Detection of Online Manipulation to Prevent Users Victimization

Sandhya Java[1], Fathima Linsha Basheer[2], Sadia Riaz[3], Manindar Jeet Kaur[4], Arif Mushtaq[5]

[1,2,3,4]Amity University Dubai, UAE, [5]Dubai, UAE
[1]sandhyajava25199@gmail.com; [2]linshaias@gmail.com; [3]sriaz@amityuniversity.ae;
[4]mkaur@amityuniversity.ae, [5]mushtaq_arif@yahoo.com

Abstract: ***The existing research on online manipulation merely examines the phenomena throughthe aspects of cognitive hacking, semantic social engineering attack, mediadisinformation tactics, and user customized content and emotional contagion. Furthermore,focus is on the way it impacts user's cognition, emotions and behavior. The concept of user victimization as a result of online manipulation has been researched but the current studies fail to come up with asolution-based approach. In this paper, through conceptual deployment of Artificial Intelligence technique's a framework is proposed that could detectonline manipulationand prevent user's victimization. The framework can be prototyped and further improved by integrating usability designing heuristics and functional requirements. However, in this research it has been substantially argued that an intelligent datamining supported by secure privacy layer will detect manipulation on user generated content and prevent unauthorized access to user's personal data, intercept spreading of inauthentic content and protect users from being victimized. The study is particularly useful for researchers who could develop an intelligent system for this particular purpose.***

Keywords: Online manipulation, user unawareness, cognitive hacking, semantic social engineering attack, media disinformation, customized content, AI

I. INTRODUCTION

Manipulation or sometimes referred as *cognitive hacking* is a characterized form of influence that is neither rational persuasion nor coercion [1]. Online manipulation on the internet is conducted for the purpose of dis-creditation, harming corporate or political competitors, propaganda as well as plain and simple trolling. To accomplish these objectives softwares like social bots, clickbots and votebots, hired professionals or online influencers are used.

The open nature of internet and the ease with which content is shared on social media has made it easier for the frequent occurrence of online manipulation, without the awareness of its users. It has influenced their cognition, opinions, emotions and perspectives about numerous different things.Online content creators take every available opportunity of collaboration, communication, and peer production to target vulnerabilities of individuals in the media ecosystem. With the objective to increase their own visibility and audience, to clearlyemphasize their content [2].

To understand the context of online manipulation and its dependence on user unawareness, we need to study how the different sources collect our personal data and modify our feeds. But this has proven to be quite hard for an individual user to acknowledge due to the fact that manipulators constantly try to steer people away from any truth about the world they do not want them to know, through the means of deceit and other fake posts especially using increased number of likes on various social media outlets to create the illusion of its popularity.The other key reason for user unawareness is their negligible attitudetowards online privacy policies. Users are quite ignorant towards how the personal information provided by them is being used for data mining and other marketing tactics. The collected user data undergoes systematic methodology of aggregation, filtration and organisation for various online manipulation purposes like user customised advertisements, altering political opinions, business frauds, emotional and cognitive victimization. The need for a stronger privacy layer on the social sites has significantly increased, especially due to the high level of user unawareness and ignorance on this specific issue.

Existing research studies conducted either examines the existence of online manipulation or its impact/association on the user's personality and behavior. This paper trails on steps for development of countermeasures against cognitive hacking – an important area of research which has not yet been entirely explored from smart solution perspective. Combating online manipulation requires detection of the misinformation, before it affects user's behavior. Likewise, prevention of unauthorized access of user's personal information assets and its misuse is also an important dimension that has not been explored. This paper proposes a solution-based approach to controlling and preventing online manipulation with the help of artificial intelligence that will essentially detect the sources spreading fake or hoax information. The data gathered is for knowledge acquisition and to provide resourceful data to smart application (or an intelligent system) which can be applied universally to prevent fraudulent activities and subsequent victimization of users. The information gathered can be put to practical use in the future to develop stronger privacy rules and laws for every company trying to extract and misuse user's data.

978-1-5386-9346-9/19/$31.00 ©2019 IEEE

This paper is divided as follows: Section II discusses development of conducted research. In section III places in a conceptual framework for further development. Discussion of Results and Conclusion is done in Section IV.

II. LITERATURE REVIEW

In this section contemporary research is highlighted on various ways in which different sources have accessed user'spersonal information and has been manipulated in the form of customized online content and advertisements. The existing literature focuses primarily on, (1) media propaganda, (2) data analytics for manipulative information, (3) cognitive hacking and its effect on user's behavior and emotions

The media supported ecosystems that prevail today provide an upper hand to manipulators for spreading fake news stories, propaganda perceptions and disseminate agendas. This is done primarily with the help of social media, memes, bots or clickbots, analytics and metrics. The core idea is to sensationalize news and get clicks for revenue or profit making – to the extent that user vulnerabilities are exploited.Research has shown that propagandists use disinformation tactics to spread political bias, hate speech, false activism commentary and even try to sway ecology-related debates – like about climate change policies. Therefore, the spread of false or misleading information is having a real and negative impact on the public consumption of news [2].

Online content creators let data analytics manipulate user's personal information to swing election campaigns around the world. So therefore, mainstream news media is usually concerned with influencing the public's opinions and their political attitudes. The controversial election of Mr. Trump has opened a Pandora box of online news manipulation for gaining personal advantages. In an article published in Forbes 2017,It was revealed that Facebook and Twitter; the two most used social mediasites, were largely responsible for distributing false stories and memes with the intent to sway the outcome of the US Elections 2016. Political strategists working on his presidential campaign used advanced personality tests based on the social media profiles they obtained from the companies to giveaway specific false news to targeted sectors of population in order to influence their votes. Three of the major segments questioned after this debacle were the privacy laws of the sites and its need to use stronger tech to block user profiles spreading the stories as well as, the immediate requirement to educate the users about these issues[3].

An article published in 2016 about CyberWarfare, mentioned the use of social media as a 'weapon' in the political propaganda system and a technique to spread disinformation. The Russians use the tool of 'trolls' – an army of fake social bots sharing the same false information repeatedly, even in different languages to target specific individuals. Publishing stories written by social media-expert propaganda writers on fake, anonymous and various conspiracy-theory sites. These sites were further shared on online forums by the bots to manipulate the reader's feelings. One specific time these trolls were used to create the feeling of fear and stop people of Finland from posting comments related to Russia online. The pro-Russian trolls had a significant effect on the attitude and actions of many Finns, some of which lost touch of true and false and others leaving social media platforms entirely. Trolling was found to have a serious impact on the freedom of speech of people, around the world[24]. The role of media is not just limited to spreading fake and fabricated news for commercial gains but recently it has become a norm for governments world-wide to use media tactics to spread pro-government news to gain support and increase their vote bank [4]. It includes paid government commentators, political bots, fake news around elections and hijacked accounts as shown in Figure 1.

Fig. 1. Prevalence of Online Manipulation Tactics

Manipulations of individuals with the help of disinformation strategies have played a vital part in the decline of online freedom for its users. That's why the different governments have limited the internet services for mobile devices especially for potential security issues. After research, Articles were found that mentioned China, Syria and Ethiopia to be the world's most atrocious internet manipulators, presenting in that respective order. Recent article published in The Guardian, [5] shows that about fifty million profiles on Facebook have been harvested by Cambridge Analytica who are studying major data breaches and understanding deep underlying connotations. They use personal information of users, taken without authorization and have used it to develop a framework which would create individual profiles for voters of the election and thereby creating personalized political advertisements for each. Business firms and governments tend to have specific objectives developed with the intention to create an impact on a large-scale population through

distinguished media propagandas and manipulative commercial advertisements. So, the current pre-dominant form of government has the potential to join public and administrators in an advanced way resulting in better coordination and control offering great equal benefit and peril [6]. Peoplehave also researched and tried to shed light on the use of social media by corporations to monitor the individuals. Big corporations have been using information drawn from 'big data analytics' to observe explore and manipulate the activities of individual social activists on social media platforms. Empirical evidence regarding various strategies used by the Oil industry in United Kingdom for responding to activists after monitoring their activities was found. They have used the stolen information to create techniques to minimize notions shared by the individuals on social media against the policies and corrupt work the industry is trying to do[22].

Exploiting[7]details and facts discovered is not a rare phenomenon, for example an individual can influence others with the help of words. So, it was rightly said "*perception management is pervasive in any contemporary community"*.

There is an extended study conducted [8] that provides insight on perception management which is managed by, i) faking news to impact stock market, ii) fake data for fraud betting in sports, iii) fake news for public perception manipulation, iv) discrediting a journalist, and v) creating fake stories for gaining public sympathy.

Another interesting article on Scientific American showed us [9] how big data mining companies produce individual psychographic profiles to effectively target individuals with hoax information and personalized advertisements, thereby bypass individual rational control, resulting in violation of their cognitive liberty and vulnerabilities, exploit user behavior and their unconscious mind.

An empirical experiment was conducted to understand the effect of customized online content on user's decision making and rationale information processing, [10] found that user's decisions, attention and cognitive processing was impacted especially, due to the goal specificity, relevant content and self-references. And online users were discovered to be more and more receptive towards personalized content and found it helpful in their decision-making process.

Just as how user generated content grabs individual's attention,popularized online contents also does the same. Online content creators tend to create illusionary fake popularity to gain user's attention. In an article, [11]it has been stated that a larger portion of Google analytics traffic might be fake as the technique used for analyzing over estimates grouping of variables in traffic parameters. It has been reported that browser and service providers combinations are sending fake traffic updates with the intent to popularize their services among users.

Literature also examines different perspectives of cognitive hacking which is described as an information system attack that may alter human user's perception, behavior and emotions.[6]The much accurate understanding of cognitive hacking in situations of altering individual's perception is explained as *'Gaining access to or breaking in to a computer information system to modify certain user behaviors in a way that violates the integrity of the entire user information system."* [12]. Therefore, cognitive hacking is a form of social engineering that may target a broad audience rather than specific individuals. Mr. Bruce Schneier, a computer specialist and a cryptographer, put forward an explanation of semantic attacks which was slightly linked to our previous understanding of cognitive hacking [13] *"Semantic attacks directly target the human-computer interface, the most insecure interface on the Internet."*

Social engineering is a collective term for all computer exploitations which furthermore can be defined as,*"Social engineering is the use of deception to manipulate individuals into divulging confidential or personal information that maybe be used for fraudulent purposes. Noun(used in the context of information security)"* [14]. A survey conducted on semantic social engineering attack [15] suggested that semantic attacks manipulated online platforms or system applications through strategic phishing using emails, unclear URLs, malware viruses like scareware, hoax websites and drive by downloads etc. to further deceive users.A conference paper [25] proposed, that in order to gain accessibility to user's information hackers don't always necessarily use algorithmic methodology but a)Physical setup where user feels secure eg.workplace or b)Psychological setting where an illusionary secure bureaucratic atmosphere is created.

The deceptions in media are not limited to politics or people perception management only; it takes a leap forward in the business world as well. The level of deception on the internet has resulted in great levels of economic loss because an intentional distribution of misinformation which influences reader's decisions & actions and this misinformation has the potential to disrupt increasingly automated business processes[6].There have been various studies that have explored the presence of decoy in various online reviews that were written by computer bots to deceive the consumer. One such study [16] discovered that about ten-point three percent of the items sold in the chosen sample had been misguided by the firm owners. Consumers were unable to distinguish between the true and fake reviews and ratings, successfully being deceived.Similarly, a qualitative study was conducted with Southern Sweden's hotel managers from 20 different hotels on their standpoint about online manipulation tactics used forthe hotel's reviews and ratings [23]. The outcome of this specific study confirmed that hotel managers used variousmanipulation techniquesto exploit hotel's ratings,ranking and reviews and involving in such forms ofmanipulation was the only appealing

coherent strategy available to increase their visibility in the highly competitive tourism business.

The effects of cognitive hacking have various sorts of psychological and emotional implications. Online theft, through scam emails, phishing websites and fake online offers has greatly led to users feeling financially victimized [17]. Physicalvictimization of individuals due to Nigerian 419 scam has often occurred where emails were sent to people out of the blue asking them for help to transfer huge amounts of their funds as they were trapped in inaccessible areas. These emails either asked the individual to share their bank details to 'help them transfer their money' which was then used to steal users funds or asked them to travel to different places in search of these people and help rescue them in exchange of huge amounts of cash which more often than not led to the individuals being kidnapped and held hostage for ransom. This scam originated from areas of Nigeria has now spread all over the world being the reason for great physical and financial victimization of individuals [18]. One of the main reason why the scam spread rapidly was due to misinformed, uneducated people& their easy trusting nature(Figure2).

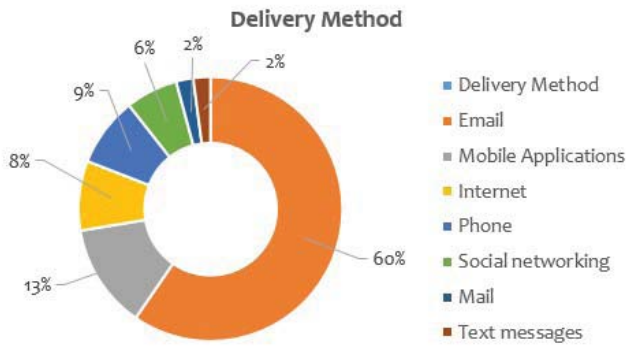

Fig. 2. Statistics showing Nigerian419 scam's delivery method

On the emotional front of cognitive hacking, false news about celebrities has manipulated emotions of individuals very easily. Which was seen in the case of Britney Spears death troll news? In 2016, due to a twitter account hacking the whole world found out that Brittany spears was dead, where a few false pictures were shared by her Record company Sony Entertainment after they were hacked. Tons of fans were in great distress over this news and tweeted condolences without prior fact checking. Later, on the record label deleted said tweets and apologized while informing the world that Brittany Spears was alive and healthy and that their account had been hacked. Several other such cases have been heard of in the past few years and every time the users coming across the cases feel emotionally manipulated and psychological distress [19].

The use of fake bots and trolls to spread disinformation has left the users feeling very vulnerable. The false information shared directly impacts the thoughts, actions and attitudes of the individual. A study conducted by Jessica Aro, stated that people felt brainwashed and taken advantage of because of their need to be able to relate with others. Some online groups manipulate these user feelings and bully them into accepting their agendas and blocking those who opposed. Visually oriented people were bought together with memes, parodies and other graphic aids. These individuals were manipulated based on their common ground and forced to further share the disinformation they read in order to increase its popularity. Such online behavior hasmost of the users feeling the loss of sense of right and wrong, feeling left out, bullied and manipulated, as well as making them quit social media altogether [24]. Likewise, an empirical and psychological study [20] discussed the patterns of victimization which involved the impacted individuals showing delinquent behavior, symptoms of depression and substance abuse due to the strong link between the online and offline behaviors. About $3/4^{th}$ i.e. seventy three percent of adolescents reported that internet manipulations had affected their emotions and behavior offline. Nearly most of the identified behaviors of the challenges faced offline included substance abuse, delinquency, depression and mental health related symptoms.

Transfer of moods among people reading and finding out about each other online is another dynamic of victimization due to online manipulation. Experiment on emotional contagion [21] suggested that feelings shared by peers on various social networking sites influenced their own moods, resulting in the success of a large-scale experiment being conducted on them without their awareness to test the emotional contagion via social sites (Figure 3).

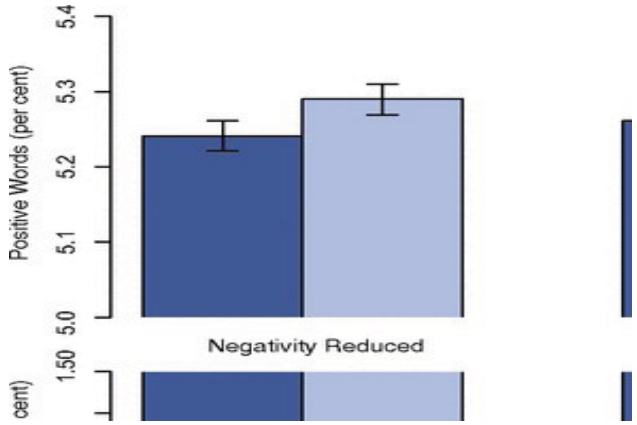

Fig. 3. Average positive (Top) and negative (Bottom) words used by people to describe their emotions (Percentage) Bars present in the graph do embody standard errors.

Investigating the privacy layer of social networking sites has become a crucial area of concern in order to understand the reason behind user's ignorance .A detailed study done on the United States (U.S) consumer privacy by TRUSTe/The National Cyber Security Alliance (NCSA) in 2016[26] established that even though 92% of online users are concerned with their online privacy yet only 31% understand how their personal data is being used. It was analyzed that

33% of population is aware that they have access to the policies regarding the privacy however only 16% ever go through them. This creates a divergence in user's awareness and inability to understand and control how their personal data is being used by third parties which results in them being able to manage user behavior.

In the defense of online service providers; they do offer various privacy policies in the 'terms and conditions' section however users frequently avoid reading them and so on an obvious note they are unaware of how their personal data is being used. An experiment was done to investigate how users read terms and condition of the privacy policies by implementing an eye tracking methodology [28]The study showed that users tend to read the privacy policies when given by default but when an option is given to skip or to read the policies, most users proceed with avoiding it altogether. Even the users who did chose the option to read the policies ended up simply scanning through it. A recent study done in University of Minnesota [29] clarifies the reasons why users don't read the privacy policies;

i. *Readability*: Online privacy policies are not written in user friendly manner rather its three or four lengthy pages with complex technical terms,without any simpler groupings nor headings so ensures low readability chance.

ii. *Time Consumption* : User would have to spend 250+ hours in a year reading all these complicated lengthy policies they encounter throughout the year.[30]

iii. *Accessibility*:Online privacy policies could be considered inaccessible for users because its usually presented where users don't usually lookeg. extreme bottom of the web site in small fonts.

iv. *Motivation:* Users feel giving away their personal data is the price thatthey should compensate in order to be a part of the 'free' online services hence they perceive that they don't have much say on how their personal data is being used.

A analysis done in regard of online privacy in e-commerce [27] called users as "*Transparent human*" as their crucial personal information is easily available online in massive amounts which can been snatched for various marketing prospects in e-commerce.

It is important to note that as users encounter themselves with privacy related issues, they are more likely to be aware and concerned. An article published in Journal of Advertising [31]suggested that users who previously reported any form of privacy invasions were more concerned and gave incomplete informationwhen asked, mostly avoiding web sites that asked for personal info and even unsubscribed from unwanted emails. Hence there is a high requirement for legal authorities take initiatives in regards of online privacy policies so as to safeguard users from online manipulations.

One of the other reasons why people even after claiming to be aware of the privacy concerns, still tendto constantly upload morepersonal information online is simply due to the instantgratification users get from their friends on social sites which directly outweighs the apparent online privacy dangers. Inregards with this concept,A research article on Facebook users was found which evaluated user's behavior, attitudeand any accidental scenarios they fall in to. This study utilized convergence of the usage patterns and privacy concerns and effectively developed a title "Facebook Iceberg". [26]

III. INTELLIGENT DETECTION OF ONLINE MANIPULATION TO PREVENT USERS VICTIMIZATION

The framework draws its tier-wise inspiration from different sources:

Tier 1: Online Manipulation occurs by way of generated personalized online content for users, use of media disinformation tactics,semantic social engineering, due to user unawareness and their victimization, emotional contagion, and cognitive hacking.

The tier is based on extensive literature review done in this study to analyze sources of online manipulation.

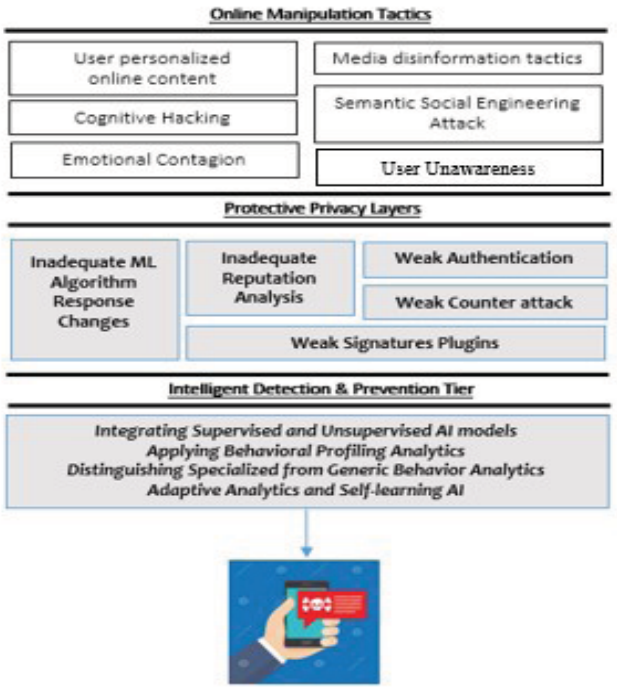

Fig. 4. Framework for Detection of Online Manipulation and Prevention to Stop User Victimization

Figure 4. shows conceptual framework to address intelligent detection of online manipulation to prevent users' victimization.

Tier 2: Protective Privacy Layer The current protective privacy layer is susceptible to encryption which is important to secure sensitive user data. As data is generally stored or received from cloud therefore, to avoid information breach, encryption methods should be secure and intelligent for making it secure. Another concern is related to data fragmentation and redundancy scattering which leads to various fragments being stored on cloud or on server, therefore, the chances or risk factors associated with data loss are high. Web firewall applications are useful for identifying possible attackers to protect online environment. User validation should be higher and enhanced measures to include integrity and encryption mechanisms that are vital for security and privacy of a system.

Tier 3: The Intelligent Detection and Prevention Tier: The need for use of AI (Artificial Intelligence) to detect internet fraud is becoming significant. Some recent applications include:

i) There are payment card and industry data security standards that ensures organizations responsible to process and store credit card information are careful to record information. Artificial intelligent replaces the card details with unique encrypted symbols so manipulators or hackers do not get access to it.

ii) Cardholders can securely manage their online payments due to Visa transaction control. Individuals experience less fraud when using these platforms. Through artificial intelligence users can make various payments through a completely secure and monitored digital wallet without the need to access the physical card or memorize account details.

iii) A new Application known as 3D Secure 2.0 has been particularly useful for analyzing contextual data, which means that the artificial intelligence is involved in learning users' behavior to determine anything suspicious or fraudulent.

As shown in Figure 4, in order to strengthen the security measures of online networks that are big data driven, new lightweight cryptographic algorithms and key management schemes are essential to develop and implement that will be supported by lowest computational power. Moreover, there is a dire need to shift every device that is connected online to have an updated kernel/firmware. It should adequately include the capability to frequently update as new threats are originated.

IV. CONCLUSION

Research has shown that there are multiple ways by which a user is being manipulated online in today's world. Data gathered elaborates on the application of high-level technology to steal users' personal information and use to it to manipulate the content shared with them. Thus, influencing their opinions, emotions as well as cognition successfully without their awareness. Not only have these people been able to manipulate individuals financially but also emotionally and in some very serious cases physically as well.

Much of the user unawareness can be due to the lack of education provided to them in this specific area as well as the avoidance of making the extra effort to verify the content they receive online and further share with others. Findings indicate a few different ways by which individuals can avoid being manipulated online is:

i) Educating the people about the manipulation tactics and ways of data protection. People need to understand how to limit the information they share on social media about themselves, so companies like Cambridge Analytica do not steal it and personalize the content shared to influence their opinions.

ii) Individuals need to understand the dire need for them to verify multiple times the content they hear, see and share online because of all the disinformation constantly shared online by media outlets especially for political propaganda. As well as limit the amount of personal information they share on these media sites.

iii) Further development and strengthening of existing privacy laws used by these companies is necessary.

iv) Systems need to be created that can identify fake posts publicized and popularized with the use of bots and fake likes.

v) Users should take the responsibility of protecting their personal data with the help of anti-virus and other such softwares.

vi) The social media handlers need to begin with cleaning up of the fake profiles that manage lewd operations against citizens, regular checking of authenticity of the suspected trolls and such measures need to be taken for protecting users and information peace.

viii) Google and other internet giants need to eradicate disinformation websites and the giant digital footprint they are leaving behind.

This research addresses a serious concern related to online manipulation and its subsequent victimization of the users. The research elaborates on countermeasures against the tactics that are being used for online manipulation through cognitive hacking, semantic social engineering attack, and customized online content. It illustrates the inadequate privacy layers of the current system and reasons as to why it is extremely necessary to strengthen our security measures on a regular

basis to fight the constant new threats. It is believed stronger measures, such as new lightweight cryptographic algorithms and key management schemes with lowest computational power are required to be developed in order to prevent user victimization. With Artificial Intelligence enabled systems it is now very much possible to do what may have not been possible earlier. Hence, the study proposes developing an artificially intelligent system to data mine and detectssources spreading misinformationwith malign intentions.

Lastly, much of the focus should be given to developing a software tool(intelligent system) which keeps in mind the privacy laws of the various social media companies and blocks out the systems trying to acquire personal data from users illegally. Software that can detectfake posts popularizedwith the help of computer bots. A lot of development is still needed and possible if appropriate tools and the tactics applied for user manipulation and victimization are connected together to give positive outcomes.

REFERNCES

[1] Noggle, Robert, "The Ethics of Manipulation", The Stanford Encyclopedia of Philosophy (summer 2018 Edition), Edward N. Zalta (ed.), URL = <https://plato.stanford.edu/archives/sum2018/entries/ethics-manipulation/>.

[2] Marwick A, Lewis R.(2017). Media Manipulation and Disinformation Online: Data&Society.

[3] Marr B., Forbes (2017)Fake News: How Big Data and AI Can Help,available from:https://www.forbes.com/sites/bernardmarr/2017/03/01/fake-news-how-big-data-and-ai-can-help/#7264ab8170d5

[4] Freedom onthe Net (2017). Manipulating Social Media to Undermine Democracy, Available from:https://freedomhouse.org/sites/default/files/FOTN_2017_Full_Report.pdf

[5] The Guardian (2018). “Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach”, AvailableFrom:https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

[6] Thompson P, Cybenko G, Giani A. (2003).CognitiveHacking, Advance in Computer, Vol.60, Information Security, Elsevier Academic Press.

[7] D. Denning,(1999). Information Warfare and Security, Addison-Wesley, Reading, Mass.

[8] Kenneth Rapoza (2017). “Can 'fake news' impact the stock market?”https://www.forbes.com/sites/kenrapoza/2017/02/26/can-fake-news-impact-the-stock-market/#560ded82fac0.

[9] Tenca M, Vayena E., Scientific American(2018).Cambridge Analytica and Online Manipulation,Available from https://blogs.scientificamerican.com/observations/cambridge-analytica-and-online-manipulation/

[10] Tam Y.K., HoS.K., (2006).Understanding the Impact of Web Personalization on User Information Processing and Decision Outcomes,MIS Quarterly Vol. 30, No. 4,pp. 865-890.

[11] Beek R., (2007) A large portion of your google analytics traffic might be fake, Retrievedfrom:https://www.emarketeers.com/e-insight/a-large-portion-of-your-google-analytics-traffic-might-be-fake.

[12] Thompson P, Cybenko G, Giani A., (2002). Cognitive hacking: A battle for the mind, Computer 35[8], pp 50– 56,Source: IEEE Xplore.

[13] Schneier B., Crypto-Gram Newsletter(2000).Semantic Attacks: The Third Wave of Network Attacks. Retrievedfrom: https://www.schneier.com/crypto-gram/archives/2000/1015.html.

[14] Social Engineering (n.d.). In Oxford Dictionary. Retrievedfrom https://en.oxforddictionaries.com/definition/social_engineering.

[15] Heartfield R, Loukas G., (2016). A Taxonomy of Attacks and a Survey of Defense Mechanisms for Semantic Social Engineering Attacks, ACM Computing Surveys(CSUR) Vol. 48 Issue 3, Article No.37.

[16] Hu N, Bose I.N, Koh N.S, Liu L.,(2012). Manipulation of online reviews: An analysis of ratings, readability and sentiments, Elsevier publication, Decision Support System, Vol.52, Issue 3.

[17] Drager D., (2011). 9 ways to prevent identity theft from your online activities, Available from:https://www.makeuseof.com/tag/9-ways-prevent-identity-theft-online-activities.

[18] Australian Competition and Consumer Commission, Scam Watch: Type of Scams (2018), “Nigerian scams”,Retrieved from:https://www.scamwatch.gov.au/types-of-scams/unexpected-money/nigerian-scams.

[19] McCarthy T., News.com.au (2018) Entertainment: Weirdest celebrity death hoaxes, Retrieved from:https://www.news.com.au/entertainment/celebrity-life/weirdest-celebrity-death-hoaxes/news-story/d2e547417e8d244fb3e005b725c73d0b

[20] Mitchell K.J, Ybarra M, Finkelhor D. (2007). The Relative Importance of Online Victimization in Understanding Depression, Delinquency, and Substance Use, Child Maltreatment,Sage Publication.

[21] Kramer A.D.I, Guillory J.E, Hancock J.T., (2014). Experimental evidence of massive-scale emotional contagion through social networks, PNAS (Proceeding of the National Academy of Science of the United States of America).

[22] Uldam, J. (2016). Corporate management of visibility and the fantasy of the post-political: Social media and surveillance. New Media & Society, 18(2), 201–219. https://doi.org/10.1177/1461444814541526.

[23] Gossling S, Hall C.M, Andersson C.A., (2016). The manager’s dilemma: a conceptualization of online review manipulation strategies, Current Issues in Tourism, Vol.21,Issue 5,pp. 484-503.

[24] Aro, J. European View (2016) 15: 121. https://doi.org/10.1007/s12290-016-0395-5.

[25] Orgill G.L, Romney G.W, Bailey M.G, Orgill P.M., (2004). The urgency for effective user privacy education to counter social engineering attacks on secure computer system, 5th Conference on Information technology education, SIGITE 2004.

[26] Debatin, B., Lovejoy, J. P., Horn, A.-K., & Hughes, B. N. (2009) Facebook and online privacy: Attitudes, behaviors, and unintended consequences. Journal of Computer-Mediated Communication, 15(1), 83-108.http://dx.doi.org/10.1111/j.1083-6101.2009.01494.x