas a partir de números curtos, e geralmente contém palavras de congratulação, recebimento de um prémio ou confirmação de recebimento de montantes. Além disso, os praticantes de fraudes enviam várias mensagens fraudulentas para vários números de uma só vez.

A análise dos detalhes das chamadas (CDR) e SMS fraudulentas, a mineração de dados, aliadas à utilização de técnicas de *Machine Learning* revelaram-se uma mais-valia para a deteção e previsão de fraudes por SMS e voz.

Os resultados preliminares desta RSL evidenciaram a existência de muitos estudos que abordam tópicos relacionados à deteção de fraudes bancárias do tipo *spam de* SMS por meio de algoritmos de filtragem e mineração de texto, porém, muito poucos voltados à deteção através da análise de CDR, o que abre espaço para futuros investigadores aprofundarem o tema.

Agradecimentos

Este trabalho é financiado por Fundos Nacionais através da agência de financiamento portuguesa FCT - Fundação para a Ciência e Tecnologia no âmbito do projeto UIDB / 50014/2020.

Referências Bibliográfica

[1] G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955.

[2] Demos, T. (2016). For the first time, more are mobile-banking than going to a branch. *WSJ, Jan*, *12*.

[3] Ozer, M., Keles, I., Toroslu, I. H., Karagoz, P., & Ergut, S. (2014). Predicting the next location change and time of change for mobile phone users. In *proceedings of the third ACM SIGSPATIAL international workshop on mobile geographic information systems* (pp. 51-59).

[4] Maji, G., & Sen, S. (2015). A Data warehouse based analysis on CDR to depict market share of different mobile brands. In *2015 Annual IEEE India Conference (INDICON)* (pp. 1-6). IEEE.

[5] Hadachi, A., Batrashev, O., Lind, A., Singer, G., & Vainikko, E. (2014). Cell phone subscribers mobility prediction using enhanced Markov Chain algorithm. In *2014 IEEE Intelligent Vehicles Symposium Proceedings* (pp. 1049-1054). IEEE.

[6] Xu, F., Tu, Z., Li, Y., Zhang, P., Fu, X., & Jin, D. (2017). Trajectory recovery from ash: User privacy is not preserved in aggregated mobility data. In *Proceedings of the 26th international conference on world wide web* (pp. 1241-1250).

[7] Tae, C., & Hung, P. (2019). Comparing ML algorithms on financial fraud detection. In *Proceedings of the 2019 2nd International Conference on Data Science and Information Technology* (pp. 25-29).

[8] Ryman-Tubb, N., Krause, P., & 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*, 130-157.

[9] Janecek, A., Valerio, D., Hummel, K. A., Ricciato, F., & Hlavacs, H. (2015). The cellular network as a sensor: From mobile phone data to real-time road traffic monitoring. *IEEE transactions on intelligent transportation systems*, *16*(5), 2551-2572.

[10] Berlingerio, M., Calabrese, F., Di Lorenzo, G., Nair, R., Pinelli, F., & Sbodio, M. L. (2014). *AllAboard: a system for exploring urban mobility and optimizing public transport using cellphone data* (No. 14-3918).

[11] Pervaiz, F., Nawaz, R. S., Ramzan, M., Usmani, M. Z., Mare, S., Heimerl, K., & Razaq, L. (2019). An assessment of SMS fraud in Pakistan. In *Proceedings of the 2nd ACM SIGCAS Conference on Computing and Sustainable Societies* (pp. 195-205).

[12] Donato, H., & Donato, M. (2019). Etapas na Condução de uma Revisão Sistemática. *Acta Médica Portuguesa*, *32*(3).

[13] Kitchenham, B., & Charters, S. (2007). Guidelines for performing systematic literature reviews in software engineering EBSE Technical Report EBSE-2007-01. *Keele, Staffs, and Durham, UK*.

ISBN: 978-989-54659-1-0

[14] Tu, H., Doupé, A., Zhao, Z., & Ahn, G. J. (2016). Sok: Everyone hates robocalls: A survey of techniques against telephone spam. In *2016 IEEE Symposium on Security and Privacy (SP)* (pp. 320-338). IEEE.

[15] Maldonado, J., Carver, J., Shull, F., Fabbri, S., Dória, E., Martimiano, L., Mendonça, M. and Basili. (2006). Perspective-based reading: a replicated experiment focused on individual reviewer effectiveness. *Empirical Software Engineering*, v.11, p. 119–142

[16] Dewi, F. K., Fadhlurrahman, M. M. R., Rahmanianto, M. D., & Mahendra, R. (2017). Multiclass sms message categorization: Beyond spam binary classification. In *2017 International Conference on Advanced Computer Science and Information Systems (ICACSIS)* (pp. 210-215). IEEE.

[17] Sjarif, N. N. A., Azmi, N. F. M., Chuprat, S., Sarkan, H. M., Yahya, Y., & Sam, S. M. (2019). SMS spam message detection using term frequency-inverse document frequency and random forest algorithm. *Procedia Computer Science*, *161*, 509-515.

[18] Choudhary, N., & Jain, A. K. (2017). Towards filtering of SMS spam messages using machine learning based technique. In *International Conference on Advanced Informatics for Computing Research* (pp. 18-30). Springer, Singapore.

[19] El-Alfy, E.S.M., AlHasan, A.A.: (2016). Spam filtering framework for multimodal mobile communication based on dendritic cell algorithm. Future Gen. Comput. Syst. 64, 98–107. doi:10.1016/j.future.2016.02.018

[20] Brownlee, J (2016). SMS Spam Corpus. http://www.esp.uem.es/jmgomez/smsspamcorpus. Visitado aos 4 de Abril de 2021.

[21] Brownlee, J (2016). Machine Algorithm Algorithms. http://machinelearningmastery.com/naive-bayes-for-machine-learning. Visitado aos 3 de Abril de 2021.

[22] Harisson, O. (2018). Machine Learning Basics with the K-Nearest Neighbors Algorithm. https://towardsdatascience.com/machine-learning-basics-with-the-k-nearest-neighbors-algorithm-6a6e71d0176. Visitado aos 3 de Abril de 2021.

[23] Gandhi, R. (2018). Support Vector Machine - Introduction to Machine Learning Algorithms. https://towardsdatascience.com/support-vector-machine-introduction-to-machine-learning-algorithms-934a444fca47. Visitado aos 2 de Abril de 2021.

[24] Witt, G. (2012). https://www.sciencedirect.com/topics/computer-science/decision-table. Visitado aos 2 de Abril de 2021.

[25] Abayomi-Alli, O., Misra, S., Abayomi-Alli, A., & Odusami, M. (2019). A review of soft techniques for SMS spam classification: Methods, approaches and applications. *Engineering Applications of Artificial Intelligence*, *86*, 197-212.

[26] Silva, R.M., Almeida T. M, Yamakami, A., (2017). MDLText: An efficient and lightweight text classifier. Knowl.-Based Syst. 118, 152–164.

[27] Lota, L. N., & Hossain, B. M. (2017). A systematic literature review on sms spam detection techniques. *International Journal of Information Technology and Computer Science (IJITCS)*, *9*(7), 42-50.

[28] Jabbar1, M., Suharjito (2020). Fraud Detection Call Detail Record Using Machine Learning in Telecommunications Company. *In Advances in Science, Technology and Engineering Systems Journal* Vol. 5, No. 4, 63-69 .

[29] Garbade, M. (2018). https://towardsdatascience.com/understanding-k-means-clustering-in-machine-learning-6a6e67336aa1. Visitado aos 2 de Abril de 2021.

[30] Yildirim, S. (2020). https://towardsdatascience.com/dbscan-clustering-explained-97556a2ad556. Visitado aos 2 de Abril de 2021.

ISBN: 978-989-54659-1-0

2021 16th Iberian Conference on Information Systems and Technologies (CISTI)
23 – 26 June 2021, Chaves, Portugal
ISBN: 978-989-54659-1-0