St. Cloud State University

theRepository at St. Cloud State

Culminating Projects in Computer Science and Information Technology

Department of Computer Science and Information Technology

10-2019

An Approach For Detecting Online Dating Scams

Ozkan Kahveci
oj0652kl@go.minnstate.edu

An Approach For Detecting Online Dating Scams

by

Ozkan Kahveci

A Starred Paper

Submitted to the Graduate Faculty of

St. Cloud State University

in Partial Fulfillment of the Requirements

for the Degree of

Master of Science

in Information Assurance

October, 2019

Starred Paper Committee:
Abdullah Abu Hussein, Chairperson
Dennis Guster
Akalanka Mailewa

Abstract

Online dating scam has been rapidly increasing the internet's rapid growth synchronically. However, there is no such tool that is available for the public to use it and prevent online dating scams. In this paper, techniques for scam detection in online dating websites profiles are described. A tool for automatically identifying fake profiles on dating websites such as e-Harmony, OkCupid, match.com is used in this paper. The web application generates a scam likelihood regarding the input profile's description by using the scam action components.

Regarding National Public Radio's news recently, online dating scams had an impact of $143 million in the United States ("Americans Lost $143 Million In Online Relationship Scams Last Year," 2019). This number indicates the link between the number of users that use online dating websites and the number of scams on these websites. The primary purpose of this paper is creating public awareness and alerting users for whom they might be contacting online dating websites.

Table of Contents

Page

Chapter Page

Appendix

List of Tables

List of Figures

Figure Page

Chapter I: Introduction

With today's online world, social networking websites not only change how people look up for information, send or receive, but also the way people interact with each other has been shaped and rapidly evolving in the online world (Fire, Kagan, Elyashar, & Elovici, 2013). That is why many websites offer dating services to match with other users on their websites based on user profile description. People on these websites read biographies of other users and decide whether to interact or not. The existence of reciprocity in these dating websites creates a new challenge to the public as to whether the existing user profile is genuine or suspicious (Whitty & Buchanan, 2016).

An ever-increasing number of Americans are going to dating sites and portable applications in order to find love and fellowship. A Pew Research Center examination uncovered that about 60 percent of U.S. grown-ups consider internet dating a decent method to meet individuals, and Match.com, one of the most prevalent dating destinations, says individuals 50 and more established speak to its quickest developing portion of clients. Be that as it may, looking for sentimental delight online can have a noteworthy drawback: Cyberspace is brimming with scammers anxious to exploit desolate hearts. The con works something like this: You post a dating profile and up pops a promising match — attractive, savvy, smart, and amiable. This potential mate professes to live in another piece of the nation or to be abroad for business or military arrangements. Be that as it may, the person appears to be stricken and anxious to become more acquainted with you better and recommends you move your relationship to a private channel like email or a talk application. Over weeks or months, you feel yourself developing nearer. You make arrangements to meet face to face; however, for your new love, something consistently comes up. At that point, you get a critical solicitation. There is a crisis (a restorative issue, maybe, or a business emergency), and your online friend needs you to wire cash rapidly. The person will guarantee to pay it back; however, that will never occur. Instead, the scammer will continue requesting more until you, at long last acknowledge you have been had. Fake suitors likewise search out focuses via web-based networking media, and they are progressively dynamic. The Federal Trade Commission (FTC) got more than 21,300 reports of sentiment scams in 2018, up 250 percent from three years sooner. Announced misfortunes totaled $143 million, the most for a customer misrepresentation. The more seasoned the person in question, the more massive the budgetary toll, as per the FTC — the middle individual misfortune for individuals matured 70 and over was $10,000, contrasted with $2,600 for all exploited people. The warning signs can be summarized as it is shown below:

-Your new romantic friend sends you an image that looks progressively like a model from a style magazine than a customary depiction.

-The individual rapidly needs to leave the dating site and speak with you through email or texting.

-He or she lavishes you with attention. Swindlers often inundate prospective marks with texts, emails, and phone calls to draw them in.

-The person in question more than once guarantees to meet you face to face yet consistently appears to think of a reason to drop.

Last month, for instance, in the United States a man who was the victim of this sort of trick – he related an assault procedure like that for a situation detailed in Chile in 2018 – in the wake of having met the individual through an internet dating website and picked up his trust, the scammer mentioned the sending of cozy photographs. Soon after they were sent, the victim got a message from a man professing to be the dad of a minor and who took steps to document charges against him for sending a tyke an express picture, except if he sent him two paid ahead of time 'cash cards' with US$300 each. The victim was educated that it was a trick after he had reached the police (“When love becomes a nightmare,” 2019).

Dating services aim to make their users meet in real life and fall in love. However, some websites cater to audiences with a specific ethnic group or cultural background (Huang, Stringhini, & Yong, 2015). Examples are christianmingle.com, lationoamericancupid.com, muslims4marriage.com. Some sites only focus on making people match based on profile descriptions. These services establish a connection between two users, and both scammers and the victim get notified. Once the connection established, the victim is ready to expose personal information (Elovici, Fire, & Gilad, 2015). Also, some dating services already expose user-profiles publicly, and this is another privacy concern. Accordingly, many users publish private information, and it gets exposed more than they thought (Elovici et al., 2015).

A surprising component of online romance scams is that the culprits of this kind of crime depend on strategies intended to make victims act, of their own volition, in manners that conflict with their advantage. To put it another way, not at all like some other digital crimes, for example, fraud, an online romance scam is just fruitful to the degree that a scammer can influence a victim to complete solicitations. This may help clarify why numerous victims have announced they censure themselves for what happened, and that, instead of getting support, they have been met with displeasure from relatives and others (Whitty and Buchanan, 2012b). However, what might make an individual comply with the solicitations of a scammer who might be found hundreds, or even a great many miles away?

Analyst Robert Cialdini has distinguished six mental standards regularly abused by those looking to pick up the compliance of others. Cialdini has talked about these standards finally in his milestone book Influence: The Psychology of Persuasion, first distributed in 1984 and later reexamined in 2007. Throughout the years, this book has turned out to be required perusing in many showcasing courses and has additionally been retooled into a school reading material, presently in its fifth version. The compliance standards laid out by Cialdini might be a valuable system inside which to comprehend the extraordinary impact culprits of online romance scams have over their victims.

Intention to keep the family name alive continues from the first time of existence of humans until now. Even though dating scams existed in the past when there was no internet, it became so comfortable with today’s technology. When we consider why scams exist in the online dating world, the financial number is the motivation behind these scams. In 2012, the online dating market value was 1.9 billion dollars (Kopp, Layton, Sillitoe, & Gondal, 2016). This market value attracts scammers for financial gain. The romance scam is being fed by vulnerable people who are desperately seeking for partners online. Also, some dating websites claim that they have over 15 million members registered, so this is a perfect amount of population for scammers (Huang et al., 2015). Even though simple scams such as 419 scams still exist on these websites, advance scammers find different methods to attract emotionally vulnerable people (Huang et al., 2015). 419 scam is in which scammers ask for money to build trust with their victims (Huang et al., 2015).

In the United States, regarding all single users who are looking for a partner, 17.000 scams have been reported in 2017 (“Americans Lost $143 Million In Online Relationship Scams Last Year,” 2019). Since Facebook, LinkedIn, and other social networks offer a look-up option for existing users, dating websites only recommend profiles for users to read (Wani & Jabin, 2017). While online dating services focus on how to find a better way to match their users, they are not paying enough attention to protect their users. The scam gab is getting bigger and bigger while the online dating industry is also growing fast. Thus, improving user recommendations will potentially help to find an eventual partner to meet in real life.

Problem Statement

Since online dating websites are not capable of verifying every user profile for existence, a fake profile can be created easily for hostile intentions.

Nature and Significance of the Problem

Online dating fraud is highly successful, which causes reasonable financial and mental damage to its victims (Whitty & Buchanan, 2016). In 2019 February NPR reported that people lost 143 million dollars because of online dating scams (“Americans Lost $143 Million In Online Relationship Scams Last Year,” 2019). This study will help to improve the understanding of online dating possible scam situations.

Objective of the Study

This study will help the public to identify fake profiles on dating websites.

This study aims to create an environment where the users are more aware of possible scams.

Study Questions/Hypotheses

Is there any software available for the public to identify the fake profiles on dating websites?

What are the potential benefits of using this software for the users?

Hypotheses 1: There are no applications available to alert users for fake profiles on dating websites.

Hypotheses 2: The software created by the researcher will aid the users to recognize if the user on the other side is a scam or not.

Summary

In general, considering the previous researches, online dating security has not been deeply researched, and this has caused both financial and mental impacts on victims. Since the online world is expanding every other day, it brings more challenges with itself. People not only look for the information they need but also look for partners that are single and looking for relationships. This intention opens a gate for scammers to exploit this new service as a financial gain. While the scammer uses this hole, scammers also leave prominent scars both financially and mentally on their target. This study focuses on how to improve the safety of online dating users against scammers on these websites. It also tries to answer if there is such a software that identifies fake profiles on dating websites. The hypotheses are shown below:

Hypotheses 1: There are no applications available to alert users for fake profiles on dating websites.

Hypotheses 2: The software created by the researcher will aid the users to recognize if the user on the other side is a scam or not.

The next chapter will focus on the background of online dating scams and existing studies that are related to online dating services.

Chapter II: Background and Review of Literature

Introduction

In this chapter, background related to dating scams and its impacts on users will be briefly explained. This brief explanation will include several reports and studies why online dating scam is such a huge problem. The next part of this chapter will include the studies that suggest a solution to online dating scams. Suggestions will have two sections. The first section will be a tool, and the second section will try to explain how this tool will be useful to prevent the online dating scam issue.

The last section in this chapter will compare the methodologies that were used before the solution of this study. It will briefly explain if the methodology that this study will offer was used in past studies. Then the previous methodologies will be analyzed why they are not useful anymore with current industrial scam techniques.

Background Related to the Problem

Violations submitted utilizing PCs, and the Internet has turned out to be omnipresent in ongoing decades. From very complex system interruptions to the most low-tech digital stalking cases, the media is pervaded with tales about how the Internet is utilized by offenders to take cash and data, launder cash, and carry out different wrongdoings. A standout amongst the most worthwhile territories of cybercrime includes online tricks, as prove by the way that, in 2015 alone, the Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center got protests totaling over $1 billion. Tricks executed over the Internet can target associations or people and may take on a large assortment of structures. Nonetheless, of all cybercrimes answered to the

FBI in 2015, the second most elevated measure of misfortune was credited to a classification of extortion that solely targets people: "Certainty Fraud/Romance" (ICCC, 2015, p. 16). Exasperatingly, proof proposes unfortunate casualties might particularly underreport this sort of misrepresentation, and that the genuine money related effect of this wrongdoing is far more prominent than what is shown by authority sources (Whitty and Buchanan, 2012a).

In any case, not at all like with numerous different scams, victims of online sentiment scams lose unmistakably more than cash. Victims of this kind of scam are mentally maltreated, frequently for quite a long time or even years. Victims have revealed encountering harm to connections and being left grief-stricken, humiliated, and profoundly embarrassed (Whitty and Buchanan, 2012b). During the ongoing preliminary of a sentiment scammer (who was eventually sentenced for duping victims of over $1.7 million), victims affirmed they had petitioned for financial protection, lost occupations, homes, and had been exposed to extraordinary money related hardship. Past their monetary misfortune, victims affirmed they had fallen into discouragement and, now and again, had mulled over suicide. A few victims even affirmed that they were explicitly mishandled, and later extorted utilizing naked photos of themselves. The irritating subtleties of the case, which included several victims, incited the judge who directed the case to allude to the scam as "the most destroying crime one would ever envision without laying hands or even eyes on another individual" (DOJ, 2017, standard. 10).

The number of online dating services is increasing rapidly, and the market is expanding more and more. However, the damage is spreading rapidly because of the lack of security in the online dating world. It is creating irreparable both mental and financial damages on its victims. In 2011, the Melbourne Herald Sun newspaper reported that Australians lost $21 million to online dating scams (Kopp et al., 2016). In 2012, a study showed that 230,000 individuals had been scammed by online dating services in England (Whitty & Buchanan, 2016). This year in 2019, National Public Radio announced that Americans lost 143$ million because of online dating scams. The numbers indicate how a single service on the internet can have an enormous impact on users.

The increasing numbers of scams make users question their security on dating services. However, there has not been such a method found to solve this issue. The complexity of online dating services is evolving every other day; however, the security of these services is getting lower. Simple theory in cybersecurity says that complexity and security are inversely proportional. In another saying, while the complexity of application increases, the security of the application will go down. So, it is always important to find the balance and keep updating the application towards that balance. Considering the services that are available for online dating, the financial loss shows that the balance policy has not been being applied to their services. The gap is increasing with every other update, and unfortunately, most updates' information shows that the application has almost none enhancements towards security.

The lack of security in online dating platforms not only harms financially, but it creates severe mental harms. All a sudden, being left alone by someone who declared love for you leaves deep cuts emotionally. Studies have shown that some victims experienced dominant depressive thoughts, and some even experienced suicidal thoughts (Whitty & Buchanan, 2016). A report by the Office of Fair Trading in the United Kingdom has shown that the scam victims lose trust, confidence, and experience damaged self-esteem and a reduced sense of self-worth (Whitty & Buchanan, 2016).

Endeavors have been made to comprehend the advanced wonder of Internet-based scams from various alternate points of view. One methodology has been to attempt to decide the commonness of the problem, by either attempting to learn the number of victims or the number of fraudulent sales. For example, a study directed by the Federal Trade Commission (FTC) found that 10.8 percent of U.S. grown-ups had been the victim of some fraud in 2011. In about 33% of these cases, the Internet was referred to as the methods by which the scam was at first advanced (Anderson, 2013). Another study, which required more than 2,300 subjects matured 40 and more established, found that 80% of respondents had been the objective of a fraudulent offer and that the Internet was the most significant single wellspring of these offers (Report On FINRA, 2018).

Concerning online romance scams explicitly, the FBI has announced that, in 2015, its Internet Crimes Complaint Center got 12,509 objections identified with "Certainty Fraud/Romance" scams (ICCC, 2015). In any case, others have recommended information, for example, these, who are needy upon victims' self-detailing, may significantly under mirror the true extent of the problem. For instance, a British study directed by Whitty and Buchanan (2012a) included asking subjects "whether they had lost cash or knew somebody by and by who had lost cash to an online romance scammer" (p. 5). These discoveries, because of a delegate test of grown-ups in the United Kingdom, have driven Whitty and Buchanan (2012a) to gauge that more than 230,000 British natives may have been victims of online romance scams somewhere in the range of 2008 and 2011. This number is far higher than those self-detailed by victims to purchaser insurance organizations in the U.K. during a similar period (Whitty and Buchanan, 2012a).

In the United States, there are various progressing endeavors to gather the information that incorporates data identified with the fiscal misfortune continued by victims of scams. For instance, since 1997, the FTC's Consumer Sentinel task has gathered buyer grievances of different sorts, including those identified with scams. Somewhere in the range of 2013 and 2015, more than four million of these grievances identified with fraud, with shoppers announcing over $4.1 billion in misfortune. Of fraud-related grievances, 31% of victims showed that the Internet or email was the technique by which they were at first reached by fraudsters (Fletcher, 2019). The FBI additionally gathers data explicitly identified with Internet-based crimes through its Internet Crime Complaint Center. In 2015, the FBI announced that "Certainty Fraud/Romance" spoke to the second-biggest fraud type by victim misfortune, with victims answering to have lost over $203 million. By and large, victims of this sort of fraud announced lost $16,260 (ICCC, 2015).

One more way to deal with the study of this point has been to investigate the conceivable hazard variables related to the victims of these sorts of scams, as well as to endeavor to all the more likely comprehend victim defenselessness to influence systems utilized by fraudsters. For instance, a study led by the AARP recognized critical contrasts between the degrees of instruction and salary of victims of various kinds of scams. For instance, victims of venture scams were observed bound to be school instructed and to report a payment of $50,000 every year or more noteworthy. Alternately, victims of lottery scams were found to have no school training, and to report a salary of under $50,000 every year. The study additionally inspected respondents' helplessness too many advertising style questions and found those 50 years and more seasoned were "fundamentally progressively inspired by the influence articulations generally speaking" (Pak and Shadel, 2011, p. 38). Concerning online romance scams, a progression of studies led by Whitty and Buchanan (2012b) have recommended that men (regardless of whether hetero or gay) might be almost certain than ladies to move toward becoming victims when utilizing an internet dating webpage. Whitty and Buchanan (2012b) have likewise noticed that victims of online romance scams will, in general, report they became hopelessly enamored rapidly, in contradistinction to studies exhibiting most genuine sentimental connections develop all the more gradually. This has driven them to conjecture that numerous online romance scam victims are "profoundly energetic to begin to look all starry eyed at, possibly leaving them helpless against being scammed" (p. 11).

Another zone of the center has been to attempt to recognize the wellspring of Internet-based scams: who the culprits are, and where they are physically found. Longe and Osofisan (2011) have challenged the generally held conviction that most development charge scams begin from West Africa, given a study of IP locations related to scam messages. The study, which consolidated a sizeable level of messages named "dating spam," found that countless scam messages started from spots outside West Africa, for example, Europe and North America. Nonetheless, Longe and Osofisan (2011) have recognized their study did not involve researching whether this example "is related to the number of volumes of Africans, Asians and other settlers' moving into the [sic] western countries" (p. 24). Others have reasoned that a superabundance of Internet-based scams executed outside West Africa is, all things considered, executed by West African-based scammers. For instance, Ultrascan (2014), a Dutch security firm that gathers and breaks down information identified with development expense scams, has noted West African culprits of development charge fraud (regularly alluded to as "419", in reference to an area of the Nigerian reformatory code) have relocated all through the world as of late: "There are 419 cells in about each nation on earth... 419er tasks are on the uptick in China (both territory China and Hong Kong), and in Malaysia. There are 419er cells in the USA, Canada, Mexico, Ghana, Brazil, Egypt, Russia, India, Pakistan, and the Czech Republic" (Ultrascan, 2014, p. 15). Online romance scams, which Ultrascan (2014) thinks about a variety of customary development charge fraud, are one of the scams routinely executed by West African scammers working throughout the world.

Due to the lack of security in online dating platforms, people have been suffering during their journey to find happiness. Past and recent researches prove the dating scam impact on its victims is such a big problem in the online world.

Literature Related to the Problem

Fire claimed that Facebook is filled with tens of millions of fake user profiles (Fire et al., 2013). The reason behind this is that Facebook does not pay enough attention to its users' privacy. The proposed solution was a tool to identify fake profiles. This tool is labeled as "Social Privacy Protector software for Facebook." The software has three security layers to improve security. The first layer focuses on users' friends' list and identifies who might pose a threat and restricts the personal information (Fire et al., 2013). The second layer focuses on basic privacy settings, such as what is available to the public (Fire et al., 2013). Third and the last year focuses on third-party applications that use personal data on Facebook (Fire et al., 2013). More than 3.000 users downloaded the tool and restricted over nine thousand friends (Fire et al., 2013). It also removed 1,792 Facebook applications from their user profiles (Fire et al., 2013).

The methods that were used by Fire are persuasive regarding 2013. Analyzing the personal data, analyzing Facebook's privacy settings, and the Facebook applications that use personal data techniques are very accurate ways to detect fake profiles. However, Fire stated that their applications ran into too many false-positive flags. Private settings and the data set that was used for machine learning were not accurately set. Thus, the accuracy of this suggested tool was not very successful in detecting fake profiles on Facebook.

In 2014, Radford questioned the service of E-Harmony. E-Harmony is another different type of dating service that uniquely claims itself in the industry. This service states that they use science, and they have researches work for their services to make online dating easy and convenient (Radford, 2014). These scientific statement goes as “developed by a team of clinical experts …l is rooted in classical psychometric theory – which uses well-established standards to measure mental abilities and traits reliably.” (Radford, 2014). Radford thought that these services make direct and explicit claims about the scientific validity of its matching algorithm (Radford, 2014). It was so strange that e-Harmony did not have any reference regarding their scientific claims. Throughout his research, Radford demanded these studies from e-Harmony. Radford found that the website was not able to provide any research regarding their service. Later senior research scientist Gian Gonzaga from e-Harmony claimed that the methods that e-Harmony uses are secret and cannot be published at Society for Personality and Social Psychology conference (Radford, 2014). He tried to offer evidence from non-peer-reviewed studies.

Regarding Radford’s results, e-Harmony is another marketing way to get people to register, and this is a scam. Radford calls this “Sweet Science of Scam,” and their methodologies cannot be trusted fully without clear evidence.

Given that the casualties of online sentiment scams consent to collaborate with the solicitations of scammers, it might be anything but complicated to embrace an unfeeling mentality toward the individuals who have fallen prey to this sort of wrongdoing. In any case, the way that these scams are so pervasive thus fruitful proposes it is not right to property the activities of exploited people to ineptitude or guilelessness. Instead, an exertion ought to be made to comprehend why the strategies utilized by online sentiment scammers can make exploited people act in such extraordinary ways. By lighting up how sentiment scammers endeavor known mental shortcomings, it might be conceivable not just to grow better methodologies toward alleviating this sort of wrongdoing yet likewise to advance more compassion toward exploited people.

Cialdini has sketched out six mental rules that are frequently misused by individuals looking to pick up the consistency of others, regardless of whether for real or ill-conceived purposes:

Reciprocation: Individuals are bound to agree to a solicitation when they feel a feeling of commitment or obligation toward the requestor. This feeling of commitment might be accomplished through giving little endowments or doing apparent favors for somebody yet may likewise be cultivated through mutual concessions: beginning with an enormous solicitation, at that point countering with a nearly littler solicitation when the first is rejected. This uses the inclination for individuals to feel a "commitment to make an admission to somebody who has made an admission to us" (Cialdini, 2007, p. 37).

Commitment and Consistency: In the wake of making an underlying responsibility, individuals regularly feel compelled to keep on acting as per that dedication, to "legitimize [their] prior choice" (Cialdini, 2007, p. 57). Individuals will, in general, adjust their mental self-view to responsibilities they accept they have made, mainly when those duties are recorded, recorded, or officially made. This inclination is particularly robust when an individual accepts the person has made a responsibility "without solid outside weights" (Cialdini, 2007, p. 93).

Social Proof: Individuals are bound to think about conduct as typical and to take part in that conduct if there is a recognition that others are doing likewise.

Liking: Individuals are increasingly inclined to consent to the solicitations of somebody they like. Enjoying can be accomplished through any number of methods, yet frequently incorporates engaging a physical quality, developing a feeling of "equivalence" (individuals will in general like individuals they see as being like themselves), compliments, nature, and building up a feeling of universal participation toward a mutual objective.

Authority: Consistency is simpler to get when it is seen that the requestor is in a place of power. This standard was maybe most broadly shown by Stanley Milgram's acquiescence tests.

Scarcity: Individuals are regularly impacted to settle on choices dependent on the dread of losing an apparent chance. The view of shortage makes a feeling of direness, prompting blunders in judgment when individuals react by settling on choices rapidly. This rule owes a lot of its solidarity to an idea known as mental reactance: "...whenever a free decision is constrained or undermined, the need to hold our opportunities makes us want them... altogether more than already" (Cialdini, 2007, p. 245).

Eloivici proposed a method for detecting spammers and fake profiles in social networks by using supervised learning. Supervised learning can be described as machine learning to simplify. Eloivici created different data sets regarding fake and legit profiles. The invention did not target a specific social network platform. The illustrated profiles were tested on different platforms such as Google+ and MySpace (Elovici et al., 2015).

Eloivici set 4 different nodes to be extracted for each user. These nodes are:

a) the number of friends of the user

b) the number of communities the user is connected to

c) the number of connections between the friends of the user; and

d) the average number of friends inside each of the user’s connected communities (Elovici et al., 2015).

Eloivici claimed that if the user has friends from different communities and the user’s friends list contains friends less than an average user has; these can be considered as red flags to identify the profile as fake. Later Eloivici simulation of these techniques in different platforms with different sizes of data sets indicated that the invention could identify fake profiles. However, Eloivici had only illustrations with limited data sets and specific steps to identify the spammers and fake profiles in social networks.

Huang stated that with one in five relationships in the United States starting on one of these dating websites (Huang et al., 2015). In this manner, the attention on these websites increased by cybercriminals and scammers. Huang had different methods to identify scammers comparing to previous ones. First of all, Huang used large-scale data to study instead of using illustrations or small-scale data. The methodologies that were suggested by Huang can be categorized into four different sub-categories:

1) Behavioral-based Detection
2) IP Address-based Detection
3) Photograph-based Detection
4) Text-based Detection (Huang et al., 2015).

The other difference between Huang's study was the timeline. The study was performed for eleven months to aim for better accuracy.

Huang's first methodology was focused on behaviors from scammers. While the real people wanted to seek out for others and start a relationship, scammers had different behaviors. This methodology analyzes the time scammers take to respond or send the first messages, and also it analyzes the number of conversations that are held by scammers simultaneously (Huang et al., 2015). The behavioral system mechanism shows similarity to the anti-spam system that is proposed by the research community (Huang et al., 2015).

The second methodology that was proposed by Huang was an IP address-based detection system. If a scammer created different profiles by using the same network, this indicates serious attention as a red flag for the detection system (Huang et al., 2015).

The third methodology is focused on the profile photos that are used by scammers. The studies show that scammers use the same photo over and over (Huang et al., 2015). These photos usually are an attractive young woman or a handsome middle-aged man (Huang et al., 2015). The detection system deploys a system that detects duplicated photos and flags those as malicious activity (Huang et al., 2015).

The last method is called a text-based detection system. This system checks if the same message was sent to different users over and over. This is actually how spam detectors work, and Hu describes that scammers use the same method also in online dating websites.

Hu analyzed the application market for dating applications in China. Since the Google play store is not available in some parts of China, the different application markets were also included in the research. Over 2.5 million applications in the application market, 967 dating applications were found for dating purposes (Hu et al., 2018). The analysis shows that significant numbers of people downloaded these applications. Later Hu dived into the applications they found and analyzed it. Hu presently endeavor to distinguish fake accounts from another perspective, i.e., the collaboration patterns. On the off chance that the accounts are genuine people, at that point, the messages ought to be significant to the subject of the discussion. In this manner, Hu play out a field concentrate on investigating the communication patterns of these fraudulent dating apps. For every family, Hu arbitrarily pick an application and introduce it on a genuine gadget. At that point, Hu register two accounts (1 male client and one female client) to sign in and begin a discussion. Moreover, we buy the premium administration for each application and analyze the outcomes when obtaining their administrations.

Regarding China’s population, a total of 967 applications was downloaded over a billion times (Hu et al., 2018). Hu and his colleagues also analyzed the reviews on these applications for each different application market, and the results were also showing that most of these applications that had over 100k reviews and most reviews were fake. Not only the reviews were fake, later Hu selected random applications among these 967 dating applications. The signatures on these applications were mostly similar, and that showed that the same developer distributed these applications into different markets with different names and different company titles (Hu et al., 2018). Hu's researches also identified that the applications were mostly targeting fake young beautiful women profiles. The responses were not related to the topic and some applications on the market required to purchase VIP or premium membership to respond to the messages (Hu et al., 2018). Hu purchased the premium membership to take a further analysis step. The total cost of 22 memberships was 176 US dollars. The research identified that once the premium was purchased, the victim was able to respond; however, the bots stop responding. Therefore, the entire point on these applications was to convince victims to purchase. The accumulated revenue estimated for these applications that were conducted in research was around 200 million US Dollars to 2 billion US dollars.

Dating websites are closely related to fake profiles on social networks such as Twitter, Facebook, and Instagram. So, Wani dives into different methods to identify fake profiles on social networks. Wani also compares the cloned profiles and fake profiles and their different intentions on scam levels. Wani gives a thorough characterization of various real and ghost profiles with an accentuation on informal online organizations. Compromised accounts are in reality official accounts; however, their proprietors do not have extensive oversight over these, and they have lost the control to a phisher or any malware specialist. As per an investigation, compromised accounts are the most troublesome sort of accounts to be identified. Another ongoing examination says over 97% of profiles are compromised instead of fake. The fake profiles are, for the most part, made to take the accreditations from genuine clients, and after that, fake profiles are deserted or deactivated.

Compromised profiles have much worth since they have officially settled a dimension of trust inside their system and in this manner, cannot be adequately recognized and expelled by the specialist co-ops. Assailants, for the most part, use compromised profiles with critical consideration to use the dimension of trust. The writers have exhibited a way to deal with distinguishing compromised accounts from two mainstream online person to person communication destinations, Facebook and Twitter, by recognizing profiles that show unexpected changes in the conduct by utilizing measurable demonstrating and peculiarity recognition. Facebook has a framework to recuperate hacked accounts once announced. There is an alternative "my account was hacked" on the Facebook help page. One more examination uncovers that the compromised genuine profiles spread more noxious substances than different kinds of fake profiles (Wani & Jabin, 2017). Profile cloning is the burglary of personality from a current user's profile and to make another fake profile utilizing stolen accreditations (Wani & Jabin, 2017). We can say that profile cloning is the way toward taking the injured individual's private data to make one more profile that can secure the private data of unfortunate casualty's companions. These assaults are called Identity Clone Attacks (ICAs), which are of two sorts of profile cloning assaults to be specific single site and cross-site profile cloning. The scammers are generally very much financed, talented people and have nearly everything accessible available to them and have authority over bargained and contaminated records (Wani & Jabin, 2017).

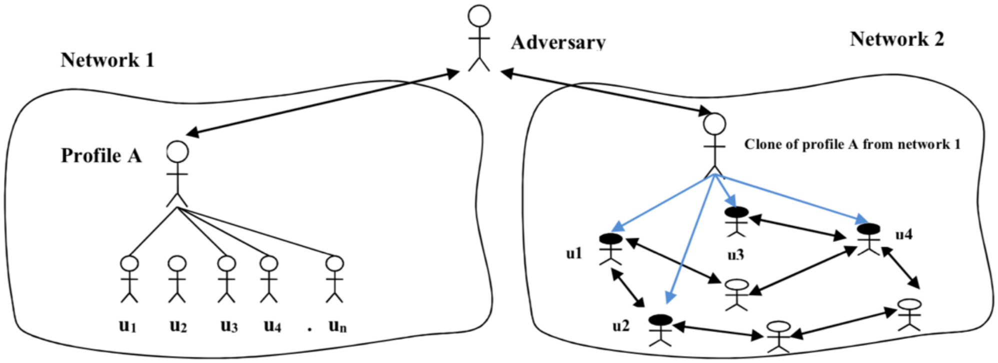


Figure 1: Intersite or Cross-Site Profile Cloning (Wani & Jabin, 2017)

Fake profiles are not quite the same as cloned ones from various perspectives. If there should be an occurrence of cloned profiles, an enemy makes one more profile of the effectively existing one, which is not the situation for fake profiles. Cloned profiles are, for the most part, made to extricate the data of an injured individual or his/her companions through the fake profiles are utilized for different purposes like spamming, promoting, and so forth. A few people make fake profiles to have one more account, while some make numerous accounts intentionally to go into individuals' sub-charts. There are two different ways to make fake profiles: one is made by composing content, and another is by physically making one more account.

What is more, there are three fundamental purposes behind making fake profiles: First, Online Social Network specialist co-ops permit one account for every versatile association or per email-id, and to defeat this farthest point, individuals make one more account utilizing diverse email-ids or telephone numbers. The second is to improve the ubiquity or the dimension of trust among the others. The third is to spread spam content among the genuine users. Fake elements exist wherever on the web like long range interpersonal communication websites, shopping sites, exchange sites and gatherings, web-based dating websites, banking frameworks, and so on. Furthermore, there is still a need to fortify safety efforts being utilized by online informal community sites to lessen editing fake profiles and to keep away from their dangers on interpersonal organizations. Fake profiles are destructive for OSNs and can be progressively hazardous in the future if not distinguished at the beginning period.

A bot is a computer program that delivers a few information to connect with people, particularly the people utilizing the web (netizens) to change their conduct. Bots produce over 60% of the complete web information. Online bots otherwise called web robots or basically, a bot is a computer program that performs different assignments rapidly and consequently, which were impractical for a human alone. Necessarily the bots were intended to help the people to accelerate their work and make it programmed. The first job of bots was to naturally total substance from different news sources, function as a programmed responder to customer inquiries, go about as a therapeutic master to determine wellbeing related issues, and programmed travel control. Be that as it may, these days, the bots are abused by the general population in different spaces. In informal organizations, bots are utilized to retweet a post without checking its source to make it viral. In online multiplayer diversions, bots are utilized to pick up the uncalled for the preferred position. Now and then, bots go about as computerized symbols to interface with people and make informal communities, which are much progressively hard to distinguish. Bots can likewise be utilized to impact users, presenting messages, and on send companion demands in informal online organizations.

Additionally, the gathering of individuals/association who are probably going to get influenced by the interruption of these personalities were likewise referenced in the table. From the practical perspective, bots are comparative as Sybil accounts, yet the principle contrast is that Sybil accounts are taken care of by users physically while bots are mechanized computer programs. The principle utilization of bots is web information slithering where a straightforward online computer program recognizes and separates the data from web servers at a lot higher speed, which was unrealistic by a human alone. Bots intended for malevolent exercises have turned into a genuine risk for the web. Different OSN specialist co-ops utilized a few different ways to battle the spambots. For instance, Twitter and Facebook have included an alternative "report as spam" to recognize a spam bot.

Facebook additionally has its Facebook Immune System (FIS) to manage such issues. At the same time, the exploration in this area is in its beginning times. Users in different OSNs guarantee that the discovery systems are getting their official accounts. As per an examination, over 8% of bots exist in Twitter organize. The more significant part of them has been created for business purposes. Bots can be of two sorts generous and harmful.

Police in the southern area of Guangdong, China have busted large rings of web-based dating scammers who acted like appealing ladies to cheat men into purchasing expensive tea and different items, Guangzhou Daily reported (2018). Nearby police reported at the preparation that they had broken 13 packs and caught 1,310 suspects (Sixth Tone, 2018). Each pack could approach up to 1,500 unfortunate casualties for every month, as their individuals would lure numerous men all the while. "These scam packs [succeed] because they catch the brain science of numerous men: When confronting lovely ladies, men lose their judgment, and feel too timid even to consider refusing," a Guangdong cop said at the preparation. As per the police, the possess utilized models' photos and the People Nearby capacity on WeChat, China's most common informing application, to bait unfortunate casualties into visiting. Following quite a while of structure up trust, they would cheat their "beaus" by utilizing anecdotal family disasters as stratagems to advance tea, wine, or interest in valuable metals through a stage constrained by the gathering. One long con included homegrown tea. Police clarified that the groups had built up a 60-day recipe for extortion: The scam specialists would go through 15 days calmly visiting, five days pushing the relationship into a sentiment, and 20 days demonstrating the beau that they had gone to deal with a weak granddad in the place where they grew up, where they were likewise figuring out how to deliver tea. The pack even enlisted models in hot jeans to posture for photographs and recordings in southeastern China's Yunnan region, one of the nation's outstanding tea-delivering areas. The scam would achieve its peak over the most recent 20 days when the beau would be more than once influenced to purchase costly tea leaves. When the objective acknowledged he had been had, he would get blocked. As indicated by Guangzhou Daily, the vast majority of the scalawags were recent college grads, while others were "moderately aged uncles who got a kick out of the chance to pick at their feet." Some systems sold tea, while others utilized tobacco, liquor, wellbeing items, or even oil depictions as their lure of decision. Many individuals have been captured for partaking in web-based dating scams in China. In 2017, police in eastern China's Zhejiang area busted a task that had utilized photographs of lovely ladies to draw exploited people into lotteries constrained by their ring. Another case in northeastern China's Liaoning region in 2016 saw 500 suspects captured.

Here is a real online dating scam story based in Australia. (Commission, 2015) Georgina’s children signed her up to Facebook and gave her some basic lessons on how to use it.

‘They told me everyone was using it and that it would help us keep in touch and see photos of my grandchildren.’ One day Georgina received a friend request from a serviceman on peacekeeping duties in Afghanistan. She decided to accept the request and allowed 'Jim' to be her Facebook friend. It did not start as a romance, but he said he was lonely and looking for friends to keep him company while he was stuck on duty in the middle of nowhere. Soon after befriending her, Jim told Georgina he had lost his wife to cancer, and his story of looking after her was similar to her own experience when her husband had died of cancer. ‘He then said he was being posted to Nigeria, but his time in the U.S military was nearly finished. He sent me pictures which I now know were stolen from someone on the internet. He kept saying he could not wait for us to be together. We became very close, and he emailed me every day, saying it was easier for him than using Facebook.’ Jim, who was a scammer, told Georgina he liked gemstones and wanted to set up a jewelry store when he retired. He said this was the best part of being in Nigeria because it was close to where the precious stones were being mined, and he could buy them very cheaply. He told Georgina he was coming to see her but had some trouble with his bank card not working in Nigeria and could not get funds to pay for an export tax on his gemstones. Georgina transferred some money to him to cover the tax, which he explained was only two percent of the value of the gemstones but still amounted to $15 000. It was much money to send, but she figured he was a right and honest serviceman, and if things worked out, they would spend the rest of their lives together. ‘All was going well until his stopover in Malaysia. Customs officials seized the gemstones and demanded payment to have them released. This time they were asking $20 000. I told him it would take some time to get the money, and I had to borrow against the family home.’ Georgina sent the money to Malaysian officials but was told Jim was now in jail for smuggling and that she needed to contact his lawyer. ‘The lawyer said he needed to get an Anti-terrorism and Money Laundering certificate, and this would be another $10 000. He said he also needed to pay for Jim’s court costs plus his fees, and this would be another $5000.’ Georgina sent the money, but then Jim said there was another government official demanding payment to extend his visa while he waited for the court to process all the documents. ‘Almost every day, I was contacted with a new demand for money. They sent me certificates signed by officials, forms to fill out, and bills for everything. If you wanted to get anything done quickly, you had to pay another fee. It seemed to me that the whole Malaysian government was corrupt. I do not know exactly how much money I sent, but it was well over $100 000. I did not care about money. I just wanted to help Jim, and I honestly thought he would pay me back.’

Even when Georgina ran out of money, the demands didn’t stop. Unsure of what to do, Georgina finally talked to the police. They explained that her experience included the characteristic features of a dating and romance scam, and it would be implausible she would get her money back. She cannot help feeling in her heart that she let Jim down, but she knows that it was all a scam.

Literature Related to the Methodology

Scam techniques on dating websites have been evolving while there is no such free tool that is available to prevent their impacts on society. The methodology that will offer the solution for this issue has two techniques to identify possible scam activity.

The first technique will focus on user profiles’ description and look for keywords that are previously identified based on past researches. This methodology will be called keyword matching. Whitty (2016) identified that if a user indicates that he is in the military or outside the country, that is a red flag for scam activity. Also, NPR indicates that if a user is acting like he or she is in love with the person they have not met in real life, it is a red flag. Not common grammar errors or errors in idioms will also indicate such a scam activity. The text-based methodology will focus on these matters and will add the total red flags in the scam likelihood.

The second methodology will scan for profile photos. If a photo that is used in the profile is public, this will indicate that the user profile is not real and designed for scam activities. The tool will compare the public database and the user profile and will generate a result. Scammers usually create a profile by using a handsome male or female public photo. The public profile that is identified on a profile will add another level into scam likelihood. This method will use different approaches to achieve the goal. The first approach will be using Vision API. Then as a second approach, Vision API will be integrated with Cloud Auto ML Vision. As the third approach, Vision API, Cloud AutoML Vision will be integrated with Google Cloud Platform (GCP). Vision API is powered with Google's deep learning models and provides:

-Face and landmark detection

-Explicit content detection

-Label detection

-Optical Character Recognition (OCR)

AutoML gives the option to train the application for custom label detection using Google's Neural Architecture Search and state-of-the-art transfer learning.

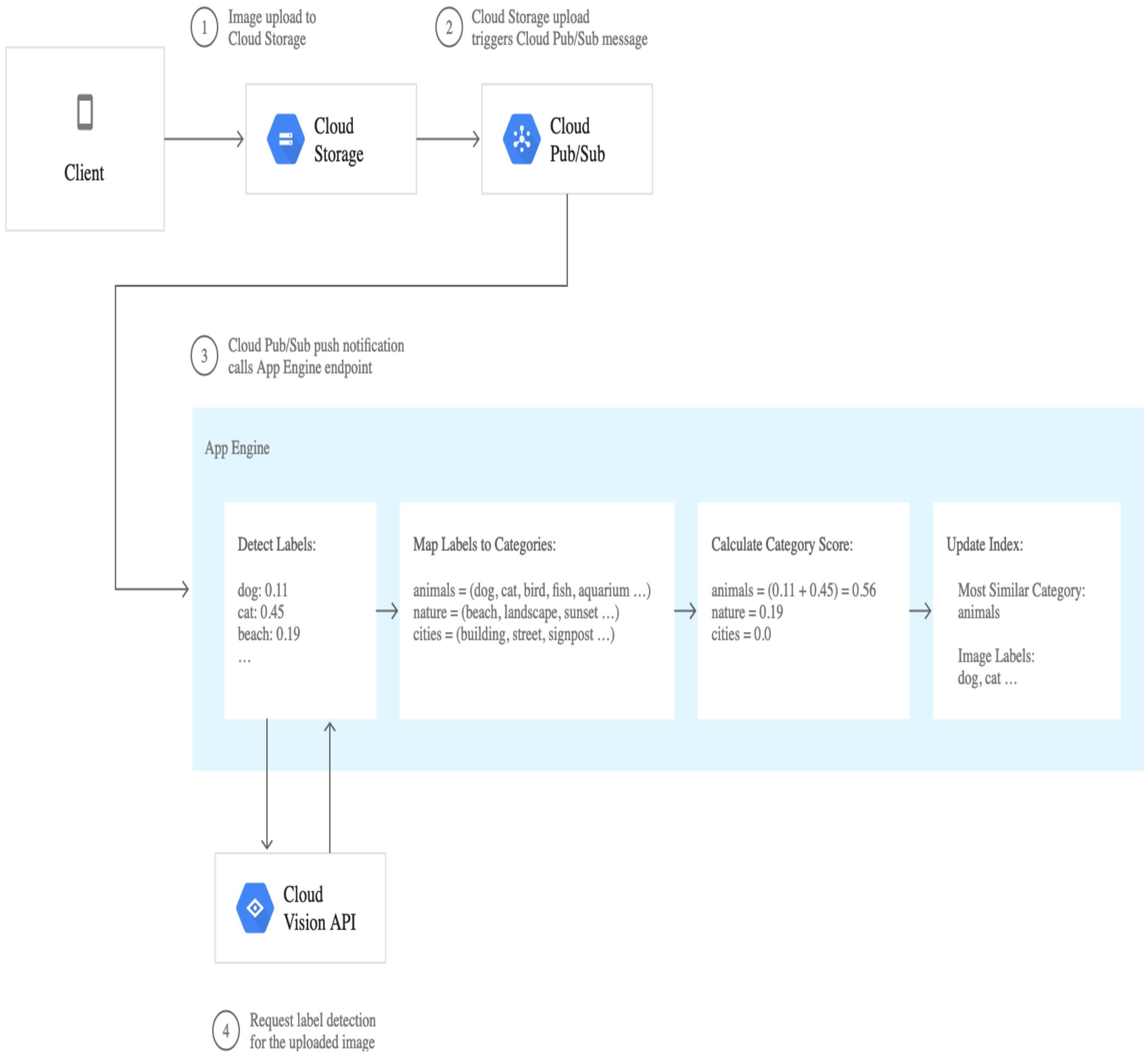
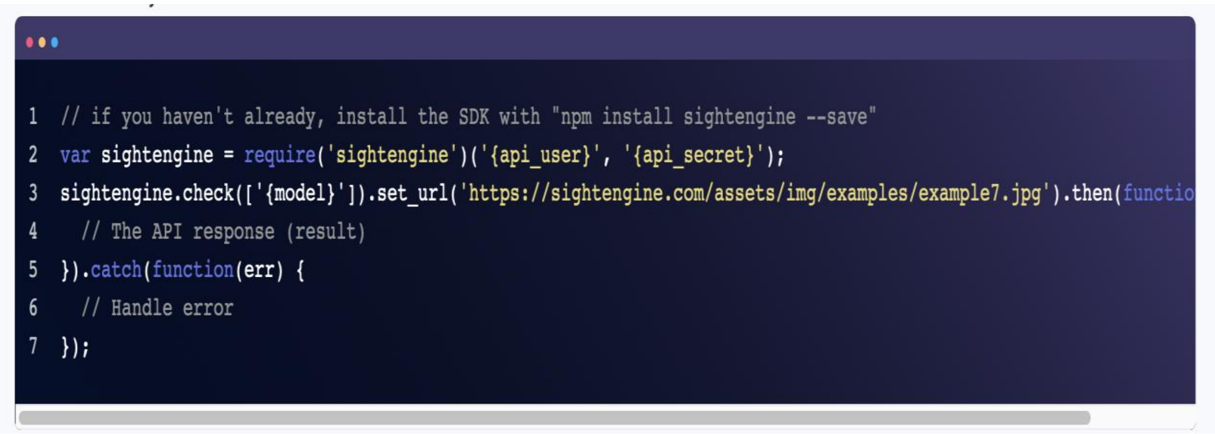

1 Image upload to Cloud Storage
2 Cloud Storage upload triggers Cloud Pub/Sub message
Client
Cloud Storage
Cloud Pub/Sub
3 Cloud Pub/Sub push notification calls App Engine endpoint
App Engine
Detect Labels:
dog: 0.11
cat: 0.45
beach: 0.19
…
Map Labels to Categories:
animals = (dog, cat, bird, fish, aquarium …)
nature = (beach, landscape, sunset …)
cities = (building, street, signpost …)
Calculate Category Score:
animals = (0.11 + 0.45) = 0.56
nature = 0.19
cities = 0.0
Update Index:
Most Similar Category: animals
Image Labels: dog, cat …
Cloud Vision API
4 Request label detection for the uploaded image

Figure 2: Vision API (Google)

Another image scanner API is called sightengine. This API was created with over 40.000 references to detect images that are commonly used in romance scams. The scam discovery motor works by perceiving appearances of individuals known to be utilized in scammer profiles. So regardless of whether a given picture of such an individual is new and obscure to our database, we will almost certainly hail it. The API was developed to detect nudity, celebrities, minors, image quality, artificial texts, weapons, alcohol, offensive & hate signs, face detection, scammers, and faces hidden with sunglasses. Here is an example of the use of sightengine API for detecting celebrities in profile photos.



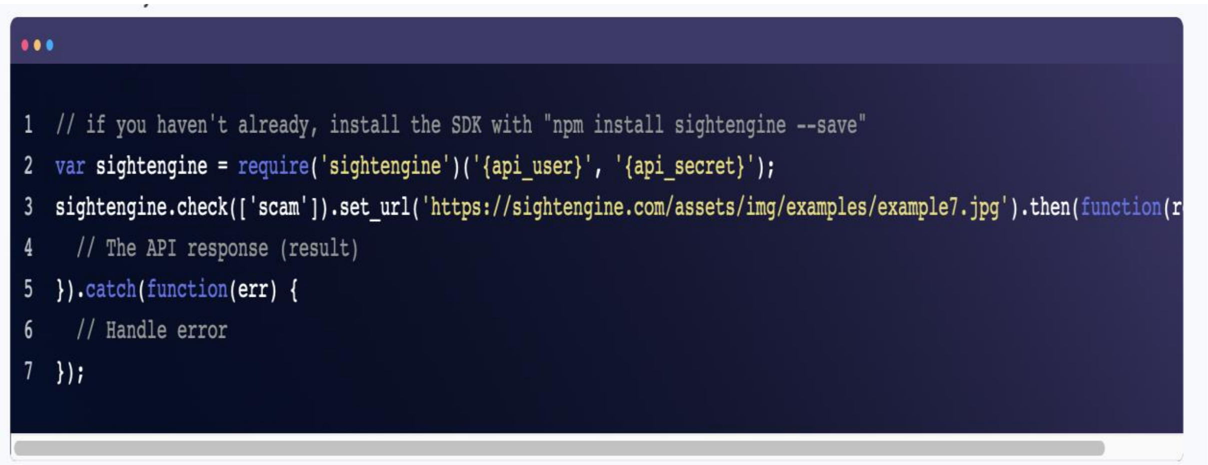
```
// if you haven't already, install the SDK with "npm install sightengine --save"
var sightengine = require('sightengine')('{api_user}', '{api_secret}');
sightengine.check(['{model}']).set_url('https://sightengine.com/assets/img/examples/example7.jpg').then(functio
  // The API response (result)
}).catch(function(err) {
  // Handle error
});
```

Figure 3: Sight Engine API (SightEngine.com)

Code in plain text:

```
// if you have not already, install the SDK with "npm install sight engine --save"
var sightengine = require('sightengine')('{api_user}', '{api_secret}');
sightengine.check([‘{model}’]).set_url('https://sightengine.com/assets/img/examples/example7.jpg').then(function(result) {
  // The API response (result)
}).catch(function(err) {
  // Handle error
});
```

Another example of the use of API for scammers:



```
// if you haven't already, install the SDK with "npm install sightengine --save"
var sightengine = require('sightengine')('{api_user}', '{api_secret}');
sightengine.check(['scam']).set_url('https://sightengine.com/assets/img/examples/example7.jpg').then(function(r
  // The API response (result)
}).catch(function(err) {
  // Handle error
});
```

Figure 4: Sight Engine API Sending Request (SightEngine.com)

Code in plain text:

```
// if you haven't already, install the SDK with "npm install sightengine --save"
var sightengine = require('sightengine')('{api_user}', '{api_secret}');
sightengine.check(['scam']).set_url('https://sightengine.com/assets/img/examples/example7.jpg').then(function(result) {
  // The API response (result)
}).catch(function(err) {
  // Handle error
});
```

SightEngine Scam API gives an option to send 2000 requests per month at no cost.

In conclusion, once user copies and the pastes the profile link in the dating website into the tool, the tool will generate a scam likelihood with a graph (Figure 5).

The tool will use the red flags that are generated by the key-word scam technique and public photo scanner technique.

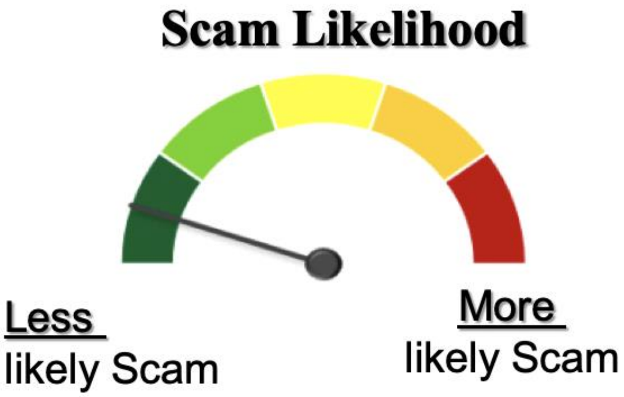


Figure 5: Scam Likelihood Indicator

Summary

This chapter covered two main topics. First, background work was covered. Background work included both psychological work and software work that has been done so far. Previous researches that tried to solve or analyze the scam on dating web services were also introduced. The background section was categorized based on the publish years by the researches. It was set as old to newer. The second section introduced the idea of the tool. Later sections discussed what could be used to make this tool alive. Two main APIs that were discussed how they would fit into this idea. The way of using their libraries was also introduced with a few simple lines of coding.

The next chapter will be more related to how the tool will be designed and used. The methodologies for the tool will be explained at a deeper level.

Chapter III: Methodology

Introduction

This part will clarify what sort of study framework with the upsides and downsides to offering an answer for the online dating scam issue. It will profoundly clarify the AI calculation that is offered by Amazon to extract information from pictures in rekognition API. Likewise, the advantages and disadvantages of rekognition API will be clarified in detail. Later the exploration will incorporate outcome information to demonstrate how it very well may be utilized to take care of the issue.

Design of the Study

With everything taken into account, both qualitative and quantitative research plans offer different understandings reliant on research focuses. This paper includes the obstructions and characteristics of both research plans. All through the past examinations exhibit that if there is a remarkable piece of total data that exists and consistent assurances supporting the data, inquiries about should move towards quantitative research plan. In any case, as to the examination point, there might be inadequate intelligent data or proof exhibited. Thus, the analyst will need to put a solitary effort to demonstrate what ought to be done to comprehend the issue. This sort of research subject will require a qualitative research plan. To plot, examine structures may fluctuate or can be united reliant on the exploration subject and past examinations.

Since the presence of past examinations are deficient in taking care of the issue, and the past investigations' information is not sufficient for the tackling issue, this investigation will utilize the mixed strategy to take care of the issue.

Data Collection

The techniques that were utilized by Fire are extremely persuading with respect to 2013. Investigating the individual information, breaking down Facebook's security settings, and the Facebook applications that utilization individual information systems are exact approaches to recognize the phony profiles. In any case, Fire expressed that their applications kept running into such a large number of false-positive banners. Interior settings and the informational collection that was utilized for AI were not precisely set. Along these lines, the exactness of this recommended device was not fruitful to distinguish the phony profiles on Facebook.

Eloivici guaranteed that if the client has companions from various networks and the client's companion’s rundown contains companions, not exactly a regular client has; these can be considered as warnings to recognize the profile as phony. Later Eloivici's (2015) recreation of these strategies in various stages with various sizes of informational indexes demonstrated that the creation could distinguish phony profiles. In any case, Eloivici had just outlined with constrained informational collections and specific means to distinguish the spammers and phony profiles on interpersonal organizations.

Past researches were showing information for various zones that are sub identified with online dating scam issues. Because of this reality, more research should have been finished. This examination will hold a light into this issue.

Tools and Techniques

Amazon Rekognition makes it simple to add a picture and video examinations to your applications. You give a picture or video to the Amazon Rekognition API, and the administration can distinguish objects, individuals, content, scenes, and exercises. It can distinguish any improper substance too. Amazon Rekognition additionally gives profoundly precise facial examination and facial acknowledgment. You can distinguish, dissect, and analyze faces for a wide assortment of utilization cases, including client confirmation, classifying individuals checking, and open wellbeing.

Amazon Rekognition depends on the equivalent demonstrated, exceptionally versatile, profound learning innovation created by Amazon's PC vision researchers to dissect billions of pictures and recordings day by day. It requires no AI skill to utilize. Amazon Rekognition incorporates a basic, simple to-utilize API that can rapidly break down any picture or video record that is put away in Amazon S3. Amazon Rekognition is consistently gaining from new information, and we continually include new names and facial acknowledgment highlights to the administration. Typical use cases for utilizing Amazon Rekognition incorporate the accompanying:

- Searchable picture and video libraries – Amazon Rekognition make pictures and put away recordings accessible so you can find items and scenes that show up inside them.

- Face-based client check – Amazon Rekognition empowers your applications to affirm client characters by contrasting their live picture and a reference picture.

• Sentiment and statistic investigation – Amazon Rekognition translate enthusiastic articulations, for example, glad, dismal, or shock, and statistic data, for example, sexual orientation from facial pictures. Amazon Rekognition can break down pictures, and send the feeling and statistic ascribes to Amazon Redshift for intermittent giving an account of patterns, for example, in-store areas and comparable situations. Note that a forecast of enthusiastic demeanor depends on the physical appearance of an individual's face as it were. It is not demonstrative of an individual's inner enthusiastic state, and Rekognition ought not to be utilized to make such an assurance.

• Facial acknowledgment – With Amazon Rekognition, you can scan for pictures, put away recordings, and spilling recordings for appearances that match those put away in a holder known as a face accumulation. A face accumulation is a record of countenances that you claim and oversee. Recognizing individuals dependent on their appearances requires two remarkable strides in Amazon Rekognition:

1. Record the countenances.

2. Search the countenances.

•Unsafe substance discovery – Amazon Rekognition can recognize grown-up and natural substances in pictures and put away recordings. Engineers can utilize the returned metadata to channel unseemly substance dependent on their business needs. The past is hailing a picture dependent on the nearness of dangerous substance, and the API additionally restores a various leveled rundown of marks with certainty scores. These names demonstrate explicit classes of a dangerous substance, which empowers granular sifting and the board of vast volumes of client created content (UGC). Models incorporate social and dating locales, photograph sharing stages, websites and discussions, applications for kids, web-based business destinations, stimulation, and internet promoting administrations.

• Celebrity acknowledgment – Amazon Rekognition can perceive VIPs inside provided pictures and in recordings. Amazon Rekognition can perceive a large number of big names over a few classifications, for example, governmental issues, sports, business, diversion, and media.

• Text recognition – Amazon Rekognition Text in Image empowers you to perceive and separate literary substance from pictures. Content in Image bolsters most text styles, including exceptionally adapted ones. It distinguishes content and numbers in various directions, for example, those usually found in standards and publications. In picture sharing and internet-based life applications, you can utilize it to empower visual hunt dependent on a list of pictures that contain similar watchwords. In media and excitement applications, you can index recordings dependent on the meaningful content on the screen, for example, advertisements, news, sports scores, and subtitles. At last, in open wellbeing applications, you can recognize vehicles dependent on tag numbers from pictures taken by road cameras.

Recognize celebrities. The celebrity API returns a variety of famous people perceived in the info picture. RecognizeCelebrities restores the 100 most prominent faces in the picture. It records perceived VIPs in the CelebrityFaces exhibit and unrecognized faces in the UnrecognizedFaces cluster. RecognizeCelebrities doesn't return big names whose appearances aren't among the most prominent 100 faces in the picture. For every superstar perceived, RecognizeCelebrities restores a Celebrity object. The Celebrity item contains the VIP name, ID, URL connects to extra data, coordinate certainty, and a ComparedFace object that you can use to find the VIP's face on the picture. Amazon Rekognition doesn't hold data about which pictures a big name has been perceived in. Your application must store this data and utilize the Celebrity ID property as one of a kind identifier for the big name. In the event that you don't store the big name or new data URLs returned by RecognizeCelebrities, you will require the ID to distinguish the superstar in a call to the GetCelebrityInfo activity. You pass the info picture either as base64-encoded picture bytes or as a kind of perspective to a picture in an Amazon S3 can. On the off chance that you utilize the AWS CLI to call Amazon Rekognition tasks, passing picture bytes isn't upheld. The picture must be either a PNG or JPEG designed document.

For instance, see Recognizing Celebrities in an Image:

This activity expects authorization to play out the rekognition: RecognizeCelebrities activity.

Solicitation Syntax

```
{
"Picture": {
"Bytes": mass, "S3Object": {
"Basin": "string", "Name": "string", "Rendition": "string"
}
}
```

Solicitation parameters. The solicitation acknowledges the accompanying information in JSON design.

The information picture as base64-encoded bytes or an S3 object. In the event that you utilize the AWS CLI to call Amazon Rekognition activities, passing base64-encoded picture bytes isn't bolstered.

On the off chance that you are utilizing an AWS SDK to call Amazon Rekognition, you won't have to base64-encode picture bytes passed utilizing the Bytes field.

Reaction Syntax

```
{
"CelebrityFaces": [
{
"Face": {
"BoundingBox": { "Tallness": number, "Left": number, "Top": number, "Width": number
},
"Certainty": number, "Tourist spots": [
{
"Type": "string", "X": number, "Y": number
} ],
"Posture": {
"Pitch": number, "Move": number, "Yaw": number
},
"Quality": {
"Splendor": number,
"Sharpness": number }
},
"Id": "string", "MatchConfidence": number, "Name": "string",
"Urls": [ "string" ]
} ],
"OrientationCorrection": "string", "UnrecognizedFaces": [
{
"BoundingBox": {
"Stature": number, "Left": number, "Top": number, "Width": number
},
"Certainty": number, "Tourist spots": [
{
"Type": "string", "X": number, "Y": number
} ],
"Posture": {
"Pitch": number, "Move": number, "Yaw": number
},
"Quality": {
"Splendor": number,
```

"Sharpness": number }

}]

356

Amazon Rekognition Developer Guide RecognizeCelebrities

}

Reaction elements. On the off chance that the activity is productive, the administration sends back an HTTP 200 reaction. The accompanying information is returned in JSON design by the administration.

Insights concerning every big-name found in the picture Amazon Rekognition can distinguish a limit of 15 big names in a picture.

Type: Array of Celebrity objects OrientationCorrection

The direction of the info picture (counterclockwise course). On the off chance that your application shows the picture, you can utilize this incentive to address the direction. The jumping box directions returned in CelebrityFaces, and UnrecognizedFaces speak to confront areas before the picture direction is remedied.

On the off chance that the information picture is in .jpeg group, it may contain interchangeable picture (Exif) metadata that incorporates the picture's direction. Assuming this is the case, and the Exif metadata for the information picture populates the direction field, the estimation of OrientationCorrection is invalid. The CelebrityFaces and UnrecognizedFaces jumping box directions speak to confront areas after Exif metadata is utilized to address the picture direction. Pictures in .png configuration don't contain Exif metadata.

Type: String

Legitimate Values: ROTATE_0 **|** ROTATE_90 **|** ROTATE_180 **|** ROTATE_270

Unrecognized faces. Insights concerning each unrecognized face in the picture. Type: Array of ComparedFace objects

Mistakes

Access denied exception. You are not approved to play out the activity. HTTP Status Code: 400

Image too large exception. The info picture size surpasses as far as possible. For more data, see Limits in Amazon Rekognition

HTTP Status Code: 400

Internal server error. Amazon Rekognition encountered an assistance issue. Attempt your call once more. HTTP Status Code: 500

Amazon Rekognition Developer Guide RecognizeCelebrities

Invalid image format exception. The gave picture organization isn't bolstered. HTTP Status Code: 400

InvalidImage format exception. The gave picture organization isn't upheld. HTTP Status Code: 400

Invalid parameter exception. The information parameter damaged a requirement. Approve your parameter before calling the API activity once more.

HTTP Status Code: 400

Invalid s3 object exception. Amazon Rekognition can't get to the S3 article determined in the solicitation. HTTP Status Code: 400

Provisioned throughput exceeded exception. The number of solicitations surpassed your throughput limit. In the event that you need to expand this point of confinement, contact Amazon Rekognition.

HTTP Status Code: 400

Throttling exception. Amazon Rekognition is briefly unfit to process the solicitation. Attempt your call once more. HTTP Status Code: 500

Search faces. For a piece of the given information, face ID scans for coordinating countenances in the accumulation the face has a place with. You get a face ID when you add a face to the accumulation utilizing the IndexFaces activity. The activity thinks about the highlights of the information face with countenances in the predefined accumulation.

We can likewise look through appearances without ordering faces by utilizing the SearchFacesByImage activity.

The activity reaction restores a variety of countenances that match, requested by likeness score with the most noteworthy similitude first. All the more explicitly, it is a variety of metadata for each face coordinate that is found. Along with the metadata, the reaction additionally incorporates certainty esteem for each face coordinate, demonstrating the certainty that the particular face coordinates the information face.

This activity expects authorization to play out the rekognition: SearchFaces activity.

The solicitation acknowledges the accompanying information in the JSON group.

The ID of the accumulation the face has a place with.

Type: String

Length Constraints: Minimum length of 1. The most extreme length of 255.

Example: [a-zA-Z0-9_.\-]+

Required: Yes

FaceId

The ID of a face to discover matches for in the accumulation.

Type: String

Example: [0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}

Required: Yes

Face match threshold. Discretionary worth indicating the base trust in the face match to return. For instance, don't restore any matches where trust in matches is under 70%. The default worth is 80%.

Type: Float

Substantial Range: Minimum estimation of 0. Most final estimation of 100.

{

"CollectionId": "string", "FaceId": "string", "FaceMatchThreshold": number, "MaxFaces": number

}

Required: No

MaxFaces

The most extreme number of appearances return the data. The activity restores the most extreme number of countenances with the most elevated trust in the match.

Type: Integer

Substantial Range: Minimum estimation of 1. Greatest estimation of 4096. Required: No

Reaction Syntax

```
{
"FaceMatches": [
{
"Face": {
"BoundingBox": { "Stature": number, "Left": number, "Top": number, "Width": number
},
"Certainty": number, "ExternalImageId": "string", "FaceId": "string", "ImageId": "string"
},
"Closeness": number }
],
"FaceModelVersion": "string", "SearchedFaceId": "string"
}
```

Reaction Elements

On the off chance that the activity is sufficient, the administration sends back an HTTP 200 reaction. The accompanying information is returned in the JSON position by the administration. FaceMatches

A variety of countenances that coordinated the info face, alongside the trust in the match. Type: Array of FaceMatch objects

FaceModelVersion

Adaptation number of the face location model related to the info gathering (CollectionId). Type: String

SearchedFaceId

The ID of the face that was looked for matches in a gathering.

Type: String

Example: [0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}

Access denied exception. You are not approved to play out the activity. HTTP Status Code: 400

inner server blunder

Amazon Rekognition encountered an assistance issue. Attempt your call once more. HTTP Status Code: 500

Invalid parameter exception. The information parameter disregarded a limitation. Approve your parameter before calling the API activity once more.

HTTP Status Code: 400

Provisioned throughput exceeded exception. The number of solicitations surpassed your throughput limit. On the off chance that you need to expand this cutoff, contact Amazon Rekognition.

HTTP Status Code: 400

Resource not found exception. The accumulation indicated in the solicitation can't be found. HTTP Status Code: 400

Throttling exception. Amazon Rekognition is incidentally incapable of processing the solicitation. Attempt your call once more. HTTP Status Code: 500

The logic can be simplified, as shown below for the solution design.

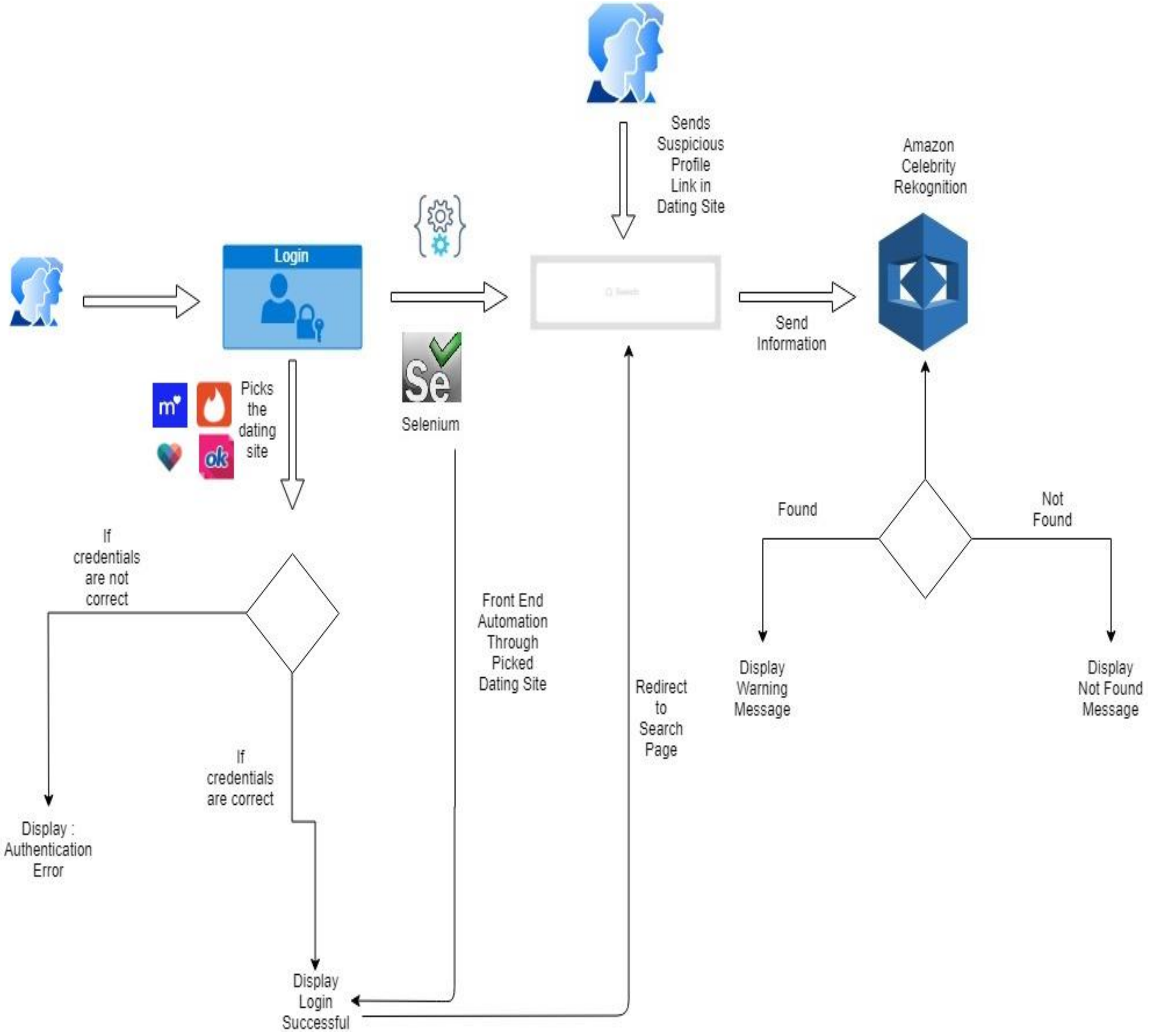


Figure 6: Implementation of Online Dating Scam Detector

Summary

This chapter dived into the solution that was implemented by using Amazon Rekognition API and Selenium library in .NET. The details of what Amazon Rekognition API offers were explained in detail. After APIs capabilities were explained, the exception handling was also explained in detail by referring to the Amazon API documentation on Amazon.com. At the end of the chapter, the solution design diagram was introduced.

Chapter IV: Data Presentation and Analysis

Introduction

The primary objective of Amazon Rekognition API distinguishes the celebrity face in the given picture. In this part, I will attempt a trial to see better how the API would create an outcome with a similar celebrity input yet in various circumstances. Every one of the information that was captured was available publicly. A significant piece of information was not exhibited since the objective was to make a place that may create issue results. Toward the finish of this trial, it will give how trustworthy the API that was utilized to illuminate the online dating scam issue.

Data Presentation

This area will demonstrate example information to test Amazon Rekognition API. The primary segment will display the name of the individual's picture that was submitted into API, and the subsequent section will report the outcome that was created by artificial intelligence. All the photographs that were sustained into API were copied from google pictures. Some male celebrities' photos were acquainted with API with facial hair and no facial hair. Likewise, some female celebrities' photographs were submitted to API with short and long hair. A portion of the photos that are not celebrities were additionally nourished into API to perceive what results were produced. The explanation was an information test was made to see how exact outcomes were created by Amazon Rekognition artificial intelligence API.

Data Analysis

Table 1

Data Samples Input Output Comparison

Input Image	**Rekognition API Result**
Jenna Fischer	Jenna Fischer
Angelina Jolie	Angelina Jolie
George Clooney (Short Facial Hair)	George Clooney
George Clooney (Long Facial Hair)	No Celebrity Faces Recognized
Abu Abdullah Hussein	No Celebrity Faces Recognized
Dennis Guster	Enrique Krauze
Mailewa Akalanka	No Celebrity Faces Recognized
Michelle Obama	Michelle Obama
Madonna	Madonna
Madonna (Wearing an Eye Patch)	Porcelain Black
Lebron James (Facial Hair)	Lebron James
Adele	Adele
Adele (Short Hair)	Adele
Rainn Wilson (No Facial Hair)	Rainn Wilson
Rainn Wilson (Facial Hair)	No Celebrity Faces Recognized

Test results in details:

- Amazon Rekognition API was fed with a picture in which Madonna was wearing an Eye Patch. The result was a celebrity; however, it was Porcelain Black. This was a false-positive result for Amazon Rekognition.

- Amazon Rekognition API was fed with a picture in which Rainn Wilson had facial hair. API was not able to detect the celebrity. It was detected that if a celebrity had facial hair, API was not able to detect the celebrity. The result was indicated as ‘No celebrity was detected.’

-Dennis Guster is a professor at St. Cloud State University in Information Assurance Department. His picture was downloaded from the department’s website and was used as an input for Amazon Rekognition API. The result was surprising, and it detected the professor’s picture as a celebrity. The indicated result was Enrique Krauze who is a Mexican historian.

Summary

Information that was fed into Amazon Rekognition API shows that celebrities who are wearing some stuff that covers their appearances may bring about an inappropriate yield. In like manner, stars who are known without having facial hairs in motion pictures are likewise making some bogus yield results as the example information has demonstrated that a non-celebrity face can be perceived as a celebrity in certain circumstances, which is another off-base outcome. In any case, later, the information that was encouraged into API with celebrities' photographs, which are appeared with a similar facial appearance in the movies they acted, was adequately perceived by Rekognition API.

Chapter V: Results, Conclusion, and Recommendations

Introduction

This section clarifies the aftereffects of the offered solution. The parts that the appropriate response was fruitful in actualizing and the result of what was accomplished was defined. The techniques and the libraries that were utilized during the execution were portrayed in detail. Later it plunges into future work, and the client situations should be possible.

Results

The software that was implemented was able to detect the celebrity photos on dating websites. During the trial version, the software was set for the OkCupid dating website. By using the selenium front-end automation, the HTML tags in the OkCupid site was automated to find the user profile photos. The profile was set with a celebrity photo which was Steve Carell. Amazon Rekognition API was able to identify the celebrity and displayed a notification with the celebrity name. However, different celebrities from outside the US was put into the profile, Amazon Rekognition API had shown a different name for the celebrity, even though it was able to identify the photo as a celebrity.

Conclusion

The examination showed that online profiles could be automated dependent on client contribution with Selenium. When the info is gotten, a picture can be filtered with Amazon Rekognition to comprehend whether the profile has a celebrity name photograph or not.

Future Work

Over time artificial intelligence will improve itself, and facial recognition will serve better results. For future work, researchers can focus on how to automate better on dating profiles yet not only the websites. This research was mainly focused on data scraping on websites and using artificial intelligence to detect faces. However, applications on phones have been trendy rather than websites. Today's world people use their phones way often than computers for dating purposes. Hence, a future researcher should make an app both on android and apple markets. The same idea can be improved by using more scam flags to identify for better results. Also, this idea can be integrated with dating platforms such as Tinder's or Match.com's apps on the apps market and can be served to the public under Tinder Safe+ or Match+.

In addition, instead of automating through the front-end, the same idea for the future can be automated through back end once dating services provide their public API. Data scraping through the back end will be way faster, and it will undoubtedly create fewer errors and better exception handling. This will also bring a better user experience.

There were more indicators detected as scam flags through this research. However, all the indicators were not implemented in the application. For future researches, more scam indicators can be implemented to serve better to the public. For example, if the IP address of the profile can be detected, and it shows that the IP address is not from the U.S, this can be implemented. Furthermore, if the dating profile had any text that was implying, he or she is outside the U.S, the profile intro can be scanned and added to the implementation.

As Facebook also came out with their dating environment, the expectation is it will become more popular, and since there is more research on scams on Facebook, there can be another application build specifically for Facebook for the future. Like the fact that Facebook has the top number of users compared to any other social network environment, the research will help millions out there by only explicitly focusing on Facebook.

References

Americans Lost $143 Million In Online Relationship Scams Last Year. (2019, Feb). Retrieved June 8, 2019, from NPR.org website: https://www.npr.org/2019/02/13/694171341/americans-lost-143-million-in-online-relationship-scams-last-year

AWS Global Infrastructure. (2019). *Machine Learning in the AWS Cloud*. doi: 10.1002/9781119556749.ch7

Cialdini, R. B. (2007). *Influence: the psychology of persuasion*. New York: HarperCollins.

DOJ Grants Financial Guide (2017). Retrieved from: https://ojp.gov/financialguide/doj/pdfs/DOJ_FinancialGuide.pdf.

Elovici, Y., Fire, M., & Gilad, K. (2015). *Method For Detecting Spammers and Fake Profiles in Social Networks*.

Fletcher, E. (2019, February 14). Romance scams rank number one on total reported losses. Retrieved from https://www.ftc.gov/news-events/blogs/data-spotlight/2019/02/romance-scams-rank-number-one-total-reported-losses.

Fire, M., Kagan, D., Elyashar, A., & Elovici, Y. (2013). Friend or Foe? Fake Profile Identification in Online Social Networks. *ArXiv:1303.3751 [Physics]*. Retrieved from http://arxiv.org/abs/1303.3751

Hu, Y., Wang, H., Zhou, Y., Guo, Y., Li, L., Luo, B., & Xu, F. (2018). Dating with Scambots: Understanding the Ecosystem of Fraudulent Dating Applications. *ArXiv:1807.04901 [Cs]*. Retrieved from http://arxiv.org/abs/1807.04901

Huang, J., Stringhini, G., & Yong, P. (2015). Quit Playing Games with My Heart: Understanding Online Dating Scams. In M. Almgren, V. Gulisano, & F. Maggi (Eds.), *Detection of Intrusions and Malware, and Vulnerability Assessment* (Vol. 9148, pp. 216–236). https://doi.org/10.1007/978-3-319-20550-2_12

Kopp, C., Layton, R., Sillitoe, J., & Gondal, I. (2016). The Role of Love stories in Romance Scams: A Qualitative Analysis of Fraudulent Profiles. *International Journal of Cyber Criminology*, *9*(2), 205–217. https://doi.org/10.5281/zenodo.56227

Longe, O., & Osofisan, A. (2011). On the Origins of Advance Fee Fraud Electronic Mails: A Technical Investigation Using Internet Protocol Address Tracers. Retrieved from https://digitalcommons.kennesaw.edu/ajis/vol3/iss1/2/

Pak, K., & Shadel, D. (2011). https://assets.aarp.org/rgcenter/econ/fraud-victims-11.pdf. Retrieved from https://assets.aarp.org/rgcenter/econ/fraud-victims-11.pdf

Radford, B. (2014). The sweet science of seduction or scam? Evaluating eHarmony. *Skeptical Inquirer*, *38*(6), 38-. Retrieved from Expanded Academic ASAP.

Sixth Tone. (2018, June 1). Over 1,300 Arrested in 'Tea Leaves' Online Dating Scam. Retrieved from https://www.sixthtone.com/news/1002397/over-1,300-arrested-in-tea-leaves-online-dating-scam.

2018 Report on FINRA Examination Findings. (2018, December 7). Retrieved from https://www.finra.org/rules-guidance/guidance/reports/2018-report-exam-findings.

2015 Internet Crime Report. (2015). Retrieved from https://pdf.ic3.gov/2015_IC3Report.pdf.

Ultrascan Advanced Global Investigations. (2014). Retrieved from https://www.ultrascan-agi.com/public_html/html/pdf_files/Pre-Release-419_Advance_Fee_Fraud_Statistics_2013-July-10-2014-NOT-FINAL-1.pdf.

Wani, M. A., & Jabin, S. (2017, May). *A sneak into the Devil's Colony- Fake Profiles in Online Social Networks*. 31.

What You Need to Know About Romance Scams. (2019, September 10). Retrieved from https://www.consumer.ftc.gov/articles/what-you-need-know-about-romance-scams.

When love becomes a nightmare: Online dating scams. (2019, February 14). Retrieved June 9, 2019, from WeLiveSecurity website: https://www.welivesecurity.com/2019/02/14/love-becomes-nightmare-scams-apps-online-dating-sites/

Whitty, M. T., & Buchanan, T. (2016). The online dating romance scam: The psychological impact on victims – both financial and non-financial. *Criminology & Criminal Justice*, *16*(2), 176–194. https://doi.org/10.1177/1748895815603773

Vision AI | Derive Image Insights via ML | Cloud Vision API | Google Cloud. (2019, Aug). Retrieved from https://cloud.google.com/vision/?utm_source=google&utm_medium=cpc&utm_ca

mpaign=na-US-all-en-dr-skws-all-all-trial-b-dr-1003905&utm_content=text-ad-none-any-DEV_c-CRE_291263994208-ADGP_Hybrid+|+AW+SEM+|+SKWS+|+US+|+en+|+BMM+~+ML/AI+~+Vision+API+~+Vision+Api-KWID_43700036256019077-kwd-475110369966&utm_term=KW_+vision +api-ST_+Vision++Api&gclid=Cj0KCQjwivbsBRDsARIsADyISJ_Tx87_0XVvub0EsVwQER0DuyGNVulhJh9j7e2w93iTd7GF02rvxGgaAvz1EALw_wcB.

Appendix A: Additional Information

Here is the code for the Online Scam Detector Tool:

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Web;
using System.Web.UI;
using System.Web.UI.WebControls;
using OpenQA.Selenium;
using OpenQA.Selenium.Chrome;
namespace WebApplication1
{
public partial class Main : Page
{
public static ChromeOptions options = new ChromeOptions();
public static ChromeDriver driver = new ChromeDriver(options);
protected void Page_Load(object sender, EventArgs e)
{
}
protected void Unnamed1_Click(object sender, EventArgs e)
{
//Setting up chrome profile
```

```
options.AddArguments(@"user-data-dir=" + "C:\\Users\\ramiz\\OneDrive\\Desktop\\dist"
+ "\\profile");
//Loading the Same Profile For Login Purposes
options.AddArguments(@"user-date-dir" +
"C:\\Users\\ramiz\\AppData\\Local\\Google\\Chrome\\User Data");
options.AddArguments("--no-startup-window");
//Login
driver.Navigate().GoToUrl("https://www.okcupid.com/login");
IWebElement email = driver.FindElement(By.CssSelector("#root > span > div > div >
div.login2017-container > span > div > form > div.login2017-fields > div:nth-child(1) >
span.oknf-typable-wrapper.oknf-typable-wrapper--text > input"));
//Accessing email value from the html form and sending input
email.SendKeys(Request.Form["email"]);
//Send Password
IWebElement password = driver.FindElement(By.CssSelector("#root > span > div > div
> div.login2017-container > span > div > form > div.login2017-fields > div:nth-child(2) >
span.oknf-typable-wrapper.oknf-typable-wrapper--password > input"));
password.SendKeys(Request.Form["pass"]);
System.Threading.Thread.Sleep(2500);
//Click On Login
IWebElement login = driver.FindElement(By.CssSelector("#root > span > div > div >
div.login2017-container > span > div > form > div.login2017-actions > input"));
```

```
login.Click();
//Wait for the automation process
System.Threading.Thread.Sleep(2500);
//Validate Login Session
try
{
IWebElement userExist = driver.FindElement(By.CssSelector("#navigation > div >
span:nth-child(2) > div.profile-button-container > button > div > div > div"));
Label1.Text = "Login Success!";
Response.Redirect("http://localhost:63581/Url");
}
catch
{
Label1.Text = "Login Failed!";
}
}
}
}
```

Url.aspx

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Web;

using System.Web.UI;

using System.Net;

using System.Web.UI.WebControls;

using OpenQA.Selenium;

using OpenQA.Selenium.Chrome;

using Amazon.Rekognition;

using Amazon.Rekognition.Model;

using System.Drawing;

using System.IO;

namespace WebApplication1

{

public partial class Url : System.Web.UI.Page

{

private string inputUrl;

protected void Page_Load(object sender, EventArgs e)

{

if(Page.IsPostBack)

{

inputUrl = TextBox1.Text;

}

}
```

```
public void Analyze_Click(object sender, EventArgs e)
{
//Navigate to the input Profile to Analyze
Main.driver.Navigate().GoToUrl(inputUrl);
//Click on the profile thumbnail pic
IWebElement profilepic = Main.driver.FindElement(By.ClassName("profile-thumb"));
profilepic.Click();
//Download the profile Image
ITakesScreenshot ssdriver = Main.driver as ITakesScreenshot;
Screenshot screenshot = ssdriver.GetScreenshot();
Screenshot tempImage = screenshot;
//Saving the image to analyze
tempImage.SaveAsFile(@"C:\Users\ramiz\source\repos\WebApplication1\WebApplication1\ProfilePics\image.png");
string photo = @"C:\Users\ramiz\source\repos\WebApplication1\WebApplication1\ProfilePics\image.png";
//Rekognition API
AmazonRekognitionClient rekognitionClient = new AmazonRekognitionClient();
RecognizeCelebritiesRequest recognizeCelebritiesRequest = new RecognizeCelebritiesRequest();
Amazon.Rekognition.Model.Image img = new Amazon.Rekognition.Model.Image();
```

```
byte[] data = null;
try
{
using (FileStream fs = new FileStream(photo, FileMode.Open, FileAccess.Read))
{
data = new byte[fs.Length];
fs.Read(data, 0, (int)fs.Length);
}
}
catch (Exception)
{
WarningLabel.Text = ("Failed to load file " + photo);
return;
}
img.Bytes = new MemoryStream(data);
recognizeCelebritiesRequest.Image = img;
WarningLabel.Text=("Looking for celebrities in image " + photo + "\n");
RecognizeCelebritiesResponse recognizeCelebritiesResponse =
rekognitionClient.RecognizeCelebrities(recognizeCelebritiesRequest);
WarningLabel.Text=(recognizeCelebritiesResponse.CelebrityFaces.Count + "
celebrity(s) were recognized.\n");
foreach (Celebrity celebrity in recognizeCelebritiesResponse.CelebrityFaces)
```

```
{
WarningLabel.Text=("This profile is using a celebrity photo: " + celebrity.Name);
}
}
protected void Cancel_Click(object sender, EventArgs e)
{
//Cleanup the text box
TextBox1.Text = "";
}
}
}
```

Here is the front-end code:

```
<%@ Page Title="Main" Language="C#" MasterPageFile="~/Site.Master"
AutoEventWireup="true" CodeBehind="Main.aspx.cs" Inherits="WebApplication1.Main"
%>
<asp:Content ID="BodyContent" ContentPlaceHolderID="MainContent" runat="server">
<html lang="en">
<head>
<meta charset="UTF-8">
<meta name="viewport" content="width=device-width, initial-scale=1">
<!--
=========================================================================
==============================-->
<link rel="icon" type="image/png" href="Images/icons/favicon.ico"/>
<!--
======================================================================
==============================-->
<link rel="stylesheet" type="text/css" href="Vendor/bootstrap/css/bootstrap.min.css">
<!--
======================================================================
==============================-->
<link rel="stylesheet" type="text/css" href="fonts/font-awesome-4.7.0/css/font-
awesome.min.css">
<!--
======================================================================
==============================-->
<link rel="stylesheet" type="text/css" href="fonts/iconic/css/material-design-iconic-
font.min.css">
<!--
======================================================================
==============================-->
<link rel="stylesheet" type="text/css" href="Vendor/animate/animate.css">
<!--
======================================================================
==================================-->
<link rel="stylesheet" type="text/css" href="Vendor/css-
hamburgers/hamburgers.min.css">
<!--
=============================================================================
==================================-->
<link rel="stylesheet" type="text/css" href="Vendor/animsition/css/animsition.min.css">
<!--
=============================================================================
==================================-->
<link rel="stylesheet" type="text/css" href="Vendor/select2/select2.min.css">
<!--
=============================================================================
==================================-->
<link rel="stylesheet" type="text/css"
href="Vendor/daterangepicker/daterangepicker.css">
<!--
=============================================================================
==================================-->
<link href="CSS/css/main.css" type="text/css" rel="stylesheet" />
<link href="CSS/css/util.css" type="text/css" rel="stylesheet" />
<!--
```

```
=========================================================================
==============================-->
</head>
<style>
#services {
width: 100%;
border:0px;
outline:0px;
}
</style>
<body>
<div class="limiter">
<div class="container-login100">
<div class="wrap-login100">
<form class="login100-form validate-form">
<span class="login100-form-title p-b-26">
Welcome To Safer Dating
</span>
<span class="login100-form-title p-b-48">
<i class="zmdi zmdi-font"></i>
<asp:Label ID="Label1" runat="server" Text=""></asp:Label>
</span>
```

```
<div class="wrap-input100 validate-input"  data-validate = "Valid email is: a@b.c">
<input class="input100" type="text" name="email">
<span class="focus-input100" data-placeholder="Email"></span>
</div>
 <div class="wrap-input100 validate-input" data-validate = "Please select service">
<input class="input100" type="text" name="dating">
 <select name="services" id="services">
<option value="okcupid">OkCupid</option>
<option value="match">Match.com</option>
 <option value="eharmony">EHarmony</option>
<option value="tinder">Tinder</option>
</select>
<span class="focus-input100" data-placeholder="Dating Service"></span>
</div>
<div class="wrap-input100 validate-input" data-validate="Enter password">
<span class="btn-show-pass">
<i class="zmdi zmdi-eye"></i>
</span>
<input class="input100" type="password" name="pass">
<span class="focus-input100" data-placeholder="Password"></span>
</div>
<Asp:Button class="login100-form-btn" runat="server" Text="Login"
```

```
OnClick="Unnamed1_Click" Height="34px" Width="300px" />
<!--
==================================================================
=============================-->
<script src="Vendor/jquery/jquery-3.2.1.min.js"></script>
<!--
==================================================================
=============================-->
<script src="Vendor/animsition/js/animsition.min.js"></script>
<!--
==================================================================
=============================-->
<script src="Vendor/bootstrap/js/popper.js"></script>
<script src="Vendor/bootstrap/js/bootstrap.min.js"></script>
<!--
==================================================================
=============================-->
<script src="Vendor/select2/select2.min.js"></script>
<!--
==================================================================
=============================-->
<script src="Vendor/daterangepicker/moment.min.js"></script>
```

```
<script src="Vendor/daterangepicker/daterangepicker.js"></script>
<!--
==================================================================
=============================-->
<script src="Vendor/countdowntime/countdowntime.js"></script>
<!--
==================================================================
=============================-->
<script src="Scripts/main.js"></script>
</body>
</html>
</div>
</div>
</div>
</asp:Content>
<!-- Url Aspx Page -->
<%@ Page Language="C#" AutoEventWireup="true" CodeBehind="Url.aspx.cs"
Inherits="WebApplication1.Url" %>
<!DOCTYPE html>
<html xmlns="http://www.w3.org/1999/xhtml">
<head runat="server">
<link rel="stylesheet" type="text/css" href="CSS/cssButton/button.css">
```

```
</head>

<body>

<form id="form1" runat="server">

<div>

<p> Please enter the url of suspected profile.</p>

<asp:TextBox ID="TextBox1" class="advancedSearchTextBox"

runat="server"></asp:TextBox>

 </div>

<button style="--content: 'Analyze';" type="submit" name="btnAnalyze" id="btnAnalyze"

runat="server" onserverclick="Analyze_Click">

<div class="left"></div>

Analyze

<div class="right"></div>

</button>

<button style="--content: 'Cancel';" type="button" name="btnCancel" id="btnCancel"

runat="server" onserverclick="Cancel_Click">

<div class="left">

</div>

Cancel

<div class="right"></div>

</button>

</br>
```

```
</br>
</br>
<asp:Label ID="WarningLabel" runat="server" Text=""></asp:Label>
</form>
</body>
</html>
```