CyberPsycho Attacks: Techniques, Causes, Effects and Recommendations to End-Users

Prashant Gupta
Defence Institute of
Advanced Technology(DU)
Dept of Computer
Science & Engineering
DIAT(DU), Girinagar, Pune,
Maharashtra, India

Manisha J. Nene
Defence Institute of
Advanced Technology(DU)
Dept of Computer
Science & Engineering
DIAT(DU), Girinagar, Pune,
Maharashtra, India

ABSTRACT
From recent years, online social network services are mostly used for marketing, social, political, religious campaign more than just connecting to the friends. Now-a-days, government of most of the countries actively participate on network enabled platforms. Many researchers worldwide are working on social network analysis to extract information from social network services to increase productivity, awareness, learning as well as finding malicious links, phishing, spams & trending viral contents. The study in this paper focuses on causes and effects of persuasive messages based on current trending news and events which effectively may influence an individual's behavior. We name this effect as Cyberspace plus Psychology effect leading to CyberPsycho attacks. In CyberPsycho attacks an attacker uses cyber space & social network to affect or change attitude or behavior, and achieve certain goals to attain political, religious, economical, social gains. It motivates social media users towards a certain objective by spreading the persuasive messages in the form of texts, images or videos. The study is unique, valuable and compels the experts in academia, researchers, technologists and end-users to understand & acknowledge the serious impact of psychological, social and cultural aspects of internet addiction. In this paper, we propose three fundamental models to address and analyze the above concerns. These three proposed models to identify occurrence of cyberpsycho attacks is the major contribution of this paper.

Keywords
Cyberpsycho Attack, Persuasive Technology, Social Network Analysis, Social Media, Semantic Analysis, Online Campaigns, Text Analysis, Cyber Attacks, Cyberpsychology.

1. INTRODUCTION
The Practical Law Company defines cyber attacks as An attack initiated from a computer against a website, computer system or individual computer (collectively, a computer) that compromises the confidentiality, integrity or availability of the computer or information stored on it [1]. Cyber attacks take many forms like hacking techniques, system intrusion, password trafficking, Internet fraud, SPAM, etc. Further, the Internet fraud matters that have a mail nexus, social engineering, exploitation malware, Internet harassment, bomb threats, ransomware, extortion and blackmail impose varied challenges in the cyber world.

1.1 CyberPsycho Attacks
Social network is an uncontrolled and ungoverned marketplace, where ideas become our part of life. As a result of this, many computing devices like mobile, laptop, tablet, desktop have become cheaper, portable and easy to use. This has made a base to use on-line services more efficiently and continuously. Using these computing devices, an individual in the society can do many on-line related transactions such as banking, investments, shopping, health, travel, food etc,. These transactions can be performed on-the-go through any computing device which are connected to Internet. Even the government gazetted notifications are been spread to the people through on-line services. Due to this, an adversary may try to use this digital media to mislead the public by spreading the false information. He / she may use many techniques such as social engineering, phishing, spamming or other methods to achieve his objectives.

1.2 Contribution of this Paper
From past 5 years, on-line social network services are been mostly used for marketing as well as for political campaigns, more than just connecting friends. In this paper, the study is focusing on causes and effects of persuasive messages based on currently trending news and events which influence individual's behavior towards adversaries desired goals. We named this effect as cyberpsycho attack i.e., Cyberspace + Psychology.

In Cyberpsycho attack, the attacker uses end-user's cyber spaces and social spaces without gaining access to end-user's computing device or network. An adversary just uses individual's emotions implied to that situation to achieve his objective. His objectives are to spread his messages to others without including his identity. Individual's who are affected by this cyberpsycho attack are influenced and are motivated to forward the viral messages without knowing the actual reasons behind it. By doing this, he or she just waste the cyber resources like network bandwidth, server/client utilization, the time of data transfer, end-user's time, end-user's money involved in communication to spread the viral messages without any intentions. The effect of this leads to people to take decisions on the basis of news or messages which they read on the social media. This messages or news may be valid or false rumors, but due to the cyberpsycho effect people do not try to verify the authenticity of the message/contents.

The study is unique, valuable and compels the experts in academia, researchers, technologists and end-users to understand & acknowledge the serious impact of psychological, social and cultural aspects of internet addiction. In this paper, we propose three fundamental models to address and analyze the above concerns. These three proposed models to identify occurrence of cyberpsycho attacks is the major contribution of this paper.

Outline of this paper: Section II describes how the cyberpsycho attacks are part of the society and the observations associated to it. Section III describes the strategies and techniques that have influenced and enabled the cyberpsycho attacks. Section IV the proposed works is explained along with the motivation, related work and proposed models to enable the analysis of cyberpsycho attacks. Section V describes the recommendations and preliminary actions to thwart the malign-objectives that work against the benefits to the society & members of the cyber - world and Section VI summarizes and concludes the study and the associated proposed work.

2. CYBERPSYCHO ATTACKS: OBSERVATION IN SOCIETY

Based on the messages, news, and recent case studies done by various researchers and analyst we categorized these effect under following categories.

Category 1: ECONOMICAL

Nowadays, many companies like Amazon, Flipkart, Snapdeal, Ebay, Firstcry, Sony Mobile, Volkswagen, Adidas, Ganna, Pantajali, Nestle, Hike, Telegram etc., are using social media marketing as their main priority, than sales and services. For example : Sony mobile India achieved over 2 million fans through social media(Facebook & YouTube), Volkswagen India received 9,60,000 updates on VW models by leveraging social media(linkedin), social media(Facebook) helped Adidas to become a cricket brand with 1 million+ fans, Gaana leveraged Facebook marketing to achieve 200% growth in daily app downloads[2].

Marketers plans to increase their budget for social media marketing. You hardly find any company who does not reach its audience using social media network and platforms.

Category 2: POLITICAL

The biggest change in Indian Politics was witnessed in 2014 Assembly election due to the impact of cyberpsycho effect. A "Survey on Impact of Social Media on Election System" by Gayatri Wani et al [3] shows how social media becomes a platform for political campaign and helps to connect with voters during elections.

Political parties in many countries, hire social media marketers to make their brand value positively high. They create advertisements based on their election campaign and create viral contents strategies to influence the targeted audience. From Google search results you can find many countries like Philippines, UK, USA and many European countries have massively used the social media for their election campaign.

Category 3: TERRORISM

In recent cases, we found that youngsters are influenced by terrorists groups using social media. Terrorists spreading cyberpsycho effect and uses online social media rather than tradition media because of its interactive usability. Social media services act as a virtual firewall to help safeguard to their identities. By using this they become a part of the mainstream which made difficult for security experts to identify them or detect cyber terrorism. As the marketer uses social media for their target audience and find out how to reach to intended audience as terrorists do.

Scholars, politicians and journalists are unanimously alarmed at the sight of the growth of this organization and are particularly concerned about the efficacy and efficiency of IS propaganda on the Internet and social media[4], which has reached users from all over the world. This implies a new kind of jihad and a new kind of mujaheddin (i.e., warrior). Fighting warriors on the physical field is no longer enough. Virtual warriors,'network warriors' ought to be taken in consideration as well: they are men and women who have been nourishing a 'narrative' that incites to hate non-Muslims and also those Muslims who do not support IS.

Category 4: RELIGIOUS

Social media has big impact on everyone's social life. Useless information, irrelevant and anti-religious post creates ambiguity about the facts, religion and makes both good and bad impact on people later on which causes communal or religious riots.

Category 5: INTERNATIONAL

A country uses cyber space to change the brand value of its country over worldwide and influence other countries investors to move towards it. Every international news, political decisions, rules & regulations are broadly broadcast through social media to change perception of others and through this they use it for their foreign diplomacy as well as tourism.

3. PERSUASIVE TECHNOLOGY AND CYBERPSYCHO ATTACK

Principles of persuasive techniques used to create messages, jokes, slogans, images, contests, quizzes, online campaign, voting, messages, video messages, advertisements, etc.,. these messages are spread to attract the targeted audience like customers, voters or people according to their objectives as described in various categories. This strategy spread the cyberpsycho effect by making content effective and insisting all the audience to participate in the strategy. The strategy makers also forces the audience to share their experience to others which makes it recursively a large impact. For example a negative impact over youngsters, which influence their mind negatively towards the society or community or country that may form a communal riots.

In Persuasive Technology, there are techniques that used to made your content presentation more valuable and redirect user to move towards your objective. These techniques widely used in various social network service providers, e-commerce organization and training and education purposes. It is also used to create persuasive message or content with the sentiments logic in domain as described in Figure 1 to make content shareable within a moments and because of easy to share features of online social network services.

Figure 1: Sentiment Logic behind Viral Contents

3.1 Techniques that enable CyberPsycho attack

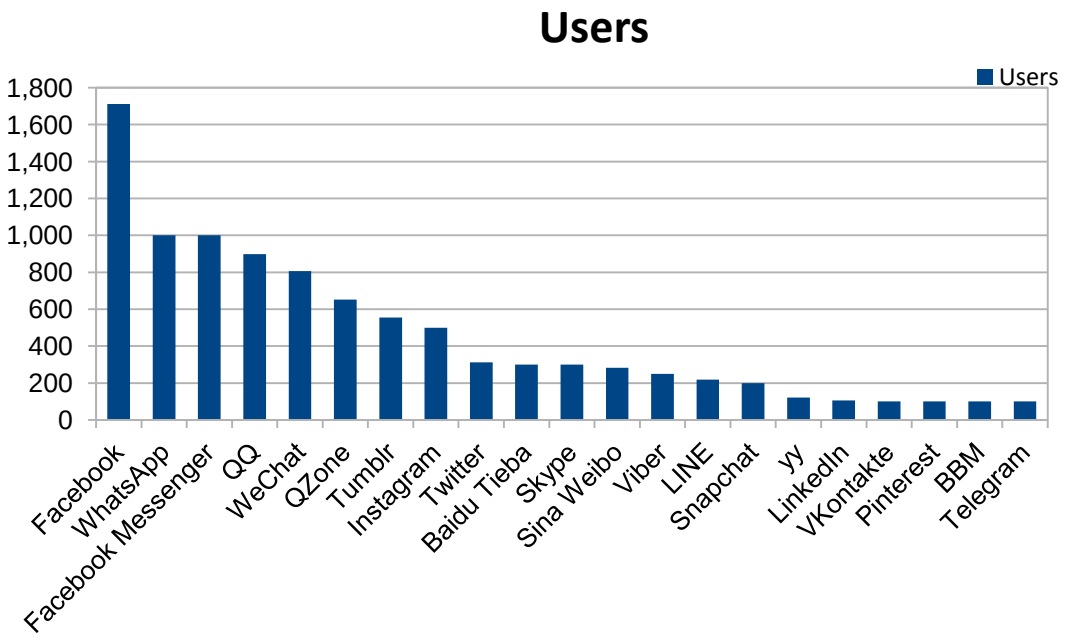
There are many mediums through which a person's attitude or behavior changed. Here this study focusing about the changes by using social networks or social media. Social media becomes part of everybody's life as statistics shows that online we are socially more connected then offline. Chart 1 shows statistics on leading social networks worldwide as of September 2016, ranked by number of active users (in millions) and users statistics shows 2.34 billion social network users worldwide, 1.71 billion active Facebook users and 313 million active monthly users on Twitter.[5]

4. PROPOSED WORK

4.1 Motivation

The observations which described above and techniques that used to enable cyberpsycho effect required to be analyze a better way, technological + psychological, to prevent any big impact. Mostly, persuasive strategies or psychology used in marketing, health, environmental conservation, safety, etc., are found to be quite effective in changing people's attitude and behaviors.

Chart 1. Global social networks ranked by number of users as Sept 2016



4.2 Related Work

In "Use of Persuasive Technology to Change End Users' IT Security Aware Behaviour: A Pilot Study" by Ai Cheo Yeo et al [6] evaluate the effectiveness of the use of persuasive technology to enhancing cyber security aspects by referring to theory of planned behavior. In this paper titled "The Role of Psychology in Enhancing Cybersecurity" by Wiederhold [7] briefly describe the importance of shifting the technology to psychology in order to mitigate the risk of cyberspace. In the research paper "Social Cybersecurity: Applying Social Psychology to Cybersecurity" by Jason Hong et al [8] have applied social psychology influence people to apply security behaviors.

Some of the research paper related to persuasive technology are as discussed below. In the first paper titled "Technological Persuasive Pedagogy: A New Way to Persuade Students in the Computer-based Mathematics Learning" by Alireza Gharbaghi et al [9] introduce a new technological pedagogy which is more effective in students' attitudes toward mathematics. Similarily in "Climate persuasive services: changing behavior towards low carbon lifestyles" by Jorge Luis Zapico et al [10] proposes a concept of "climate persuasive services" as information communication technologies applications that change personal attitudes regarding climate change and/or change behavior towards reducing greenhouse gases emissions. "Computer Vision Based People Tracking for Motivating Behavior in Public Spaces" by Jacob A. Hyman [11] designs a system to permit automatic study of of the impact of motivational messages on people's stair use.

Hongyu Gao et al [12] "Detecting and Characterizing Social Spam Campaigns" studies to quantify and characterize spam campaigns contains obfuscated URL & text, launched using accounts on online social networks. "Mining (Social) Network Graphs to Detect Random Link Attacks (RLA)" by Nisheeth Shrivastava et al [13] analyses the static social network graph to detect RLA to find spammers by profiling properties of whom they send the messages to, instead of what they are sending. In an RLA, a group of malicious users attack a large, randomly selected set of victims and incorporates a large number of existing attacks (like email spams, telemarketing calls, etc.), and also identifies the collaborative nature of these attacks to evade detection.

4.3 Proposed Methodology

In following sections we proposes models which combines technological and psychological services which can be used to detect and analyses the cyberpsycho effect. The block diagram of parameters of cyberpsycho effect is shown in figure 2 in which persuasive techniques are used to create

viral contents which spread using technology and services with some objective that psychologically impact on society.

- *Persuasive Technology*

Persuasive Technology: Persuasive Technology[14] is a vibrant interdisciplinary research field, focusing on the design, development and evaluation of interactive technologies aimed at changing users' attitudes or behaviors through persuasion and social influence, but not through coercion or deception. Dr BJ Fogg[15] defined captology as design, research, and analysis of interactive computing products created for the purpose of changing people's attitude or behaviors.

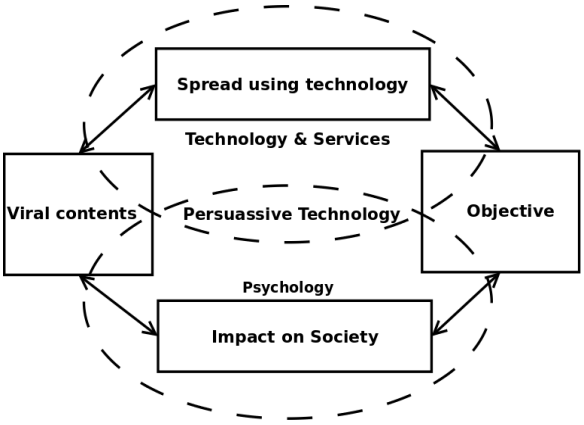


Figure 2: Parameters of CyberPsycho Effect

- *Viral Contents*

Viral contents are may be in different digital form like text messages, jokes, slogans, graphical images, textual images, video messages, articles, mails, campaigns, etc.,

- *Objectives*

Objective of cyberpsycho attack depends upon the adversaries nature. As described earlier, objectives fall under many categories as general categories described earlier.

- *Technology & Services*

There are many technical tools and services which provide services to users to make contents attractive and impressive. Social network service providers as shown in chart 1 provides attractive user friendly platform in which one can easily put their content online without having much computational technical knowledge.

4.4 Proposed Models to enable the analysis of CyberPsycho Attack

Model-1

Figure 3(a) represents the model to analyze cyberpsycho attacks using multimedia contents.

Technical Requirements

S/w Techniques: Browsers, Data Mining tools, Programming Languages & Framework, NLP tools

General Steps For Model-1:

1. Extracting data from various social networks using data extraction tools
2. Extracting keywords related to trending news
3. Extracting semantics using natural language processing tools
4. Classification of results according to categories

Information we may get text- keywords, syntax, metadata-date, time, location, user profile, system data- device details, social network service name. After semantic analysis of user data we can relate it to the cyberpsycho attack categories.

Model-2

Figure 3(b) represents the model to analyze cyberpsycho attacks using multimedia contents.

Technical Requirements

S/w Techniques: Network packet analyzers, Data Mining tools, NLP tools

General Steps For Model-2:

1. Extracting packets from networks data using packet analyzer and extraction tools
2. Analysis of packets and extract keywords related to trending news
3. Extracting semantics using natural language processing tools
4. Classification of results according to categories

Information we may get text- keywords, syntax, metadata-date, time, location, user profile, system data- device details, social network service name. After semantic analysis of user data we can relate it to the cyberpsycho attack categories.

Model-3

Figure 3(c) represents the model to analyze cyberpsycho attacks using multimedia contents.

Technical Requirements

S/w Techniques: Browsers, Image processing Tools, Data Mining tools, Natural Language Processing tools, Programming Languages & Framework

General Steps For Model-3:

1. Extracting multimedia data from various social networks using data extraction tools
2. Extracting images or data related to trending news
3. Extracting semantics using natural language processing tools
4. Classification of results according to categories

Information we may get text- keywords, syntax, metadata-date, time, location, user profile, system data- device details, social network service name. After semantic analysis of user data we can relate it to the cyberpsycho attack categories.

5. ACTION & RECOMMENDATIONS

It is observed that the marketing strategies are always with an objective of influencing an individual to buy the products or use their services with which financial and economical gains are attained. Popup advertisements, flash of an applet , browsing history noted by the web-crawling programs may be disabled.

End-User must never click on the web-links that lure them with the messages promising them the free internet-access, free-talk-time, free-loyalty-points, free-goodies, etc. Nothing comes free should be the motto while using cyberspace.

End-user must not be part to the activity of forwarding spam messages or spam-mails. End-user must always develop a habit to check the authenticity of the forwards.

End-users must think over responding various views, messages, news, advertisements, campaigns, surveys, images, videos broadcast over social networks services even if its forwarded by their knowing person to avoid any kind of active cyber attacks as well as cyberpsycho attack.

The end-users need to be cyber literate. They need to understand that the above stated methods of using cyberspace may not cost money directly, but forms/provides a fundamental base for a huge misuse. It can lead to sever-loss-impact on the resources of cyberspace; and societal-behavioral-changes in an individual.

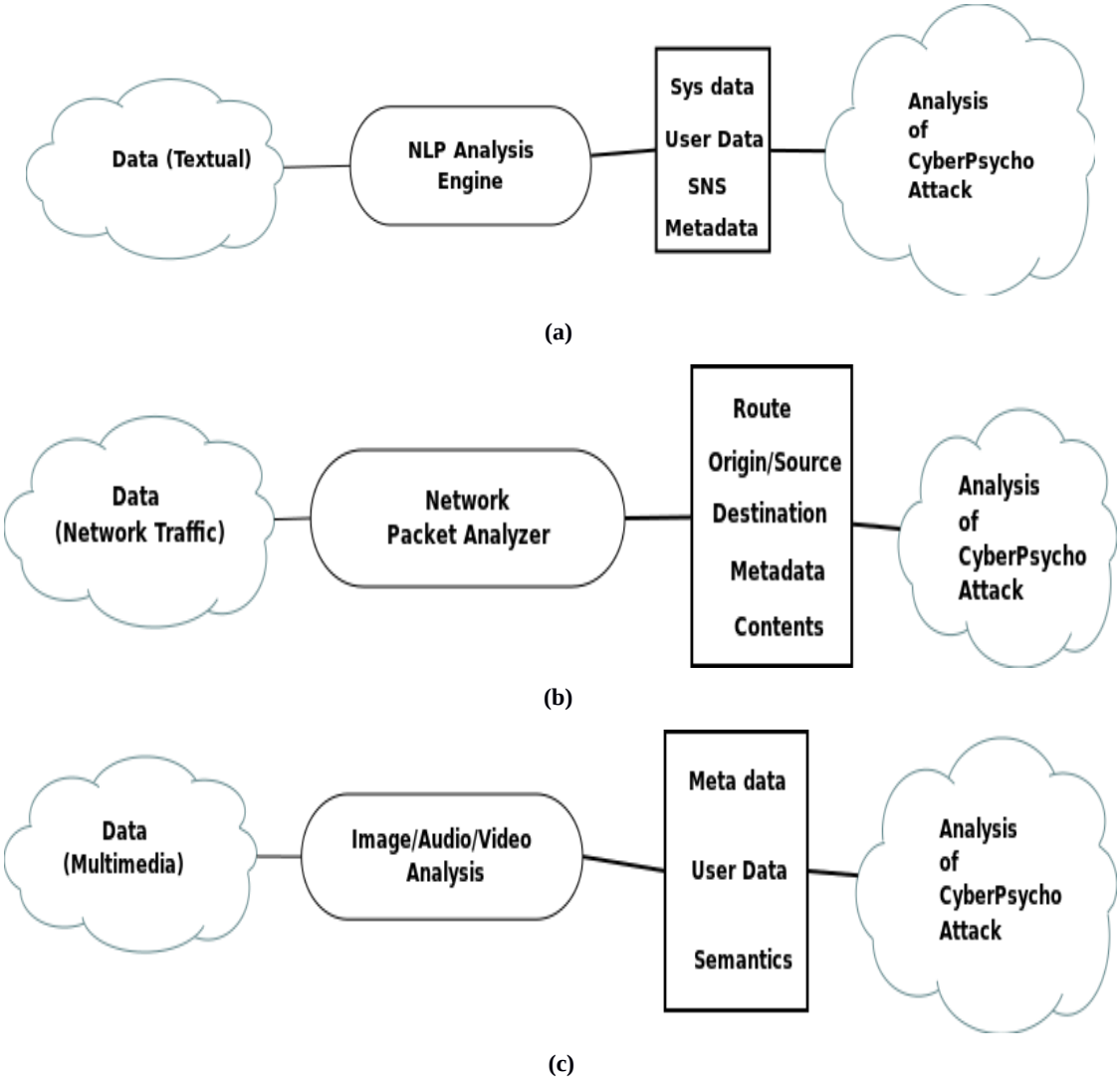


Figure 3: Proposed (a) Model-1 (b) Model-2 (c) Model-3 for Analysis of CyberPsycho Attack

6. CONCLUSION

Cyberpsycho attack is the most powerful and dangerous attack as it is lethal than any other weapon or tool either for cyber warfare or kinetic warfare because it can change behavior or attitude of not only one individual but also group of educated people or a society or in bigger the whole country. It may impacts on various domain like finance, politics, religion etc. Attacker can easily deploy the trigger without any physical appearance and hiding his identities. Now-a-days government have to stop internet services to control the effect. But this leads to disconnection of people from their networks and in a positive scenario current status of the situation and help can't be able to reach to end users. But organizations have to start working on such kind of activity through recording the communications over social media and stopping that services only at the place and time of some events that cause a bad impact but it has to be done a more better way, technological+psychological, to prevent any big impact.

The study in this paper introduce a new kind of attack and proposed approaches to analyzes attacks behavior which is completely different from previously defined cyber attacks. The study is unique, valuable and compels the experts in academia, researchers, technologists and end-users to understand & acknowledge the serious impact of psychological, social and cultural aspects of internet addiction. In this paper, we propose three fundamental models to address and analyze the above concerns. These three proposed models to identify occurrence of cyberpsycho attacks is the major contribution of this paper.

7. REFERENCES

[1] Vince Farhat, Bridget McCarthy and Richard Raysman, Holland & Knight LLP, The Practical Law Company white paper. Cyber Attacks: Prevention and Proactive Responses.

[2] http://www.digitalvidya.com/wp-content/uploads/2015/04/Top-Social-Media-Marketing-Case-Studies.pdf

[3] Wani, Gayatri, and Nilesh Alone. Survey on Impact of Social Media on Election System.

[4] Erika Lisa Panuccio. ISIS Network Warriors. Making Jihad on the web

[5] https://www.statista.com/topics/1164/social-networks/ accessed on 18 October 2016

[6] Yeo, A. C., Rahim, M. M., & Ren, Y. Y. (2008). Use of Persuasive Technology to Change End-Users' IT Security Aware Behaviour: A Pilot Study. World Academy of Science, Engineering and Technology, International Journal of Social, Behavioral, Educational, Economic, Business and Industrial Engineering, 2(10), 1086-1092.

[7] Wiederhold, B. K. (2014). The role of psychology in enhancing cyber-security. Cyberpsychology, Behavior, and Social Networking, 17(3), 131-132.

[8] Hong, J., Das, S., Kim, T. H. J., & Dabbish, L. Social Cybersecurity: Applying Social Psychology to Cybersecurity.

[9] Gharbaghi, A., Aris, B., Ahmad, M. H., & Rosli, M. S. (2013). Technological Persuasive Pedagogy: A New Way to Persuade Students in the Computer-based Mathematics Learning. Journal of Education and Practice, 4(14), 43-49.

[10] Zapico, J. L., Turpeinen, M., & Brandt, N. (2009, April). Climate persuasive services: changing behavior towards low-carbon lifestyles. In Proceedings of the 4th International Conference on Persuasive Technology (p. 14). ACM.

[11] Hyman, J. A. (2003). Computer vision based people tracking for motivating behavior in public spaces (Doctoral dissertation, Massachusetts Institute of Technology).

[12] Gao, H., Hu, J., Wilson, C., Li, Z., Chen, Y., & Zhao, B. Y. (2010, November). Detecting and characterizing social spam campaigns. In Proc of the 10th ACM SIGCOMM conf on Internet measurement (pp. 35-47). ACM.

[13] Shrivastava, N., Majumder, A., & Rastogi, R. (2008, April). Mining (social) network graphs to detect random link attacks. In 2008 IEEE 24th International Conference on Data Engineering (pp. 486-495). IEEE.

[14] Fogg B.J., Persuasive Technology: using computers to change what we think and do, Morgan Kaufmann Publishers, CA, 2003

[15] B. J. (1997, March). Captology: the study of computers as persuasive technologies. In CHI'97 Extended Abstracts on Human Factors in Computing Systems (pp. 129-129). ACM.