

# Reveal: Online Fake Job Advert Detection Application using Machine Learning

Prashanth C  
Department of Computer Science and  
Engineering  
Sri Sai Ram Engineering College,  
Autonomous  
Chennai, India  
cprashanth00@gmail.com

Deepanjali Chandrasekaran  
Department of Computer Science and  
Engineering  
SRM Institute of Science and  
Technology, Ramapuram Campus  
Chennai, India  
deepuchandru2001@gmail.com

Bhuvanashree Pandian  
Department of Computer Science and  
Engineering  
SRM Institute of Science and  
Technology, Ramapuram Campus  
Chennai, India  
apbhuvana2001@gmail.com

Kavitha Duraipandian  
Department of Computer Science  
SRM Institute of Science and  
Technology, Ramapuram Campus  
Chennai, India  
kavithad3@srmist.edu.in

Thomas Chen  
Department of Computer Science and  
Engineering  
City, University of London  
London, UK  
tom.chen.1@city.ac.uk

Mithileysh Sathiyarayanan  
Research & Innovation  
MIT Square, London  
City, University of London  
London, UK  
mithileysh@mitsquare.com

**Abstract**— New technologies are rapidly emerging to fight increasing Job scams. Online Job scams are onerous to detect, thus giving the perpetrators plenty of time to flee the area in which the crime was committed, because of this fact the criminals can be in another country far away from the scene of the crime by the time it is detected. In today's digital world, we see many such instances where a particular person is targeted. The introduction of the internet and the quick access of social networking sites (including Twitter and Instagram) prepared the door for unprecedented levels of knowledge distribution in human history. Humans can be vulnerable and easily deceived making technological advances inadequate for Online Job scams. Fake recruitments are advertised to entice people to apply, so fraudsters can gain personal information such as residential address, email address, contact number, date of birth, previous job history, bank details and steal complete identify. In this paper, we developed Reveal, a machine learning-based web application, to identify fake online job advertisements such that the applicants are cautious in applying for jobs that are authentic and reliable.

**Keywords**— Online Scams, Cyber Threats, Digital Crime, Internet Security, Fraud Detection.

## I. INTRODUCTION

To analyse and forecast internet job postings across a range of online sites is quite challenging. To identify whether a job advert is genuine or not needs a good research. It would be easier for job applicants to focus on genuine jobs advertised if such fraudulent job adverts can be identified and removed. Especially, with economic crisis and the coronavirus impact, significantly job opportunities are reduced and job loss are on increase. This has created several computer fraud and digital crimes where many applicants get trapped into. In recent days, many companies prefer to post their vacancies online so that the links can be accessed easily and timely by the job-seekers. However, this intention is wrongly used by the fraudsters to use the company and job information to trick candidates for acquiring personal and bank details. In many cases, fraudsters take money from job applicants in guaranteeing a job and/or hack their bank accounts. Fraudulent job advertisements are also posted against a reputed company for damaging its reputation and credibility. This paper aims to identify online fake job posts. This fraudulent job post-detection draws good attention for obtaining an automated tool for identifying fake jobs and reporting them to people for avoiding application for such

jobs. Our application Reveal gets the input (URL) from the user in order to check whether the job advert is genuine or fake, then lists in a particular site like indeed, monster, quikr, and so on. Once the input URL link is validated, the web scraping process starts and the URL changes to Html format and we retrieve the related details. Such information would be verified with the original data available on our reveal site. The subsequent sections demonstrates how we used the methodology to build our tool.

## II. RELATED WORKS

Cybercrime is among the most dangerous offenses currently confronting the globe, posing a potential threat to persons and businesses and resulting in significant financial damages. As per cyber security initiatives assessment 2021, the global price of malware losses is almost \$6 trillion every year. As a result, we urgently want Information Security to maintain Confidentiality, Integrity, and Availability (CIA) to counter such frauds. This can be accomplished by putting in action well-known data security tactics like avoidance, monitoring, and response [1].

Computer fraud can be an untrustworthy misrepresentation of the fact proposed to prompt another to abstain from doing something that causes loss. Computer crime can be summarized as a criminal activity that involves information technology infrastructure, in addition to unauthorized access, illegal interception, any data interference, computer or systems interference, abuse of devices, forgery, blackmail, embezzlement, and some electronic fraud. Employment scam is one of the serious issues in recent times addressed in the domain of Online Recruitment Frauds.

Often false information looks somewhat like factual reporting that it is indeed hard for humans to spot the difference. As a result, computerized technologies for detecting fake information, such as machine learning and data mining models, are becoming a necessity. Many types of research are focused on developing better and automated methods towards online spam detection over real-time to distinguish misleading information from factual reporting. A group of experts suggested their algorithms on machine learning and deep learning techniques. Such approaches, nevertheless, do have reliability limits. A better strategy is

required to address such challenges and successfully detect bogus information [2].

False information identification is composed of three viewpoints: how misinformation is written, how false information circulates, and how an individual is connected to false information. To identify fake stories, characteristics linked to news channels and social surroundings are retrieved, and machine learning techniques are applied [3].

Scams in the recruiting process may arise, which, of course, might lead to long-term financial losses. Scam control can be accomplished by using a Decision Support System (DSS) to choose individuals based upon those requirements and specifications. A DSS can indeed be one alternative plan for reducing forgery, as well as the outcomes of the shortlisting can be made quickly, allowing managers to acquire actual information from every job candidate [4].

Acquiring an effective automatic system for detecting fraudulent offers and reporting information to people to prevent enrolling for such employment invites great enthusiasm. To detect phony advertisements, a machine learning technique is used that utilizes numerous categorization techniques. In this scenario, a classifying algorithm separates bogus job postings from a bigger pool of job postings and notifies the user [5]. In recent times, the online job business has emerged as a new sort of weird scam known as Online Recruitment Fraud (ORF). Fraudsters use ORF to make attractive employment proposals to prospects while stealing their personal and financial data [6].

To breach any renowned business' reputation, fake job adverts might be advertised. Numerous machine learning algorithms are available for detecting job scams. The supervised technique is used to demonstrate the usage of multiple classifications in the identification of job scams [7]. Cybercrime incidents were happenings of certain major crimes that represent a significant threat to international commerce, current societal security. Cybercrime is a combination of different offenses and modern illicit activities. Specific cyberattacks incidents are occurrences of specific criminal violations some of which are increasing exponentially, especially evidenced by different national crime statistics and polls [8].

Whenever it comes to malware and online crimes, big data becomes a complexity to crime forensic analysts. Conventional investigative methods and computer forensics technologies are becoming less effective as their capacity to deliver necessary outcomes in a rapid and resource-constrained way deteriorates. The use of computational forensics related to modern big data analysis helps identify as well as prevent cyberattacks remains a key potential alternative for Digital Crime Analysis. As a result, machine learning and computational techniques should be included in the research [9].

The challenge of job scam prediction could be described as the method of identifying a portion of an Applicant Tracking System's information that's also intended to be used for dishonest operations rather than legitimate recruitment. Connecting details concerning the linguistic, organizational, and contextual properties of that material are normally how a strategy is accomplished. Job scam prediction is clearly recognizable from other important issues such as phishing emails, hacking, Website vandal, online harassment, trolls [10]. Recognizing false news presents a

number of unique and hard proposed solutions. Although false information may not be a new issue and organizations used the media outlets to carry out propagandist and influencing activities for hundreds of years, the development of internet news content has amplified the overall potency of false news, challenging traditional professional conventions. There seem to be various elements of such a topic that render detection and tracking particularly difficult [11]. We can predict fraudulent jobs with the use of machine learning, which might assist candidates in making the best decisions and remaining vigilant. The model will be trained like a Sequential Neural Network with GloVe Algorithm and would use NLP to understand individual emotions. As a result, LinkedIn job postings will be predicted by the trained model [12]. Evaluate a data set and classify job advertisements as fake or genuine with ml algorithms. The study makes a significant addition by including contextual information in the feature set, which resulted in significant increases in accuracy, precision, and recall. Depending on the research technique, more bogus employment will be found in the filtration phase if many sophisticated backend filtration technologies can be deployed on such platforms. Frequent customers will be prevented from inadvertently disclosing personal information by registering for positions that do not exist [13]. Economic security, personal protection, information protection, confidentiality, and cybercriminals are the most serious modern challenges. The main concern in e-shopping, and can be solved if confidentiality and anonymity are provided [14]. Applicant Tracking Systems (ATS) - aids in the recruitment of excellence and the placement of job applicants. Such tools made the recruiting process faster, more precise, and less expensive. The ATS ensures a simplified process that begins with the creation of the job role and ends with the posting of the job posting on prominent job websites (such as Indeed, Monster) and also social media sites (such as LinkedIn, Twitter). The used ATS tries to build a complete applicant profile for each receiving cv, containing detailed information on the person's qualifications, job experience, talents, personal contacts, and career path [15].

KNN, decision tree, support vector machine, naive Bayes classifier, random forest classifier, gradient boosting, and neural network are examples of data mining methods and classification techniques that can be used to determine whether a job posting is legitimate or not. Studies with 18000 data from the Employment Scam Aegean Dataset (EMS CAD). The classification challenge is very well to the use of a deep neural network as a classifier. For this deep neural network classifier, they utilized 3 thick layers. The developed algorithm assumes a bogus job advertisement with a classification result of around 98 % (DNN) [16]. Piracy is defined as the unauthorized stealing of material from such a licensed user and afterward disseminating it to others. It is among the most popular types of assault. Torrent websites are real instances of this; such sites contain all media (films, games, and Television programs) within hours of its release for no cost. As a result, ordinary people do not end up spending on genuine goods and instead obtain a pirated version from such platforms [17].

To commit an offense, little skill or knowledge is necessary. A weak individual can be easily attacked with just a few technical skills combined with very little intelligence.

In comparison to conventional offenses, cybercrime is much more horrible and destructive. Inside this present growth environment, that is entirely reliant on the internet, so each country and individual need to be knowledgeable about cyberattacks, illegal behaviour, and the norms that govern it. "Hacking oneself is indeed the preferred approach to protect oneself against hackers" [18-19]. Governments and public safety organizations must consider the potential and broadly applicable international norms, regulatory measures, including protocols for investigating hackers involved in corruption or counterterrorism funding activities [20].

According to research, cybercrimes are on the rise, and the number of casualties is between the ages of 20 and 29. As per the survey, India is ranked 3rd for the frequency of cyber-crime. According to several publications reviewed, cyber-crime affects women, youngsters, and elderly individuals. It is nearly impossible to eliminate cyber-crime without a worldwide determination to do so. To make use of the online era's perks, we must defend ourselves against cyber-crime and be very attentive and informed of current forms of fraudulent methods [21].

Some of the top Cyber Security Threats involve Ransomware, hacking, Data Leakage, Scammer Attacks, and Computer Viruses. Modern Challenges in Cyber Security is constantly increasing with the enhancement of innovative idea [22]. To protect computer programs from proper evaluation, malware authors implement a variety of avoidance methods. In a virtual environment, the avoidance approach strives to confuse code and even interrupt efforts at disassembling, debugging, or identification, making malware analysis more difficult [23].

Because of the difficulty in investigating cybercrime and the absence of reliable evidence, the amazing rise of computers and Internet services has created the problem of cybercrime dissemination. Furthermore, existing rules and prevention efforts are ineffective in preventing similar crimes. Because of the absence of legal security, corporations and governments must implement strong technological security to protect themselves from individuals who would steal, refuse accessibility to, or delete sensitive data [24]. The establishment of a standardized approach for measuring ICT expenditure for the protection of cybercrime and many other security concerns resulted from the consideration of the problem connected with evaluating investments in information security. The approach is based on the usage of tools and techniques that have previously been used to measure the value of organizational resources and the risk of systems [25].

Blockchain technology is an example of a new invention being explored to make internet settings more secured. Nicolas Blasco and Nicholas Fett look into the benefits and drawbacks of blockchain networks, an emerging technology that seeks to make virtual platforms safer and more efficient. The authors particularly analysed the role of implementing security in cybercriminals within the theoretical model of prevention and detection theories [26].

### III. METHODOLOGY

To classify bogus job postings, the project makes use of multiple datasets. The dataset is made up of verified job information. Fig.1 shows the home page of the website which has the options to check the job advert is real or fake.

Fig.2 shows the space to insert the URL link of any employment website in order to know the job advert is real or fake. The user can input the URL of job portals such as Indeed in the first section. Jobs from the web page are retrieved using web scraping, and each job is compared to the original data set accessible before being classed as real or fraudulent.

#### A. Natural Language Processing

NLP is a branch of artificial intelligence that involves a computer's capacity to comprehend, interpret, manipulate, and possibly synthesize human language. Computers can read text, hear speech, understand it, measure sentiment, and identify which bits are significant using natural language processing (NLP).

#### B. Web Scraping

Web scraping is the practice of extracting data and information from such a website with bots. The scraper could then copy the full website to another location. A multitude of technology companies that depend on data gathering adopt web scraping. This is very useful in order to extract job post data with the proper time, role, requirements, and address details for collecting the information for further processing.

The link is passed as input and the URL is validated. The web scraper collects all data for each job of the respective search query. The data includes job name, company name, job location, salary. The original dataset contains the same details of authentic jobs such as job name, company name, job location, and salary. The job name, company name, location, the salary of each job from scraped data is compared with job name, company name, location, the salary of the original data. If all the details match, then the job is marked as authentic, but if any one of the details did not match it is marked as fake. Then each of the jobs listed are flagged as fake or authentic.

#### C. Machine Learning

To classify bogus job postings, the project makes use of multiple datasets. The dataset is made up of verified job information. The data set is obtained from various APIs and collected from various companies while posting in job portals. The data is maintained as dynamic centralized data. The data set is stored as csv file. The dataset contains 18000 rows of data i.e. data of 18000 jobs. This dataset consists of fake and authentic jobs. The necessary columns of job data such as job name, company name, location, salary etc. The machine learning algorithms such as random forest, linear regression, support vector machine, decision trees are trained with the dataset. The prediction of each algorithm is tested using the test data. The algorithm which has higher prediction is selected, tested and trained again. The user inputs are tested with the model developed. Then the job is marked as fake or authentic. Fig.5 shows the classification process with the testing and training dataset.

## IV. RESULTS

#### A. Real Time Survey

The main aim of conducting a survey was to understand what people think about online fake job adverts listed by various companies or organizations. We had a questionnaire with nearly 20 questions to understand the fake job adverts patterns like the company location (Chennai,

Vellore, Kaniyambadi), designation (Information Technology and Services, Internet, Marketing and Advertising), Experience requirements, Employment Type(Part-time, Full time) much more. From the survey, we acquired some findings.

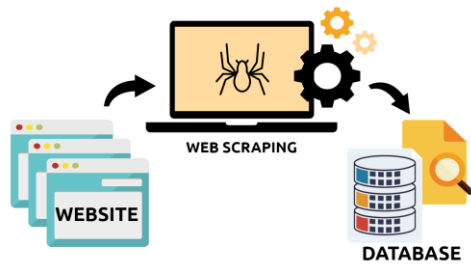


Fig.4 Web Scrapping Process

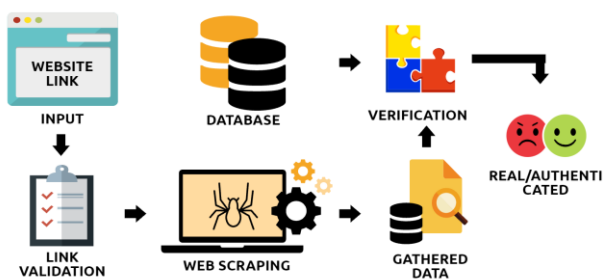


Fig.5 Process of Job Post Detection

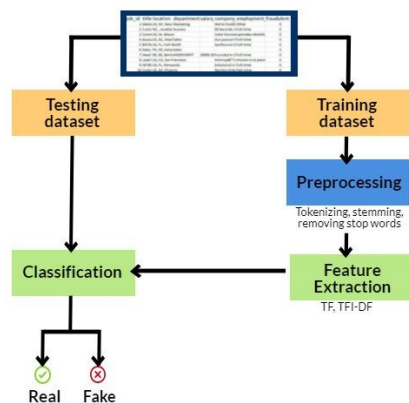
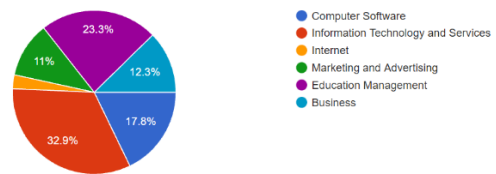


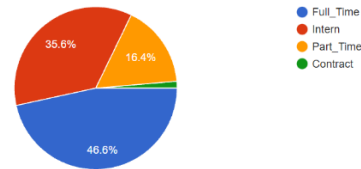
Fig.6 Classification Flow Chart

Most of the fake advertisements are from the IT & Education sector (73%). Most of the applicants are full-time and interns, especially freshers (82%), who get trapped in the scams by using multiple online sites in random google search. In most cases, 41% applicants, were asked to pay amount upfront and 54.8% people were asked to provide complete personal details. When questioned, 90% participants have found several fake jobs advertised and again 90% of participants have not filed any case or complaint against the company or fake adverts. The results helped us to develop a tool that can help people quickly identify fake jobs.

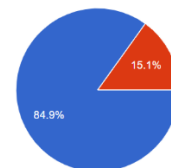
1.The fake company belongs to which industry?



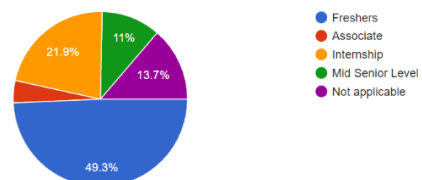
2.What is the employment type provided by that company?



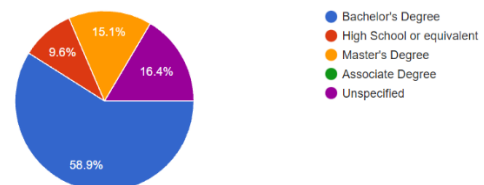
3.Did the job information have its Company Logo?



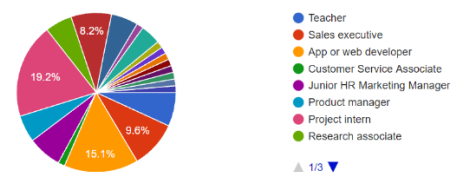
4.Experience required by that company



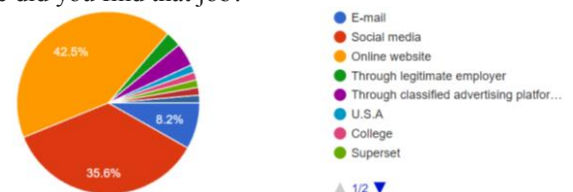
5.Education required by that company



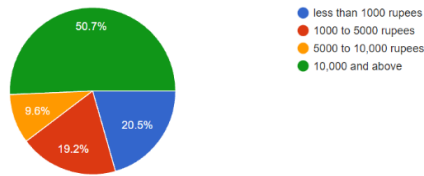
6.What job offer did you get?



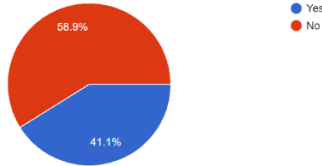
7.Where did you find that job?



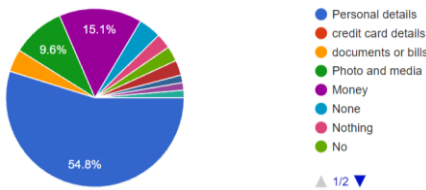
8.How much salary did the fake job offer?



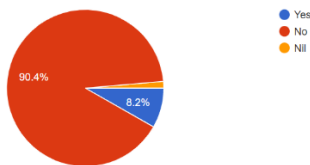
9. Were you asked to pay some amount in advance?



10. What did they steal from you?



11. Did you file a complaint about this fake job?



12. Have you ever found a fake job on social media?

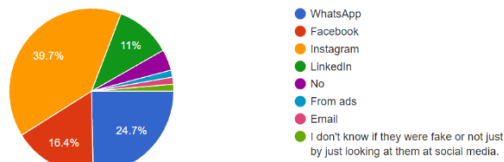


Fig.1 shows our Reveal, screenshot of our job advert verification tool. Fig.2 shows the screenshot from the Indeed Job Search. We copy the URL from the Indeed website (Fig.3) to test it in our Reveal Tool. Fig. 4 shows the outcome of the URL check which contains several job advert profiles. Several companies are flagged as fake and authentic. It means job adverts (from the URL) are matching or not-matching based on the original data (simulated data). Thus, our tool aids in quickly understanding which jobs are fake. describes job advert as not matching with the original data (simulated data) collected from the internet.

## REVEAL TOOL

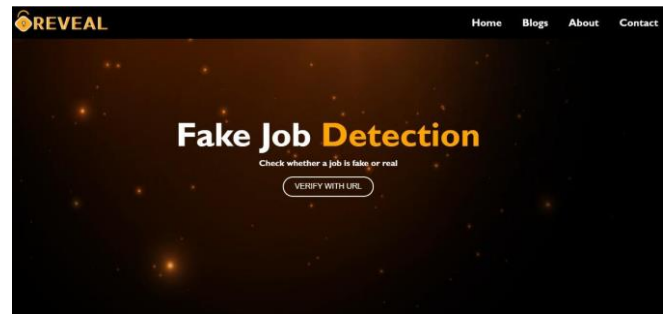


Fig.1 Reveal: A screenshot of the job advert verification tool.

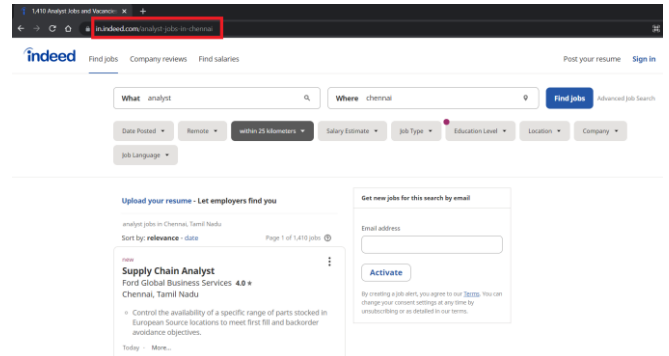


Fig.2 Screenshot from Indeed Job Search. We copy the URL to test it in our Reveal Tool.

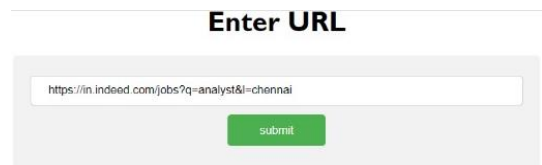


Fig.3 The URL from the Indeed Job Website is tested in our Reveal Tool.

Job Title	Company	Location	Temporarily Remote	Not Found	Fake
Business Analyst	Patel Software Solutions Pvt Ltd.	Chennai, Tamil Nadu		Not found	Fake
Junior Associate/Analyst - Software Quality Analyst	Lawson Software Pvt Ltd	Chennai, Tamil Nadu	Temporarily Remote	Not found	Fake
ARK, NYC Analyst	IBM	Chennai, Tamil Nadu		Not found	Authenticated
Customer Service & Operations Analyst, Webchat	Northstar Group	Chennai, Tamil Nadu		Not found	Fake
Data Analyst	Shell	Chennai, Tamil Nadu		Not found	Fake
Analyst - 0080 Tips - IG	MR. Cooper	Chennai, Tamil Nadu		Not found	Fake
Data Analyst	Morgan Learning & Analytics Pvt Limited	Chennai, Tamil Nadu		Not found	Fake
Investment Banking Analyst	Princo	Chennai, Tamil Nadu		Not found	Fake
Compliance Analyst	Princo	Chennai, Tamil Nadu		Not found	Fake
Junior Informatica ETL support analyst	CACTUSGLOBAL LTD (www.cactusglobal.com)	Chennai, Tamil Nadu		Not found	Fake
Analyst - 3284	Securix Global	Chennai, Tamil Nadu		Not found	Fake
FP&A Analyst	Phelps	Chennai, Tamil Nadu		Not found	Fake
Analyst	TransUnion	Chennai, Tamil Nadu		Not found	Fake
Agm Support Analyst	IBM	Chennai, Tamil Nadu		Not found	Fake
Financial Analyst (FP&A)	ProPal	Chennai, Tamil Nadu		Not found	Fake
Customer Service & Operations Analyst	Northstar Group	Chennai, Tamil Nadu		Not found	Authenticated
Account Business Analyst	CH Software	Chennai, Tamil Nadu		Not found	Fake
Financial Analyst	World Bank Group	Chennai, Tamil Nadu		Not found	Fake
Analyst	Shell	Chennai, Tamil Nadu		Not found	Fake

Fig.4 List of jobs flagged as fake and authentic.

## V. CONCLUSION & FUTURE WORK

In today's digital world, we see many instances where young students are targeted and their personal details are captured in the form of fake job adverts. These things are performed to entice people to apply, so fraudsters can gain personal information such as residential address, email address, contact number, date of birth, previous job history, bank details and steal complete identify. In this paper, we developed Reveal, a machine learning-based web application, to identify fake online job advertisements such that the applicants are cautious in applying for jobs that are

authentic and reliable. Our application Reveal gets the input (URL) from the user in order to check whether the job advert is genuine or fake, then lists in a particular site like indeed, monster, quikr, and so on. Once the input URL link is validated, the web scraping process starts and the URL changes to Html format and we retrieve the related details. Such information would be verified with the original data available on our reveal site. The user can search for a list of jobs or a single job with information using a URL. This procedure is both relevantly quick and accurate. The database is updated on a regular basis. In the future we will be carrying out more analysis by connecting multiple databases and languages. We'll also strive to apply a wider range of machine learning and visualisation techniques [27-32] to classify fraudulent online job posts. We will also aim to detect fake jobs in different regions and languages across the globe.

## REFERENCES

- [1] Bandar Alghamdi, Fahad Alharby, "An Intelligent Model for Online Recruitment Fraud Detection", *Journal of Information Security*, 2019, pp. 155-176.
- [2] Tao Jiang, Jian ping li, Amin ul Haq, Abdus labor, and Amjad al, "A Novel Stacking Approach for Accurate Detection of Fake News", *Vol. 9*, 2021, pp. 22626-22639.
- [3] Karri sai Suresh reddy, karri Lakshmana reddy, "fake job recruitment detection", *JETIR August 2021, Vol. 8*, pp. d443-d448.
- [4] Tulus Suryanto, Robbi Rahim, Ansari Saleh Ahmar, "Employee Recruitment Fraud Prevention with the Implementation of Decision Support System", *Journal of Physics Conference Series*, 2018, pp.1-11.
- [5] C. Jagadeesh, Dr. Pravin R Kshirsagar, G. Sarayu, G.Gouthami, B.Manasa, "Artificial intelligence based Fake Job Recruitment Detection Using Machine Learning Approach", *Journal of Engineering Sciences*, Vol. 12, 2021, pp. 0377-9254.
- [6] Lal, Sangeeta, Rishabh Jiaswal, Neetu Sardana, Ayushi Verma, Amanpreet Kaur, and Rahul Mourya. "ORFDetector: ensemble learning based online recruitment fraud detection." In *2019 Twelfth International Conference on Contemporary Computing (IC3)*, pp. 1-5. IEEE, 2019.
- [7] Samir Bandyopadhyay, Shawni Dutta, "Fake Job Recruitment Detection Using Machine Learning Approach", *International Journal of Engineering Trends and Technology (IJETT)*, Vol. 68, 2020, pp. 48-53
- [8] George Tsakalidis, Graduate Student Member, IEEE, and Kostas Vergidis, "A Systematic Approach Toward Description and Classification of Cybercrime Incidents", *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, Vol. 49, 2019, pp. 1-20
- [9] Andrii Shalaginov, Jan William Johnsen, Katrin Franke, "Cyber Crime Investigations in the Era of Big Data", *IEEE International Conference on Big Data*, 2017, pp. 3672-3676.
- [10] Sokratis Vidros, Constantinos Kolias, Georgios Kambourakis and Leman Akoglu, "Automatic Detection of Online Recruitment Frauds: Characteristics, Methods, and a Public Dataset", *Future Internet* 2017, pp. 2-19.
- [11] Shu, Kai, Amy Sliva, Suhang Wang, Jiliang Tang, and Huan Liu. "Fake news detection on social media: A data mining perspective." *ACM SIGKDD explorations newsletter* 19, no. 1 (2017): 22-36.
- [12] Devsmit Ranparia; Shaily Kumari; Ashish Sahani, "Fake Job Prediction using Sequential Network", *IEEE 15th International Conference on Industrial and Information Systems (ICIIS)*, 2020, pp.339-343
- [13] Syed Mahbub, Eric Pardede, "Using Contextual Features for Online Recruitment Fraud Detection", *27th International Conference on Information Systems Development*, 2018.
- [14] Najma Imtiaz Ali, Suhaila Samsuri, Muhamad Sadry, Imtiaz Ali Brohi, Asadullah Shah, "Online Shopping Satisfaction in Malaysia: A Framework for Security, Trust and Cybercrime", *6th International Conference on Information and Communication Technology for The Muslim World*, 2016, pp. 194-198.
- [15] Vidros, Sokratis; Kolias, Constantinos; Kambourakis, Georgios, "Online recruitment services: another playground for fraudsters", *Computer Fraud & Security*, 2016, pp. 8-13.
- [16] Sultana Umme Habiba, Md. Khairul Islam, Farzana Tasnim, "A Comparative Study on Fake Job Post Prediction Using Different Data mining Techniques", *2nd International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST)*, 2021, pp. 543-546.
- [17] Sarvesh Tanwar, Thomas Paul, Kanwarpreet Singh, Mannat Joshi, Ajay Rana, "Classification and Impact of Cyber Threats in India: A review", *8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, 2020, pp. 129-135.
- [18] Veena, K., and P. Visu. "Detection of cyber crime: An approach using the lie detection technique and methods to solve it." In *2016 International Conference on Information Communication and Embedded Systems (ICICES)*, pp. 1-6. IEEE, 2016.
- [19] Gunjan, Vinit Kumar; Kumar, Amit; Avdhanam, Sharda, "A survey of cybercrime in India", *15th International Conference on Advanced Computing Technologies (ICACT)*, 2013, pp. 1-6.
- [20] Thangiah, Murugan; Basri, Shuib; Sulaiman, Suziah, "A framework to detect cybercrime in the virtual environment", *International Conference on Computer & Information Science (ICCIS)*, 2012, pp. 553-557.
- [21] Datta, Priyanka; Panda, Surya Narayan; Tanwar, Sarvesh; Kaushal, Rajesh Kumar, "A Technical Review Report on Cyber Crimes in India", *International Conference on Emerging Smart Computing and Informatics (ESCI)*, 2020, pp. 269-275.
- [22] Sajal, Sayeed Z.; Jahan, Israt; Nygard, Kendall E, "A Survey on Cyber Security Threats and Challenges in Modern Society", *IEEE International Conference on Electro Information Technology (EIT)*, 2019, pp. 525-528.
- [23] Gunjan, Vinit Kumar; Kumar, Amit; Rao, Allam Appa, "Present & Future Paradigms of Cyber Crime & Security Majors - Growth Rising Trends", *4th International Conference on Artificial Intelligence with Applications in Engineering and Technology*, 2014, pp. 89-94.
- [24] Govil, Jivesh; Govil, Jivika, "Ramifications of cybercrime and suggestive preventive measures", *IEEE International Conference on Electro/Information Technology*, 2007, pp. 610-615.
- [25] Rok Bojanc and Borka Jerman-Blažič, "Standard approach for quantification of the ICT security investment for cybercrime prevention", *Second International Conference on the Digital Society*, 2008, pp. 7-14
- [26] Sinchul Back, Jennifer LaPrade, "The Future of Cybercrime Prevention Strategies: Human Factors and A Holistic Approach to Cyber Intelligence", *International Journal of Cybersecurity Intelligence and Cybercrime*, 2019, pp.1-4.
- [27] M. Sathiyarayanan, C. Turkay, and O. Fadahunsi. "Design of Small Multiples Matrix-based Visualisation to Understand E-mail Socio-organisational Relationships." In *2018 10th International Conference on Communication Systems & Networks (COMSNETS)*. 2017.
- [28] M. Sathiyarayanan,, and N. Burlutskiy. "Design and evaluation of euler diagram and treemap for social network visualisation." In *2015 7th international conference on communication systems and networks (COMSNETS)*, pp. 1-6. IEEE, 2015.
- [29] M. Sathiyarayanan,, and D. Pirozzi. "Spherule diagrams with graph for social network visualization." In *2016 8th International Conference on Communication Systems and Networks (COMSNETS)*, pp. 1-6. IEEE, 2016.
- [30] M. Sathiyarayanan,, and D. Pirozzi. "Social network visualization: Does partial edges affect user comprehension?." In *2017 9th international conference on communication systems and networks (COMSNETS)*, pp. 570-575. IEEE, 2017.
- [31] M. Sathiyarayanan, and D. Pirozzi. "Linear-time diagram: A set visualisation technique for personal visualisation to understand social interactions over time." In *2016 2nd International Conference on Contemporary Computing and Informatics (IC3I)*, pp. 259-264. IEEE, 2016.
- [32] M. Sathiyarayanan, AK. Junejo, and O. Fadahunsi. "Visual Analysis of Predictive Policing to Improve Crime Investigation." In *2019 International Conference on contemporary Computing and Informatics (IC3I)*, pp. 197-203. IEEE, 2019.