IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 16 May 2022, accepted 30 July 2022, date of publication 8 August 2022, date of current version 11 August 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3197225

RESEARCH ARTICLE

Online Recruitment Fraud Detection: A Study on Contextual Features in Australian Job Industries

SYED MAHBUB, ERIC PARDEDE, (Senior Member, IEEE), AND A. S. M. KAYES, (Member, IEEE)

Department of Computer Science and Information Technology, La Trobe University, Bundoora, VIC 3086, Australia

Corresponding author: A. S. M. Kayes (a.kayes@latrobe.edu.au)

ABSTRACT The purpose of this study is to investigate the effects of contextual features on automatic detection accuracy of online recruitment frauds in Australian job market. In addition, the study aims to unearth the significance of localisation of such approaches. The study first generates a dataset based on a local and semi-structured advertising platform in Australia. The labelled dataset is then used to train a learning model on several content-based and contextual features. The existence of advertising body in relevant government and non-government registries in Australia, along with the internet presence of the advertiser, were considered as contextual features. The extraction process of such contextual features was automated as well. The study concludes that the inclusion of contextual features improves the performance measures of the automated online recruitment fraud detection model. The practical implication of the study is two-folds. Firstly, the contextual feature space generation engine can be used with any dataset, with minimal localisation efforts. Secondly, such learning models can be used at the back end of online job recruitment portals to detect and prevent online recruitment frauds. The study not only demonstrates the positive impact of using contextual features in fraud detection using a real-life dataset, but it also demonstrates how these contextual features can be extracted automatically from the web, based on localised company registries.

INDEX TERMS Online recruitment fraud, fraud detection, employment scam, contextual features.

I. INTRODUCTION

Apart from a very few industries who rely on headhunting agencies for actively seeking out workers on their behalf, majority of the industries in Australia, and around the world for that matter, rely on online job portals for recruitment of employees. With the increasing popularity and convenience of online job portals, it is critical at this stage to address the fraudulent activities, which these portals are susceptible to. Online Recruitment Fraud (ORF) is a fraudulent activity, where job seekers are lured into applying for fake jobs to get them to reveal sensitive information about themselves. The implications can be as little as financial loss and as major as identity theft. According to the ongoing report from the Scamwatch team of Australian Competition and Consumer Commission (ACCC), there have been 174 reported cases of employment scams across Australia during the month of February 2022, alone. Among 174 reported cases, 16.1% incurred financial loss and the total amount adds up to 142,762 Australian Dollars [1].

Given the reduced employment activities across the world because of COVID-19, on the hindsight, the number of reported cases was less compared to the number of cases just three years ago. During the month of February 2019, the total number of reported cases was 240. Among the reported cases, only 17.2% incurred financial loss, which was equivalent to 101,588 Australian Dollars [1]. Other losses include identity theft, phishing, data harvesting, and so on, and the implications of such activities are more severe than financial loss since, compromised personal information may bring upon legal and criminal liabilities on otherwise innocent people.

One of the main platforms for these fraudsters are online recruitment portals, where a job advertisement can be easily deceived to be authentic, when in fact, is a fake with the sole purpose of scamming desperate job seekers. However, imposing heavy restrictions on these portals is not the answer to the problem since, the portals not only provide a convenient

The associate editor coordinating the review of this manuscript and approving it for publication was Ahmed Farouk.

way to hire people, but also provide an opportune way to apply for jobs for people on a job hunt. The flexibility of creating professional profiles and applying for a position with just a few clicks makes it less cumbersome for applying for a job. The added benefit is the ample time at hand for professional skill development initiatives. Furthermore, given the volume of job circular being published each day around the world and the volume of applications that are being submitted, it is infeasible to manually screen the activities for fraudulent behavior. Under these circumstances, it is imperative to come up with an automatic fraud detection system, which is scalable, practical, and effective.

A. THE CONTRIBUTIONS

In our previous research work [2], we emphasized on the importance of contextual features in determining the legitimacy of the advertising body. In this study, we generate a novel dataset, which is of a local origin. We also propose a detection model, that considers authenticity of a job circular not only based on the features in the circular, but also based on the authenticity of the organization or individual who is responsible for publishing the circular in the first place, by validating their internet footprint. The contributions of this work are briefly summarized as follows:

- We propose a multi-layer framework to detect ORF in Australian job market that decouples the areas of concerns in the detection process.
- We build an engine to generate the contextual features by analyzing the internet footprint of the advertising body in Australian context.
- We demonstrate how the contextual features can be extracted automatically to improve the detection accuracy of ORF.
- We generate a localized dataset from a semi-structured advertising platform in Australia.

B. THE OUTLINE OF PAPER

The rest of the paper is organized as follows. The next section (section II) will lay down the background of ORF detection, including the current state-of-the-art solutions proposed by the related works, and clarify our motivation behind some of the research choices. The subsequent sections (section III, IV, and V) will present our research methodology including the details of the dataset, our research findings, and draw a conclusive discussion including future research directions, respectively.

II. BACKGROUND AND MOTIVATION

The use of contextual features in detection of ORF was first introduced by our previously published conference paper [2] back in 2018. Although the use of contextual feature in ORF is fairly recent, several other domains of fraud detection utilized the concept of contextual features for a while now. In this section, we first introduce some domains of fraud detection that capitalizes on the concept of contextual features for automatic detection of fraudulent online behaviors. We then introduce state-of-the-art solutions that exists in the field of ORF detection. We then present a brief comparative analysis of existing solutions with our work, before outlining our motivation and research questions.

A. RELATED WORK IN OTHER DOMAINS OF FRAUD DETECTION

The generalized area of fraud detection consists of, but not limited to domains, such as phishing, email spam, cyberbullying, Wikipedia vandalism, trolling, opinion fraud, astroturfing, malware attack, cross-site scripting, online predation, financial fraud, identity theft, employment scam and so on. It is outside the scope of this paper to cover previous research works in all of these domains. However, in terms of related approaches, a number of research works focused on including contextual features in the features space design for machine learning models.

The research work by Stringhini, *et al.* [3] designed a feature space based on empirical analysis on social networks traits and trained a Random Forest classifier to detect email spam, whereas Boykin and Roychowdhury [4] focused on extracting features from the message body and message header for training a Bayesian classifier. Yeh, *et al.* [5] on the other hand, focused on meta-heuristics to propose a feature space based on user behavior. More recent work on spam detection [6], [7], [8] focused on hybrid feature selection algorithms. The approach of extraction of binary features from online text was adopted by Dinakar, *et al.* [9] to classify YouTube comments to detect cyberbullying, whereas extraction of numerical features from URLs was proposed by Kumar and Subba [10] for phishing attach detection. Similar research works used NLP techniques such as Term Frequency–Inverse Document Frequency (TF-IDF), lexical analysis, syntactic-semantic analysis, to detect improper behaviors such as phishing, Wikipedia vandalism and cyberbullying [11], [12], [13]. User contexts of online social network (OSN) such as gender information and user activity history were considered by several research works [14], [15], [16], [17], [18], in the domain of cyberbullying and trolling. Group and individual behavioural characteristics, textual, and discrete features were utilized by several research works [19], [20], [21], [22], [23] to identify crowdturfing and induced activities on OSN. However, these approaches of feature space design are not adequate for ORF detection, as the categories of features, included in the feature space, largely depend on specific problem domain. Additionally, the structured nature of online recruitment advertisements begs careful consideration towards feature selection for successful fraud detection. Localised behavioural trends, directions, and user-base can also be considerable factors in the area of ORF.

B. RELATED WORK IN THE ORF DOMAIN

Despite the severity of the threat of ORF, very few research works have been conducted to address the problem. The

problem of ORF was first addressed by Vidros, *et al.* [24], where the authors explained the role of Application Tracking Systems (ATS) in the candidate hiring process. The authors also mentioned the severity of exploitation of such ATSs. Identity theft, financial loss and loss of privacy were some of the main highlights of their motivation. The research work lists some of the challenges of recruitment fraud domain which include lack of adherence to any communication protocol, short and one-time interaction of users with job advertisements and impersonation of fraudsters as an existing business and so on. The output of the research was a generated set of empirical rules by analysing real-world data.

The same research group proposed a more substantial framework [25] including the Employment Scam Aegean Dataset (EMSCAD) dataset [26], which was made public and contains 17,880 real-life job instances. The authors conducted bag-of-word (bow) modelling and empirical analysis on a subset of the EMSCAD dataset. Their empirical analysis on geographical constraints, textual analysis of spam words, analysis of HTML elements and binary analysis provided affective baseline information for ORF detection. The empirical ruleset generated in the first paper [24] was expanded in the second [25] and served as a base for the rule set based binary features. The authors achieved a highest accuracy of 90.56%, recall value of 0.906 and precision value of 0.906 using J48 decision tree classifier of WEKA for their binary analysis of features.

Later, in 2019, the research work by Alghamdi and Alharby [27] utilised the same public dataset and proposed an ensemble classifier to detect ORF instances. The authors performed a feature selection using support vector machine and applied a random forest classifier. The authors demonstrated a 97.4% accuracy in detecting fraudulent instances of job postings in the EMSCAD dataset. However, the research reported a very low recall value for the fraudulent class label, which was not addressed by the authors.

The research conducted by Nindyati and Nugraha [28] proposed an approach of using behavioural context-based features to determine the legitimacy of a job advertisement with the purpose of implementing a Training Need Analysis (TNA) system to create an effective employment solution. The authors extracted data from Google Jobs in Indonesia and used lexical, syntactic, semantic, and contextual features as proposed by some of the previous works [2], [25]. In addition, the authors considered behavioural features such as use of several providers and jobs average posting distance. Their analysis of the localised dataset revealed an accuracy of 90% in detecting fraudulent recruitment posts.

Another research work by Tabassum, *et al.* [29] considered the localisation of data. The authors extracted data from one of the prominent job portals in Bangladesh, i.e., BD Jobs, and used the features presented in EMSCAD dataset as a reference for feature space design. The work also reported several cultural differences in the nature of the data, for example, job advertisements in Bangladesh do not usually report details about the profile of the company, or the precise range of salary. The work by Goyal, *et al.* [30] also used a fact validation dataset generated from Indian job recruitment portal, in addition to EMSCAD dataset. The authors proposed a fact validation model using knowledge graphs. However, the source of the fact-validation dataset was not reported.

The research work by Lal, *et al.* [31] proposed an ensemble classifier to detect ORF. The authors considered three baseline classifiers, i.e., J48 decision tree, Logistic Regression, and random forest and applied ensemble techniques, such as average, majority, and maximum votes on these baseline classifiers to propose ORFDetector Framework. The authors reported an average accuracy of 95.5%. However, the authors set out the motivation based on employment scam incidents in India, but fails to relate how the framework, which was trained based on EMSCAD dataset, will generalise in Indian context.

The work by Mehboob and Malik [32] proposed an extreme gradient boosting method on the same publicly available EMSCAD dataset and demonstrated how the XGBoost algorithm outperformed other machine learning algorithms. The authors performed multi-stage feature reduction to reach the best combination of 13 features, which showed improved detection performance. The authors concluded that ORF can be detected with more accuracy based on the information whether a company who posts the job advertisement is a recruitment firm. However, the authors did not provide sufficient clarity on how the feature was populated in the methodology.

The research work by Li, *et al.* [33] proposed an exploratory method to classify recruitment data that are imbalanced. The authors proposed a LightGBM ORF detection model by using data sampling and ensemble learning techniques, on the EMSCAD dataset. The authors reported improved performance measures of learning model with hybrid data sampling, against the baseline case of unbalanced EMSCAD dataset.

The research work by Nasser, *et al.* [34] proposed an Artificial Neural Network (ANN)-based model, where authors reported several data pre-processing steps using NLP techniques, including cleaning, tokenisation, etc., for the purposes of generating a Bag-of-Word (BOW) model, using count vectorization.

The research conducted by Chiraratanasopha and Chayintr [35] focused more on proposing a set of features that relays more information on the behavior of fraudsters who commit ORF. Their research utilised the EMSCAD dataset and demonstrated that information on the exaggeration and credibility can improve the performance measures of ORF detection models. The authors used several machine learning algorithms including k-nearest neighbour (KNN), support vector machine (SVM), and decision tree (DT) to evaluate their approach and reported an accuracy of 97.64%.

C. COMPARATIVE ANALYSIS AND RESEARCH MOTIVATION

Having discussed the few research works above, it is apparent that the approaches mainly focused on analysing different

textual and structural features on the EMSCAD dataset and applied different machine learning approaches to improve the detection accuracy of ORF. However, none of the work discussed in this section explored identifying the internet footprint of the advertising company, as a contextual feature. In our previous research work [2], we demonstrated the significance of such contextual feature and how they can improve the detection accuracy drastically. As demonstrated in the first sub-section (II-A), the contextual information about participating actors, in detection of difference improper behavior on the web has been considered across multiple domains. For example, several work in cyberbullying detection [14], [15], has considered the contextual features involving the bully, such as, gender information, previous bullying behaviour, etc. In the domain of opinion fraud detection, contextual features of the spammers themselves has been considered in detecting spamming activities in social networks [3], [19], [20]. These studies demonstrates that the actor who is involved in initiating an improper behaviour has context specific features, which can reveal relevant and significantly important information. The idea of using contextual features for ORF detection is somewhat similar. In ORF, the actor in question is the offering organisation who is responsible for the advertised position. Contextual information such as the offering organisations internet footprint, i.e., online existence, can be critical when it comes to identifying the reliability and authenticity of the organisation itself. In Australia, popular recruitment portals also suggest their users to search the internet to reveal information about the organisational background for the offering company before applying for an advertised job [36], [37]. Our previous research [2] introduced the concept of contextual information such as, the presence of company website, the age of company website, existence of company LinkedIn page, etc., and demonstrated that inclusion of such contextual features increases the performance measures of ORF detection models. However, a subset of the contextual features was populated manually due to implementation limitations involving Google APIs. Moreover, our previous research used a subset of the EMSCAD dataset to perform experimentation with, since manual extraction of the contextual features were not feasible for the entire dataset of almost 18,000 job instances. In our current research work, we address this limitation by automating the extraction process of features, specific to localised context.

It is also worthwhile to note that EMSCAD has been the source of data for majority of the relevant research in the domain of ORF, since it is the only publicly available dataset. However, it is mostly specific to American job market, since the source of data for EMSCAD is Workable, an US-based job recruitment portal. The cultural aspects of such portals might not be relevant to other parts of the world. For example, there are thousands of Fly-in-fly-out (FIFO) workers in Australia, who work in the mining sector. The nature of their works in the mining section is highly unusual. The workers do continuous works of 7 days on and then take the next 7 days off. An advertisement for these types of work may seem illegitimate in some parts of the world but may be completely authentic in Australia. Therefore, localisation of data source can should also be considered since nature of jobs varies based on regions of the world. In other words, if the intention of a research is to propose a framework to battle ORF in Australian context, the source of the data should also be of Australian origin.

Keeping these factors in mind, our research sets out to address several of these limitations by answering the following three research questions:

- ***RQ1***. Can a dataset specific to a regional job market (Australia) reveal more information about recruitment fraud in the region?
- ***RQ2***. Can there be an automated system that can extract contextual features given the name of a local company?
- ***RQ3***. Can the extracted contextual feature add value in improving the performance measures of an ORF detection model?

Table 1 below summarises the existing work in the field of ORF detection, against our proposed research work. The table demonstrates that apart from our proposed work, only two other research works [28], [29] considered focusing on localised factors (dataset origin highlighted in yellow). However, they were conducted under Indonesian and Bangladeshi contexts. The table also demonstrates that the usage of contextual features is infrequent among existing solutions to detect ORF. Perhaps, the difficulty level of contextual feature extraction and localisation of context plays a role in the sparseness of their usage. The last two rows (highlighted in light grey) of the table lists down our previously published work [2] and the current work, respectively. Our current work does make use of the contextual features and extend the feature set including automation of feature extraction. It also generates a localised dataset in Australian context.

In this paper, we address the research questions and make novel contributions. Firstly, we do not only reiterate the significance of contextual features from our previous work, but we also propose a multi-layer framework that automatically generates these contextual features to check the viability and reliability of companies who advertises a job in Australia. Secondly, we work with a novel dataset, which is highly relevant for Australian context since the source of the dataset is a local advertisement platform. Last but not the least, our experimentation reveals that the consideration of such automatically generated contextual features improves the performance measures of the ORF detection model on the newly generated dataset.

The next section outlines the details of our research methodology, including information about the dataset, the structure of our multi-layer framework that incorporates the contextual feature extraction engine, and the experimental setups, which demonstrates the effectiveness of such contextual features on our local dataset.

TABLE 1. Comparative analysis of related work.

Research Work	Publication Year	Dataset Used	Features used		Study Targeted for Localised Job Market	Dataset Origin (if localised)
			Content-Based Features	Contextual Features		
Vidros, et al. [25]	2017	EMSCAD	Yes	No	No	-
Alghamdi, et al. [27]	2019	EMSCAD	Yes	No	No	-
Nindyati and Nugraha [28]	2019	Google Jobs (Indonesia)	Yes	Yes	Yes	Indonesia
Tabassum, et al. [29]	2021	BD Jobs (Bangladesh)	Yes	No	Yes	Bangladesh
Goyal, et al. [30]	2021	EMSCAD and Indian Portal	Yes	Yes	No	-
Lal, et al. [31]	2019	EMSCAD	Yes	No	No	-
Mehboob and Malik [32]	2021	EMSCAD	Yes	Yes	No	-
Li, et al. [33]	2021	EMSCAD	Yes	No	No	-
Nasser, et al. [34]	2021	EMSCAD	Yes	No	No	-
Chiraratanasopha and Chayintr [35]	2022	EMSCAD	Yes	Yes	No	-
Mahbub and Pardede [2]	2018	EMSCAD	Yes	Yes	No	-
This work	-	Gumtree (Australia)	Yes	Yes	Yes	Australia

III. PROPOSED METHODOLOGY

Towards outlining our research methodology clearly, this section is divided into sub-sections, where we elaborate on the dataset, the method of research, and experimental setups, separately.

A. THE GUMTREE DATASET

To address the localisation issue of our primary goal was to select job recruitment portal, which is local to Australia. Among the popular recruitment portals, we considered several, including SEEK,[1] Glassdoor,[2] Indeed,[3] and Gumtree.[4]

Our analysis revealed that the first three are highly structured and not susceptible to many cases of recruitment frauds. Even if they are, due to the highly structured nature of these portals, it is difficult to differentiate between fraudulent and legitimate job circulars. On the contrary, Gumtree, as a platform, is highly unstructured and informal. The platform is not only used for recruitment but also used as a local advertisement platform. People buy and sell goods and services on Gumtree, which is very similar to Facebook Marketplace.[5]

To facilitate the posting of all kinds of advertisements, the platform does not have a very rigid structure on a granular level when it comes to adding a new job advertisement, which leaves fraudsters with options to omit details and focus on lucrative and luring descriptions. Moreover, Gumtree does not have a strict reviewing policy before an advertisement of any sort is posted for the public. So, due to the loosely structured template of advertisement and openness of posting any content, the platform apparently seems a place that fraudsters would lean towards to initiate recruitment frauds. Further analysis revealed that the platform has been target of employment scam very recently in the state of South Australia, while the state was under lockdown due to COVID-19 restrictions [38].

During the second half of the month of June 2019, we collected job advertisements from Gumtree for a total of 166 categories. These categories include, accounting, administrative office support, teaching, engineering, etc. The collected advertisements were then screened to remove duplicates and irrelevant advertisements. Example of an irrelevant advertisements is one that was mistakenly posted as a job in Gumtree, but in fact is an advertisement for a product, an advertisement where a person is seeking a job rather than offering one, etc. At the end of the screening process, we ended up with a total of 2,276 job advertisements, scattered across these 166 categories. The attributes that each of these job advertisements contained are given in Table 2, along with the description of each of the attributes and some example instance values from the dataset.

In the next step of the data pre-processing stage, the dataset was annotated by three independent human annotators. Each of the annotators were given a copy of the dataset, along with a set of instructions. They were asked to put a label on each of the instances. A 'no' label indicates that the advertisement is not a fraudulent one, i.e., a legitimate instance of job advertisement on Gumtree, and a 'yes' label indicates that the instance is a fraudulent advertisement with ulterior motives. The 2-page instruction sheet contained descriptions which lays out the ORF context, along with some examples of fraudulent job advertisements. The job description of one such example from the instruction sheet is given below:

> *"We are hiring people to work from home! Earn loads of cash! The easiest money ever! For more information, forward your CV with all necessary contact details to the following email address: ****@****.com". Include your driving license number in the CV for verification* purposes."

[1] https://www.seek.com.au/
[2] https://www.glassdoor.com.au/
[3] https://au.indeed.com/
[4] https://www.gumtree.com.au/
[5] https://www.facebook.com/marketplace

TABLE 2. Gumtree job advertisement attributes.

Attribute	Description	Example
AD ID	The unique ID of a job advertisement. This was collected to ensure the uniqueness of a job advertisement.	1218958311
Category	The category of the job.	Merchandiser
Images	Number of images (i.e., logos) that were uploaded along with the job.	0, 1, 2, etc.
Job title	The title of the job.	Fixed Plant Electrician
Address	The location of the job being offered (mostly city/state).	Perth, Australia
Body	The main content of a job advertisement. On Gumtree, this field is an open text field where the poster can write anything.	We are looking for an experienced carer located in the Manly area. Must be able to work more than 20 hours per week. Requirements Certificate III or IV in either Individual Support Aged Care Home and Community Care or Disability or similar First Aid certificate Police clearance Manual handling Minimum 12 months experience in similar role (desired) Valid driver's license and car (desired) Your role will include Assistance with daily living activities Light household duties Meal planning and preparation Mobility assistance Companionship Medication reminders Reporting changes in health or behavior If you possess all the required skills please apply by sending your resume to adm******@******.
Date listed	The date on which the advertisement was listed.	14/06/2019
Salary type	The type of salary being offered.	Hourly rate, Annual Salary Package, Commission only, etc.
Advertised by	The type of organization who is advertising.	Private, Agency, Not provided, etc.
Job type	The nature of the job.	Full-time, Part-time, Casual, etc.
Salary details	The details of the annual package, hourly rate, or other details such as superannuation, commission, etc.	25$ per hour, 120000 per annum, commission on top of hourly pay, etc.
Poster name	Name of the advertising organization, or the person who is posting.	Hays Healthcare, Ava Research Pty Ltd.
Label	The class label of the job advertisement.	'yes', or 'no' (more information is given below as part of annotation process).

Along with examples, the annotators were instructed to look for a set of characteristics in a job advertisement, which may indicate the fraudulence. These included:

- The title is lucrative, and contains catchphrases like, easy money, work from home, extra cash, etc.
- The description is vague and does not contain proper outline of the job description.
- The description does not contain proper outline of the required qualification.
- The advertisement does not provide specific information about job type (part-time, full-time, casual), salary type (hourly rate, annual package), location of the job, etc.
- The name of the poster is not a recognized organization and does not have an internet footprint, i.e., if we are to search google with the name of the organization, a proper reference or a website does not come up.
- The advertisement asks for sensitive information such as, passport/license number, bank account details, etc

After the labelled data were received from the three annotators, the final label of each job advertisement was evaluated based on majority voting. The three annotators agreed on the class label approximately 87% of the time. However, to avoid bias of the negative (innocent) class label, oversampling of the positive (fraudulent) class label was performed to reach the final dataset size of 2,738, out of which 495 (18.07%) were fraudulent advertisements. Table 3 contains examples of a fraudulent job advertisement and an innocent advertisement from the actual dataset, respectively. Given the large number of attributes, only the description of these two fraudulent advertisements is given in the table.

B. BINARY FEATURE VECTOR GENERATION AND GENERATION OF CONTEXTUAL FEATURES

For the next stage of data pre-processing, the labelled dataset was transformed into a binary feature vector, to be used to train and evaluate machine learning models. For each job advertisement, the binary feature vector contained a combination of 0's and 1's to represent the values of each binary feature. Apart from the content-based features, contextual features were also considered, as specified in the previous section of this paper. The contextual features aimed to identify the legitimacy of the posting organization by checking their internet footprint. The idea is that the existence of a company in a reputed and reliable registry (or database) ensures that the internet footprint of the company is solid, and any advertisement made by the company is more likely to be authentic. On the contrary, an advertisement by a person or an organization, who is not registered with any authorities, may indicate a case of fraudulent recruitment advertisement.

TABLE 3. Examples of legitimate and fraudulent job advertisements from the labelled dataset.

Example 1: Advertisement for a telemarketer (labelled as fraudulent)
Description: "*Work from home and relax. Generate the sales with a phone and Computer. Lists of business will provided to you to kick you off. All product and service detail will be handed to you with simple guidelines. We have 3 people across the globe earning just over $4500 / Month with just 4 hrs of work per week. Do you posses the skills to open and close a sale? Get paid what you are worth. Dont just be a number on the wall the more you close the more you earn. Only the passionate will succeed and have the salary to match a winners mentality.*"
Example 2: Advertisement for a refrigeration technician (labelled as legitimate)
Description: *"HVAC/Refrigeration Technician required for a role in Sydney. Your new company This client is well established across Australia and in the Sydney market they strive to maintain their prestigious reputation by completing all contracts to the highest standard and on schedule. Your new role Your new role will involve the design process through to installation as well maintenance and repair. Working within a professional team your duties will include diagnosing faults general service and minor/major repairs. u" What you'll need to succeed " You MUST be trade certified Must have valid driving license Must have a white card u" What you'll get in return " Great hourly rates Central locations Ongoing work for the right candidates Work for a prestigious company What you need to do now u" If you're interested in this role click apply now to forward an up-to-date copy of your CV."*

In addition to existence of a company in relevant registries, we also considered whether the advertiser is a recognised organisation by crosschecking if their name is identified as an 'organisation' by Named Entity Recognition (NER) models. We further investigated the internet footprint of the poster by checking whether the poster has an organisational website, i.e., a website which indicates the presence of the poster on the virtual space as a legitimate organisation.

To ensure that the reference registry for contextual feature generation was reliable, we used three different company registries in Australia. Two of these are registries of companies maintained by a non-government organization, who also happen to be popular recruitment portals in Australia. The other registry is the Australian Government's registry for registered businesses.

The registries that were used as a lookup reference for populating contextual features for this study are:

- The SEEK company registry [39], which is maintained by SEEK, the most widespread recruitment portal in Australia, and contains information and reviews on Australian companies.
- The Indeed company registry [40], which is maintained by Indeed, another popular recruitment portal in Australia, and contains information and reviews on Australian companies.
- The Australian Business Register (ABR) registry [41], which is maintained by the Australian Government. Any organization who legally conducts business in Australia is required to apply for an Australian Business Number (ABN). When an organization is issues with an ABN, their trading name and aliases are included in the ABR registry. Hence, it is the most reliable source of data for our reference.

The first three binary contextual features that we considered are, whether the poster (person or organization) is present in the SEEK company registry, the Indeed company registry, and the ABR registry, independently. In addition to these three features, we have also considered two additional characteristics of the advertiser:

- We checked whether the name of the advertiser is recognised as an *organisation name* by a Named Entity Recognition (NER) model. The rationale behind selecting this contextual feature was to leverage the fact that most fraudsters may approach prospective candidates with non-organisational profile name to avoid screening and searching by candidates.
- We further checked the existence of a company website for the advertising body. The rationale behind this was to be able to capture fraudulent advertisements in case the advertiser decides to use a fake organisational name. For checking the existence of company website, we referred to Google's search engine. Within the scope of this research, a valid website refers to a website URL that fulfils the following requirements:
  - The URL contains the name of the organisation, in some form.
  - The URL is not a reference to a social media profile, such as, Facebook, LinkedIn, Instagram, etc.
  - The URL is not a reference to a news or information repository, such as, Wikipedia.

Table 4 below, lists down all the binary features considered for training the learning models. Except the class label, all binary features have the value 1, if the answer to the specific question is yes. Otherwise, the value for the feature is 0. The class label has the value 'y' if the instance is labelled as fraudulent job advertisement, 'n' otherwise.

C. THE MULTI-LAYER DETECTION FRAMEWORK

We implemented a multi-layer framework for ORF detection. The framework is made up of three layers:

- The first layer is the data collection layer, which was implemented using Python Beautiful Soupe.[6] This particular layer of the framework was responsible for the generation of the Gumtree dataset.
- The next layer was the data analysis and fraud detection layer, which was responsible for binary feature vector generation and training and evaluation of learning

[6] https://pypi.org/project/beautifulsoup4/

TABLE 4. Binary content-based and contextual features.

Feature type	Feature
Content-based features	containsSpamWord?
	hasConsecutivePunctuation?
	hasMoneyInTitle?
	hasMoneyInDescription?
	hasExternalPrompt?
	hasNonOrganisationalEmailLink?
	isTelecommuting?
	hasConsecutiveCapitalLetter?
	educationLevelIsLow?
Contextual features	isInSeekRegistry?
	isInIndeedRegistry?
	isInABRRegistry?
	isRecognisedAsORG?
	hasAValidWebsite?
Class label	isFraudulent?

models. For machine learning, the WEKA[7] suite was used. Several experimentations were conducted using multiple machine learning algorithms, which we will outline later in this section.

- Finally, the contextual feature extraction layer was responsible for looking up the three registries and populating the contextual features given the name of an organization. The layer also incorporates the population of the other two contextual features by utilising the name of the poster. We designed the contextual feature generation layer, based on the logical discussion outlined in the previous sub-section. Our approach and associated tools and technologies are further clarified through the illustration in Figure 1 below. The figure illustrates the step-by-step process which is carried out in the contextual feature generation layer to generate the values of the contextual features using an input from the previous layer, which is essentially the name of the poster.

The data analysis layer made use of the contextual feature extraction layer by passing on the name of the posting organization. The binary feature vector generation engine was developed using Java and the contextual feature generation engine was developed using Python. Python NLP package spaCy[8] was used for the purposes of contextual feature generation. The package contains an NER model that is capable of identifying named entities, including ORGANISATION, PERSON, DATE, EVENT, etc. The contextual feature generation engine also used Beautiful Soup, and Python difflib[9] packages to utilise Google's search engine and analysis of the identified URLs.

The purpose of such a design of the framework is threefold:

- Firstly, the separation of concern for each of these layers ensures that they can be developed and used independently. For example, the contextual feature extraction layer only works with an organisation name as an input. So, it can be used with a different application as well, provided the caller of the layer forwards a named entity.
- Secondly, the individual layers can be enhanced by adding more functionality, without impacting other layers.
- Lastly, the decoupled architectural structure of the layers also enables future extension of the framework. For example, in addition to contextual feature generation layer, we can introduce another layer for linguistic feature generation for fraud detection purposes for future extension of the framework.

A flowchart representation of our research methodology is presented in Figure 2, which also outlines the different layers within the flow of actions.

TABLE 5. Experimental setup based on feature space.

Experimental label	Feature Space
A	Content-based features
B	Content-based + Contextual Features

D. EXPERIMENTAL SETUP

With the purpose of identifying consistency of performance measures, we have used multiple algorithms from the WEKA suite for machine learning. These included J48 Decision Tree, Naïve Bayes classifier, JRip rule-based classifier and Random Forest classifier. For each of these machine learning algorithms, we conducted two experiments. The first experiment was conducted with the feature space in the binary feature vector that did not include the contextual features, and the second experiment was conducted where the feature space included the contextual features.

The experimentation setup was purposefully designed this way to identify the effects of contextual features on the performance measures. Table 5 summarises the two experimental setups that was consistently maintained for each of the learning algorithms, along with the label that was assigned to each of them to be distinguished clearly.

The purpose of using multiple machine learning algorithm was solely to verify the consistency of acquired performance measures across different algorithms. The selection of these four algorithms within the collection of algorithms from WEKA suite was made based on their explicable and appropriateness, given the nature of the data.

Figure 3 visually represents the difference between experiments A and B, in terms of how the feature space varied across the two experiments. The figure also illustrates the where the machine learning models in WEKA fit into the prediction process of ORF instances. The next section outlines the findings of all the different experimentation across the two feature space setups and machine learning algorithms and draws a discussion on the findings.

[7] https://www.cs.waikato.ac.nz/ml/weka/
[8] https://spacy.io/
[9] https://docs.python.org/3/library/difflib.html

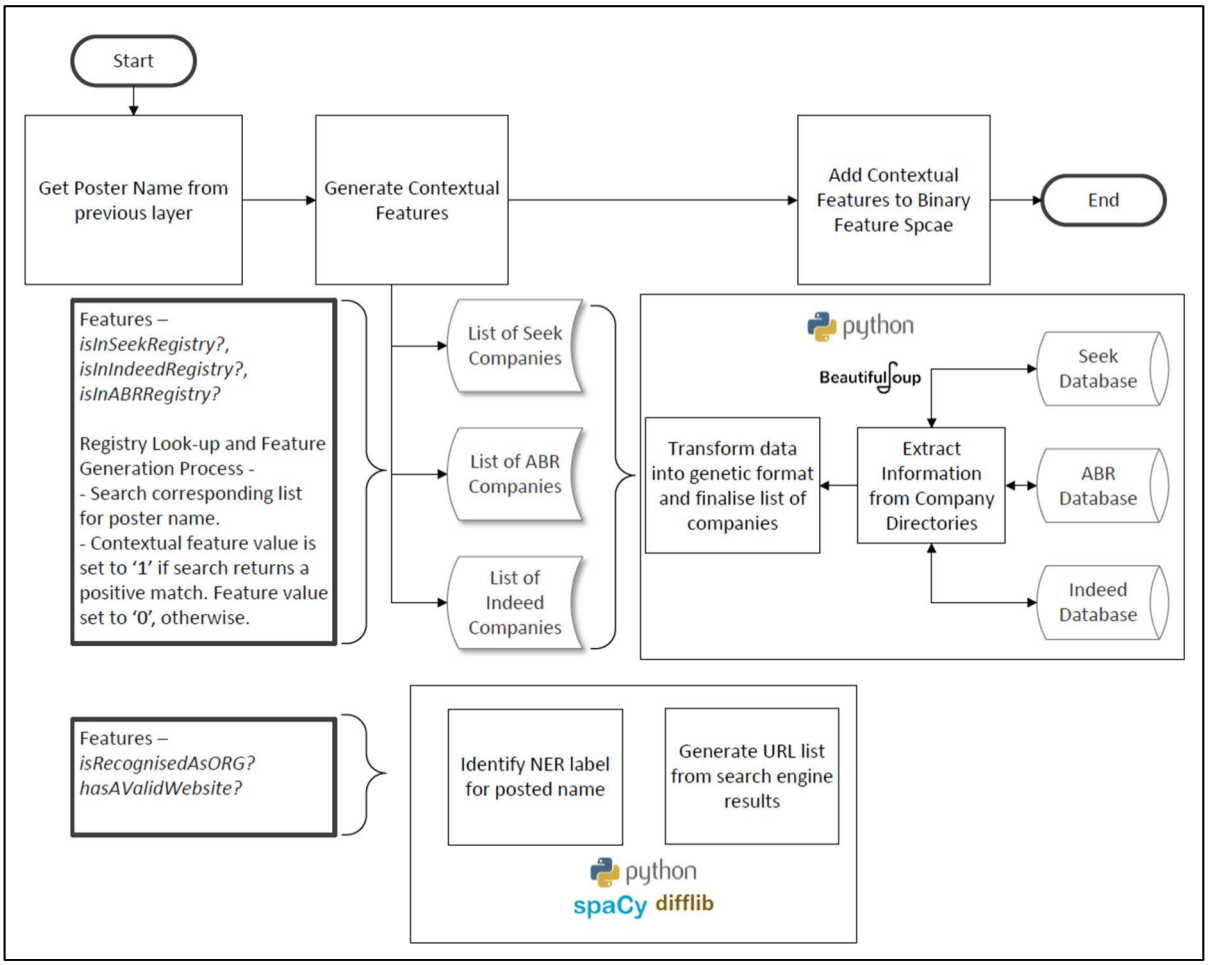

FIGURE 1. Contextual feature generation layer - the underlying process.

IV. EXPERIMENTAL FINDINGS AND DISCUSSION

Our experimental findings are summarised in Figure 2 below.

As illustrated in Figure 2, across all four algorithms, the values of accuracy, precision, and recall were consistent (with one exception of Naive Bayes giving a slightly lower recall) in terms of the improvement of measures with the inclusion of contextual features in the feature space. For example, the experimentation conducted with J48 decision tree reveals improved accuracy of 91.64% in experiment B, over 88.89% in experiment A, where the feature space included and excluded contextual features, respectively. The corresponding values of precision for class label 'y' (fraudulent class label) were 0.79 in experiment A, and 0.898 in experiment B. The recall value for the same class label also showed improved value of 0.606 in experiment B, compared to the value of 0.525 in experiment A. Similar improvements of performance measures were noted for the other algorithms as well, with Random Forest showing the best performance measures. For Random Forest classifier, the accuracy for experiment B, which included the content-based and contextual features, was 91.8%, with the precision value of 0.827, and recall value of 0.695.

As outlined in the related work section, apart from our proposed work, only two other research works [28], [29] considered focusing on localised factors. However, they were conducted under Indonesian and Bangladeshi contexts, respectively. The research word by Nindyati and Nugraha [28] reported an accuracy of 90% for the best-case scenario. Their highest values among multiple machine learning algorithm for precision and recall were 0.87 and 0.85, respectively. Our experimental findings reveal an accuracy of 91.86%, a precision value of 0.898, and a recall value of 0.695, which exceeds the reported measures in terms of accuracy and precision. The work by Tabassum, *et al.* [29], reported accuracies within the approximate range of 94-96%. However, the research did not report any other performance measure, such as, precision or recall, to demonstrate the robustness of their proposed approach. It is also critical to note that a direct comparison of performance measures of our experimental findings with these localised research works is not reasonable since the experimental findings were for different localised datasets. Therefore, we consider the measures we have reported for experiment A as the benchmark, against which, we evaluate our findings in experiment B, to be able to

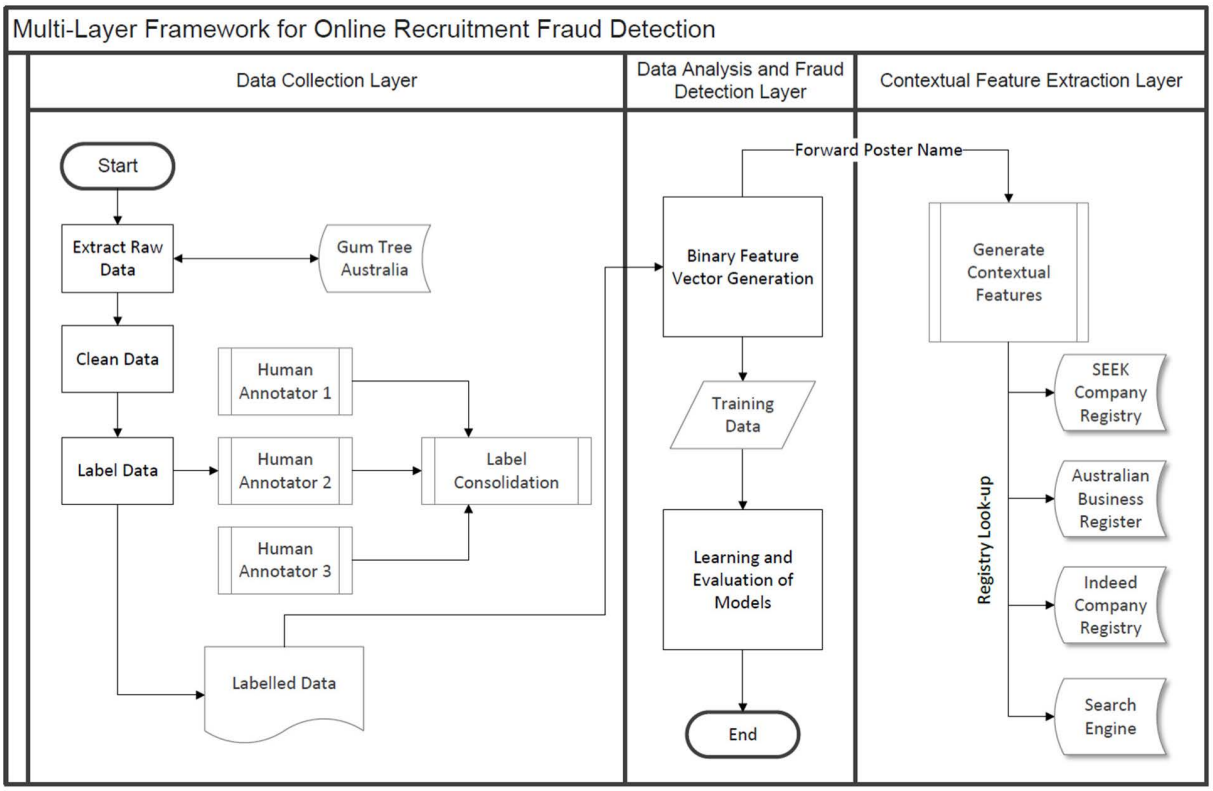

FIGURE 2. The multi-layer framework for ORF detection.

attribute the improvements of accuracy, precision, and recall in experiment B to the addition of contextual features in the feature space.

The experimental results and the dataset itself reveal interesting information to answer the research questions outlined in the motivation section. The interpretation of such improvements of performance measures in experiment B, where contextual features were included in addition to the context-based features, over experiment A, where only content-based features made up the feature space, provides clear insight into the importance of contextual features in ORF detection. Moreover, the improvements reflect the reliability of selection of SEEK, Indeed, and ABR registries as the data sources for contextual feature generation process under Australian localised circumstances, in addition to recognition of organisation names and examination of organisational websites.

Our analysis further revealed that more than 51% of the fraudulent instances of ORF did not have a valid organisational website and more than 60% of the fraudulent instances were posted by non-organisational entities, i.e., posters who advertise privately and not as an organisational representative. Although majority of the fraudulent instances did not have a company record in the ABR registry, which is the only government registry of companies in Australia that was used as a reference data source for contextual feature generation, we have found that majority of the fraudulent instances, where the poster was indeed an organisation, the organisation entries do exist in the Seek and Indeed registries.

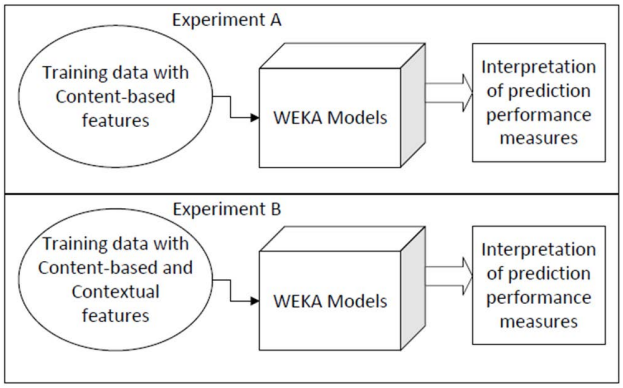

FIGURE 3. Difference in feature space between experiments A and B.

This phenomenon reveals how ABR registry, being a government registry in Australia, is more accurately maintained, as opposed to the Seek and Indeed registries, which may have more fraudulent entities registered as genuine organisations.

Apart from these findings, the low number of positive cases of recruitment fraud before oversampling our dataset reveals how less prone Gumtree is, to recruitment fraud. As discussed in the methodology section before, given the nature of the advertisement platform, our initial assumption was that the platform would be much more prone to such fraudulent behavior. As reported by an interesting study recently by Grant-Smith, *et al.* [42], there are several observed delivery

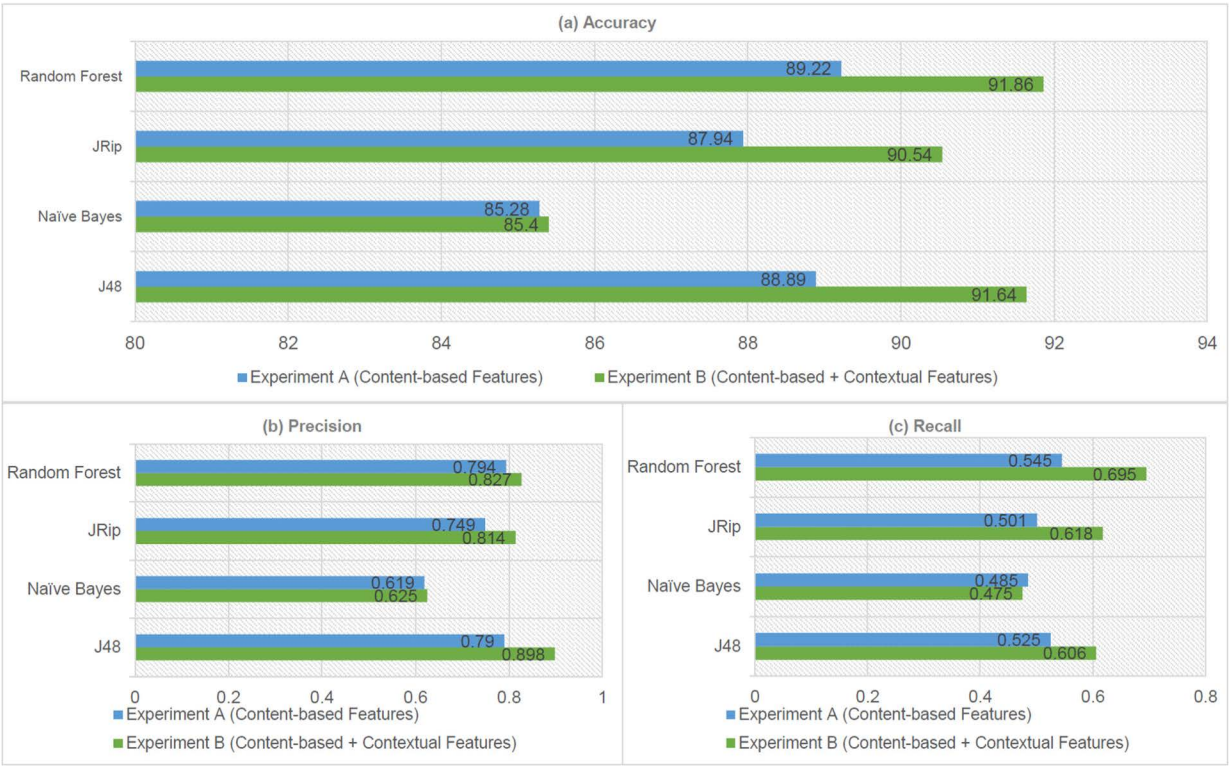

FIGURE 4. Experimental results across different setups and algorithms: (a) Accuracy, (b) Precision for class label 'y', (c) Recall for class label 'y'.

modes for employment scan in Australia, where email, phone calls, and in person visits are some of the most reported modes, in addition to internet platforms. Perhaps, other mediums of online recruitment fraud, such as, phishing emails, phone calls, need to be studied next for further information on most damaging tool used by the fraudsters responsible for numerous reported cases in Australia.

V. CONCLUSION AND FUTURE DIRECTIONS

With the increase in reported cases of ORF in Australia, it is now more critical than ever to address the problem. The first line of defence should be automatic detection efforts, which will significantly reduce the overhead of screening and policing activities conducted by law enforcement agencies. Our research proposes a multi-layer framework for ORF detection, which incorporates the generation of contextual features, based on multiple Australian Government and non-government company registries. Our research further demonstrates how inclusion of these contextual features improves the detection accuracy of ORF. However, our investigation also reveals that platforms like Gumtree may not be very prone to these sorts of fraudulent behaviours, which demands future studies of other mediums used by the fraudsters, such as, emails or smartphone text message services.

The future extension of this work will potentially explore additional contextual features, by learning more about the psychological aspects of the fraudster's mindset. The race between the adaptation of fraudsters with the changing detection strategies and the evolution of detection strategies, demands continuous development of feature space by studying the nature of fraudulent behaviours. In addition to the extension of contextual feature space, future extension may include the study of other forms of electronic communications to have a more comprehensive coverage of the domain. Last but not the least, future extensions can potentially consider exploring similar data sources in Australasian context to further increase the maturity of the dataset.

REFERENCES

[1] Australian Competition & Consumer Commission (ACCC). (2022). *Jobs & Employment Scam*. Accessed: Mar. 15, 2022. [Online]. Available: https://www.scamwatch.gov.au/types-of-scams/jobs-employment/jobs-employment-scams

[2] S. Mahbub and E. Pardede, "Using contextual features for online recruitment fraud detection," in *Proc. 27th Int. Conf. Inf. Syst. Develop. (ISD)*, Lund, Sweden, 2018, pp. 1–11.

[3] G. Stringhini, C. Kruegel, and G. Vigna, "Detecting spammers on social networks," in *Proc. 26th Annu. Comput. Secur. Appl. Conf.*, 2010, pp. 1–9.

[4] P. O. Boykin and V. P. Roychowdhury, "Leveraging social networks to fight spam," *Computer*, vol. 38, no. 4, pp. 61–68, Apr. 2005.

[5] C.-Y. Yeh, C.-H. Wu, and S.-H. Doong, "Effective spam classification based on meta-heuristics," in *Proc. IEEE Int. Conf. Syst., Man Cybern.*, vol. 4, Oct. 2005, pp. 3872–3877.

[6] H. Mohammadzadeh and F. S. Gharehchopogh, "A novel hybrid whale optimization algorithm with flower pollination algorithm for feature selection: Case study email spam detection," *Comput. Intell.*, vol. 37, no. 1, pp. 176–209, Feb. 2021.

[7] N. Sun, G. Lin, J. Qiu, and P. Rimba, "Near real-time Twitter spam detection with machine learning techniques," *Int. J. Comput. Appl.*, vol. 44, no. 4, pp. 338–348, Apr. 2022.

[8] R. M. K. Saeed, S. Rady, and T. F. Gharib, "An ensemble approach for spam detection in Arabic opinion texts," *J. King Saud Univ., Comput. Inf. Sci.*, vol. 34, no. 1, pp. 1407–1416, Jan. 2022.

[9] K. Dinakar, R. Reichart, and H. Lieberman, "Modeling the detection of textual cyberbullying," in *Proc. Int. AAAI Conf. Web Social Media*, vol. 5, 2011, pp. 11–17.
[10] Y. Kumar and B. Subba, "A lightweight machine learning based security framework for detecting phishing attacks," in *Proc. Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Jan. 2021, pp. 184–188.
[11] Y. Zhang, J. I. Hong, and L. F. Cranor, "Cantina: A content-based approach to detecting phishing web sites," in *Proc. 16th Int. Conf. World Wide Web*, 2007, pp. 639–648.
[12] W. Wang and K. McKeown, "'Got you!': Automatic vandalism detection in Wikipedia with web-based shallow syntactic-semantic modeling," in *Proc. 23rd Int. Conf. Comput. Linguistics*, Beijing, China, Aug. 2010, pp. 1146–1154.
[13] Y. Chen, Y. Zhou, S. Zhu, and H. Xu, "Detecting offensive language in social media to protect adolescent online safety," in *Proc. Int. Conf. Privacy, Secur., Risk Trust Int. Conf. Social Comput.*, Sep. 2012, pp. 71–80.
[14] M. Dadvar, F. D. Jong, R. Ordelman, and D. Trieschnigg, "Improved cyberbullying detection using gender information," in *Proc. 12th Dutch-Belgian Inf. Retrieval Workshop (DIR)*. Ghent, Belgium: Univ. of Ghent, 2012, pp. 1–3.
[15] M. Dadvar, D. Trieschnigg, R. Ordelman, and F. D. Jong, "Improving cyberbullying detection with user context," in *Proc. Eur. Conf. Inf. Retr.* Berlin, Germany: Springer, 2013, pp. 693–696.
[16] J. Cheng, C. Danescu-Niculescu-Mizil, and J. Leskovec, "Antisocial behavior in online discussion communities," in *Proc. Int. AAAI Conf. Web Social Media*, vol. 9, 2015, pp. 61–70.
[17] S. Mahbub, E. Pardede, and A. S. M. Kayes, "Detection of harassment type of cyberbullying: A dictionary of approach words and its impact," *Secur. Commun. Netw.*, vol. 2021, pp. 1–12, Jun. 2021.
[18] K. Maity, A. Kumar, and S. Saha, "A multi-task multi-modal framework for sentiment and emotion aided cyberbully detection," *IEEE Internet Comput.*, vol. 26, no. 4, pp. 68–78, Jul./Aug. 2022.
[19] K. Lee, S. Webb, and H. Ge, "Characterizing and automatically detecting crowdturfing in Fiverr and Twitter," *Social Netw. Anal. Mining*, vol. 5, no. 1, pp. 1–16, Dec. 2015.
[20] C. Xu, J. Zhang, K. Chang, and C. Long, "Uncovering collusive spammers in Chinese review websites," in *Proc. 22nd ACM Int. Conf. Conf. Inf. Knowl. Manag.*, 2013, pp. 979–988.
[21] N. Su, Y. Liu, Z. Li, Y. Liu, M. Zhang, and S. Ma, "Detecting crowdturfing 'add to favorites' activities in online shopping," in *Proc. World Wide Web Conf.*, 2018, pp. 1673–1682.
[22] D. Gavra, K. Namyatova, and L. Vitkova, "Detection of induced activity in social networks: Model and methodology," *Future Internet*, vol. 13, no. 11, p. 297, Nov. 2021.
[23] B. Liu, X. Sun, Q. Meng, X. Yang, Y. Lee, J. Cao, J. Luo, and R. K.-W. Lee, "Nowhere to hide: Online rumor detection based on retweeting graph neural networks," *IEEE Trans. Neural Netw. Learn. Syst.*, early access, Apr. 6, 2022, doi: 10.1109/TNNLS.2022.3161697.
[24] S. Vidros, C. Kolias, and G. Kambourakis, "Online recruitment services: Another playground for fraudsters," *Comput. Fraud Secur.*, vol. 2016, no. 3, pp. 8–13, Mar. 2016.
[25] S. Vidros, C. Kolias, G. Kambourakis, and L. Akoglu, "Automatic detection of online recruitment frauds: Characteristics, methods, and a public dataset," *Future Internet*, vol. 9, no. 1, p. 6, Mar. 2017.
[26] University of Aegean Laboratory of Information & Communication Systems Security. (2017). *Employment Scam Aegean Dataset*. Accessed: Apr. 12, 2018. [Online]. Available: http://emscad.samos.aegean.gr/
[27] B. Alghamdi and F. Alharby, "An intelligent model for online recruitment fraud detection," *J. Inf. Secur.*, vol. 10, no. 3, p. 155, 2019.
[28] O. Nindyati and I. G. B. B. Nugraha, "Detecting scam in online job vacancy using behavioral features extraction," in *Proc. Int. Conf. ICT Smart Soc. (ICISS)*, Nov. 2019, pp. 1–4.
[29] H. Tabassum, G. Ghosh, A. Atika, and A. Chakrabarty, "Detecting online recruitment fraud using machine learning," in *Proc. 9th Int. Conf. Inf. Commun. Technol. (ICoICT)*, Aug. 2021, pp. 472–477.
[30] N. Goyal, N. Sachdeva, and P. Kumaraguru, "Spy the lie: Fraudulent jobs detection in recruitment domain using knowledge graphs," in *Proc. Int. Conf. Knowl. Sci., Eng. Manag.* Cham, Switzerland: Springer, 2021, pp. 612–623.
[31] S. Lal, R. Jiaswal, N. Sardana, A. Verma, A. Kaur, and R. Mourya, "ORFDetector: Ensemble learning based online recruitment fraud detection," in *Proc. 12th Int. Conf. Contemp. Comput. (IC3)*, Aug. 2019, pp. 1–5.
[32] A. Mehboob and M. S. I. Malik, "Smart fraud detection framework for job recruitments," *Arabian J. Sci. Eng.*, vol. 46, no. 4, pp. 3067–3078, Apr. 2021.
[33] J. Li, Y. Li, H. Han, and X. Lu, "Exploratory methods for imbalanced data classification in online recruitment fraud detection: A comparative analysis," in *Proc. 4th Int. Conf. Comput. Big Data*, Nov. 2021, pp. 75–81.
[34] I. M. Nasser, A. H. Alzaanin, and A. Y. Maghari, "Online recruitment fraud detection using ANN," in *Proc. Palestinian Int. Conf. Inf. Commun. Technol. (PICICT)*, Sep. 2021, pp. 13–17.
[35] B. Chiraratanasopha and T. Chay-Intr, "Detecting fraud job recruitment using features reflecting from real-world knowledge of fraud," *Current Appl. Sci. Technol.*, vol. 22, no. 6, p. 12, Feb. 2022.
[36] Indeed. (2019). *Indeed Career Guide*. Accessed: Apr. 10, 2021. [Online]. Available: https://au.indeed.com/career-advice/finding-a-job/the-essential-job-search-guide
[37] SEEK. (2020). *Job Hunting*. Accessed: Apr. 4, 2021. [Online]. Available: https://www.seek.com.au/career-advice/job-hunting
[38] J. Bassano. (2020). *Scammers Target SA Job Seekers*. Accessed: Jan. 21, 2021. [Online]. Available: https://indaily.com.au/news/2020/05/06/scammers-target-sa-job-seekers/
[39] SEEK. (2021). *Seek Company Directory Listing*. Accessed: Feb. 10, 2021. [Online]. Available: https://www.seek.com.au/companies/browse
[40] Indeed. (2021). *Find the Best Companies to Work*. Accessed: Jan. 21, 2022. [Online]. Available: https://au.indeed.com/companies
[41] Australian Government. (2021). *ABN Lookup*. Accessed: Jan. 10, 2021. [Online]. Available: https://abr.business.gov.au/
[42] D. Grant-Smith, A. Feldman, and C. Cross, "Key trends in employment scams in Australia: What are the gaps in knowledge about recruitment fraud," QUT Centre Justice Briefing Papers, Queensland Univ. Technol. (QUT), Brisbane, QLD, Australia, Tech. Rep. 21, 2022.

SYED MAHBUB received the bachelor's degree in computer science and engineering from the Bangladesh University of Engineering and Technology, in 2012, and the master's degree in information technology from La Trobe University, in 2016, where he is currently pursuing the Ph.D. degree in social network analysis and feature engineering. He worked as a Software Engineer for three years in the industry. He is an Associate Lecturer with the Department of CS and IT for the past three years. His research interests include natural language processing, social network analysis, and feature engineering.

ERIC PARDEDE (Senior Member, IEEE) received the master's degree in information technology and the Ph.D. degree in computer science from La Trobe University, Melbourne, Australia. He is currently an Associate Professor with La Trobe University. He has been published more than 100 publications in international journals and conference proceedings in the research areas. His research interests include data analytics, IT education, and entrepreneurship.

A. S. M. KAYES (Member, IEEE) received the Ph.D. degree from the Swinburne University of Technology, Australia. He is currently a Senior Lecturer of cybersecurity with the Department of Computer Science and Information Technology, La Trobe University, Melbourne, Australia. His research interests include information modeling, data privacy and security, context-aware access control, the Internet of Things, and cloud and fog security.