Cyberbullying Response System on SNS

Sei-Youen Oh

Abstract: ***The system is designed to search for cyberbullying-related data and to respond by phase to the cyberbullying on the basis of the data authenticity. In particular, each analyzed data is used for D/B for follow-up cyberbullying data authenticity identification and is stored in D/B for follow-up cyberbullying response, therefore preliminary cyberbullying crime signs will rapidly detect and ultimately, its consequent crime damage will be minimized.***

In terms of data collection and analysis, the proposed model collects cyberbullying data widely present in various forms, while the previous only collects limited data on Twitter. To complement another limitation of the previous, not being able to analyze video, image and freeform letters, the proposal utilizes SNA to analyze bullying data in freeform letter, image and abstract vocabulary. Furthermore, the existing model does not have DB for follow-up utilities, the proposed model applied a DB for follow-ups for more effective operations of cyberbullying data authenticity identification and response module. Cyberbullying crime response method has also been enhanced in its effectiveness, by enabling phased countermeasures, and storing and analyzing the processed result from response module, to respond to future cyberbullying. Consequently, the proposed model is designed to minimize probable victimized damages by improving effectiveness of rapid and accurate phased measures – via data collection and analysis module, expert system, knowledge-based database, D/B1 for follow-up cyberbullying data authenticity identification, crime response module and D/B2 for follow-up cyberbullying response.

The proposed Cyberbullying Response System on SNS enabled an enlarged volume and variety of SNS data collection, compared to the previous model, utilized SNA for analysis, enhanced preliminary prediction accuracy to future cyberbullying and allowed more rapid and adequate phased crime response against it – thus, crime damage from cyberbullying is expected to be minimized.

Keywords: Cyberbullying, SNS, Cyberbullying Response System, Social Network Analysis, Victims.

I. INTRODUCTION

Through recent generalization of smartphone supply and internet utility, cyber violence, such as cyberbullying and harassing, in our society has radically been increased and developed into a serious problem. Particularly, 1 out of 5 adolescents is addicted to smart-phone[1] and having the addicted adolescents discovered to more likely be exposed to cyberbullying, the seriousness of the harmful consequence from it can be assumed. Such cyberbullying occur in cyberspace, not in physical space, thus it is less perceived as a crime and its assailants rarely feel guilty [2,3]. Moreover, considering that victims may be bullied with no time and spatial constraint, thus extreme actions, including suicide, in the worst case, may be committed by the victims, hence, preparing pragmatic precautions and countermeasures against cyberbullying must be demanded above all.

Thus, the research recognizes the consequences of cyberbullying occurring particularly among adolescents in our community, and would like to propose Cyberbullying Response System on SNS to preliminarily minimize any possible damage through rapid and precise phased countermeasures.

II. THEORETICAL DICUSSION

A. Theoretical Discussion

- Concepts and Types of Cyberbullying

Definition of cyberbullying has been determined by various scholars - Patchin & Hinjuja(2006) defined as intentional, deliberate and repetitive harm via electronic devices [4], Smith et al(2008) as hostile and intentional behavior by an individual or a group via electronic devices against who is not capable of defending oneself[5]. In addition, traditional bullying and cyberbullying have a difference in that, while the former is generally when an individual is repetitively and consistently, but negatively exposed to another individual or a group, and the latter is repetitive and hostile practices or behaviors through electronic devices against who cannot effectively protect oneself [6].Observing terminologies of such cyberbullying, the United States and Canada have officially, since 1970s, designated harassments and ostracizing at school as bullying, Japan and Korea defined intentional and constant harassing behaviors against the weak under the power imbalance as Ijime and Wangdda. [7,8].

Cyberbullying types are diversely differentiated depending on their behaviors and contents, and linking them to relevant foreign and domestic types, 10 different categories may be listed as in Table 1[9,10].

Table- I : Cyberbullying Types

Cyberbullying Types	Contents	Related Foreign Cyberbullying Terminology	Related Domestic Cyberbullying Terminology
Cyber stalking	Behaviors inducing fear by sending words, writings, pictures and images through the Internet and smartphones despite of denial by a specific receiver	Cyber stalking	
Cyber slander	Spreading pictures or videos of a specific person that is unwanted to be disclosed to others, for criticism and insult	Happy slapping Photo-shopping	

Revised Manuscript Received on July 22, 2019.

***Sei-Youen Oh,** Department of Police Administration, Semyung University 65, Semyeong-ro, Jecheon-si, Chungcheongbuk-do, 27136, Republic of 1Korea. s092724@naver.com.

Cyber impersonation	Pretending to be a specific person on cyberspace by exploiting the ID	Impersonation Masquerading Identity theft	ID Theft
Cyber coercion	Forcing and sending a specific person on errands that are not desired by the person via the Internet and smartphones		Cyber Order Cyber Extortion Game-Item Shuttle Wi-Fi Shuttle
Sexting	Sending sexual messages or insults to a specific person	Sexting	
Cyber exclusion	Intentionally rejecting or excluding a particular person on cyberspace	Exclusion	Anti-Café
Flaming	Intentional behavior to provoke a specific person, to induce controversies or disputes, thus making the person in issues	Trolling Flaming	
Cyber outing	Revealing information of another without an agreement, which the specific person would not want to disclose	Outing	

- Recent Cyberbullying Status

2018 'Cyberbullying Actual Status Result' by Korea Communications Commission and National Information Society Agency indicates 32.8% of cyberbullying experience rate, that is, 3 out of 10 internet users either inflicted(21.6%) or were victimized(24.7%). Such figure presents 6.7% higher than the experience rate from the previous 2017 'Cyberbullying Actual Status' result and the number of cyberbullying reports has increased by year, 900 in 2012, 1,082 in 2013, 1,283 in 2014, 1,462 in 2015 and 2122 in 2016, thus the seriousness of cyberbullying among adolescents is presumable[11].

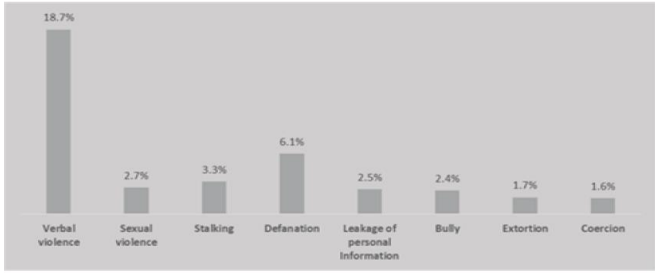


Figure 1: Cyberbullying Experience Rate by Type

Looking at the cyberbullying experience rate by type as in Figure 1, verbal violence(18.7%) was the highest, then defamation(6.1%), stalking(3.3%), sexual violence(2.7%), leakage of personal information(2.5%), outcast(2.3%), extortion(1.7%), coercion(1.6%)2 have followed. Furthermore, as in Figure 2 with causal means of cyberbullying, chatting, messenger and online games were the major channels for the commitments, and SNS, community, email, text messages, and personal homepage have been noticed as other possible crime spots[12].

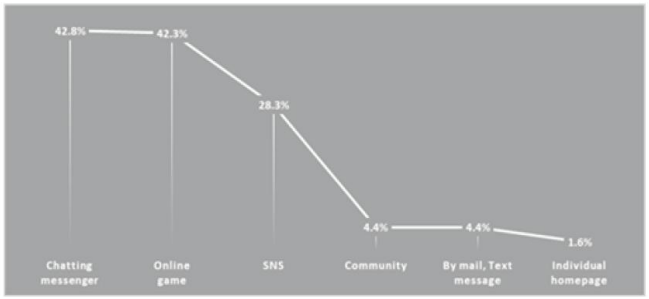


Figure 2: Causal Means of Cyberbullying

III. CYBERBULLYING RESPONSE SYSTEM ON SNS

A. System Composition

The system is to respond to cyberbullying by phase through discovering cyberbullying-related data on SNS and examining the data authenticity. Cyberbullying Response System on SNS figures out preliminary crime signs of cyberbullying, then ultimately is a system to minimize any possible crime damage. The system consists of 6 components - data collection and analysis module, expert system, knowledge-based database, D/B1 for follow-up cyberbullying data authenticity identification, crime response module and D/B2 for follow-up cyberbullying response.

- **Data Collection :** Data collection is all executed on SNS of users - Instagram, Twitter, Facebook and blogs. Data collection procedure involves collection of all cyberbullying data in word, image, video forms from all users of SNS - Instagram, Twitter, Facebook and blogs, then the collection is stored in D/B.
- **Data processing analysis Modules :** Data processing analysis Modules is a module to judge suspicious data of cyberbullying among the various data collections from SNS and to store them. This system utilizes expert system and knowledge-based database to examine the authenticity of the suspicious data. Moreover, as a mean to analyze the collected cyberbullying data, SNA(Social Network Analysis) is utilized. Such analysis method enables various outcomes, such as inferences via pictures, videos, images, standardized and freeform data, and even algorithms. Thus, in fact, huge amount of cyberbullying data can be analyzed.
- **Expert System/Knowledge-based Database:** Expert System/Knowledge-based Database is a system enabling authenticity confirmation and accurate data identification by matching the suspicious data in Data processing analysis Modules with other cyberbullying data stored in it.
- **Follow-up Utility D/B1 (D/B for Cyberbullying Data Authenticity Identification) :** Follow-up Utility D/B1 is a storage D/B for precisely confirmed data of cyberbullying after its authenticity is identified in its data state of suspicion. This D/B is used as cyberbullying judgement material D/B allowing more accurate and faster confirmation on data authenticity.

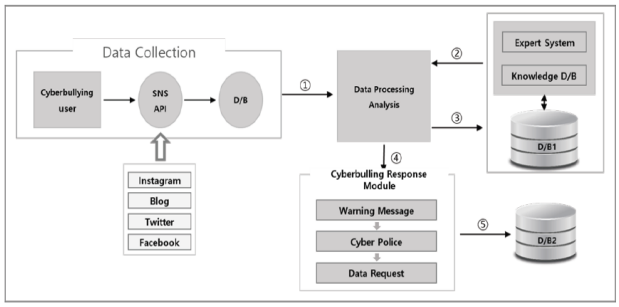
- **Cyberbullying Response Module:** Cyberbullying Response Module is a phased cyberbullying response module to minimize any damage from Cyberbullying accurately and rapidly based on the cyberbullying data extracted from Data processing analysis system.
- **Follow-up Utility D/B2 (Follow-up D/B for Cyberbullying Response) :** Follow-up Utility D/B2 is a D/B to predict and respond to any future cyberbullying more rapidly and accurately by storing processed result from the Cyberbullying Response Module.

B. Function process procedures of Proposed System

This system enables activation of phased cyberbullying response module by collecting suspicious data relevant to cyberbullying, then directly selecting data that matches to cyberbullying from the data collection in various forms - words, images and videos.

Therefore, Cyberbullying Response System on SNS as in below Figure 3.

Figure 3: Proposal Model System of Cyberbullying Response System on SNS



Sept 1: Among all SNS(Instagram, Twitter and Facebook) users, data of those who might have inflict or have been victimized in cyberbullying is collected and transferred to Cyberbullying processing analysis Modules. Cyberbullying processing analysis Modules judge and extract any suspicious cyberbullying data from the diverse collection in word, image and video forms.

Sept 2: Extracted data, being suspected to be cyberbullying related, is gone through matching process to identify its authenticity by means of expert system and knowledge-based database.

Sept 3: Confirmed cyberbullying data from expert System and knowledge-based database is transferred to and stored in D/B1.Transferred and stored data into D/B1 is re-sent to expert system and knowledge-based database so that the data can be used as a material to help future judgement of authenticity identification of other suspected data sets.

Sept 4: On the basis of cyberbullying data having its authenticity confirmed by Cyberbullying processing analysis Modules, cyberbullying response module is operated.

① Provide warning, alarm text messages to cyberbullying assailants, victims and guardians

② Notice to Cyber-police and Execute countermeasures

③ SNS enterprises are required, by Cyber-police, to provide basic data for investigation purposes

Sept 5: Transferring and storing the processed result from cyberbullying response module into D/B2, the data is utilized for probable future cyberbullying responses and prediction

IV. PROPOSED MODEL ASSESSMENT

As described in Table 2, the chapter would like to comparatively revise the existing, cyberbullying detection system[13], and the proposed, Cyberbullying Response system on SNS, in their effectiveness, functions and operations

Table- II: Name of the Table that justify the values

Category	Existing system	Proposed system
Data Collection	-Twitter -Collects only limited data in formal text and english word	-SNS -Collects all data in informal, abbreviation word, image and video
Data Analysis	-Utilize cyberbullying detection system to analyze data in formal text, english word	-Utilize SNA to analyze data in informal, abbreviation word, image and video -Utilize Expert System and Knowledge-based Database for extraction of suspicious data from comparative analysis
D/B	-Data Collection D/B -Consisting of System Database	-Data Collection D/B -Follow-up Utility D/B1 for Cyberbullying data authenticity identification -Follow-up Utility D/B2 for Cyberbullying response
Crime Response Operation Method and Utility	-Unitary crime response method -Disposal of analyzed data after usage	-Phased crime response method -Utilized as post-cyberbullying security material

First, in terms of data collection, the existing model only collects limited data in formal text and english word from Twitter, thus has difficulties in accurately gathering cyberbullying data widely existing on SNS such as Instagram, blogs and Facebook. However, the proposed model collects cyberbullying data from SNS - not only Twitter, but also Instagram, blogs and Facebook, hence enabled collection of more diversified data compared to the existing.

Second, in terms of their operations, the existing employs cyberbullying detection system only to analyze formal text and english word data on Twitter, thus any bullying data in image, video, abstract words and freeform letters could not be analyzed, however, the proposed one employs SNA to analyze data in informal, abbreviation word, image and video forms. Furthermore, having Expert System and Knowledge-based Database, comparative analysis and extraction of suspicious data were enabled, hence analysis on various cyberbullying data has become possible even with higher accuracy.

Third, in terms of DB, the existing model have D/B for cyberbullying data collection from Twitter and System Database having data judged to be cyberbullying data stored. However, the proposed model has D/B to collect cyberbullying data from SNS, D/B1 for follow-up authenticity identification of cyberbullying data and D/B2 for follow-up cyberbullying responses, therefore, data is separately stored and phased operations of all data authenticity identification and response modules have become much more effective.

Fourth, in terms of crime response methods, the existing model consists of warning for cyberbullying and police operations, thus practical evidence investigations is difficult and no progressive action to enhance crime response and countermeasures for the future is practiced. However, the proposed model enables selective phased operations and rapid evidence collection and stores processed result from Cyberbullying Response module and let it be utilized for future cyberbullying countermeasures, effectiveness to cope with cyberbullying has been increased, rapid crime response has been allowed and crime damage is minimized

V. CONCLUSION

As distribution of smartphones and the Internet utility have become generalized, recently, throughout the world, cyberbullying such as online harassment and outcast among adolescents has increased, and its consequence is severe. Particularly, as cyberbullying occurs on cyberspace, unlike other crime types such as school violence in physical space, assailants are less likely to perceive their guilt of violence or crime - hence, more serious crimes may be developed. In addition, compared to such seriousness of cyberbullying among adolescents, practical measures are significantly inadequate, thus cyberbullying is increasing and, in the worst cases, the victims are put to extreme actions, including suicide. Hence, preparation of practical remedies for cyberbullying prevention and countermeasure is urgently required than ever. Therefore, the research recognizes the severity of cyberbullying, complemented the existing cyberbullying response system on Twitter, thus proposed a system model with phased responses against cyberbullying enabled on SNS.

The system consists of 6 components - data collection and analysis module, expert system, knowledge-based database, D/B1 for follow-up cyberbullying data authenticity identification, crime response module and D/B2 for follow-up cyberbullying response - and crime damage from cyberbullying is expected to be minimized through collecting, analyzing, storing and utilizing the huge cyberbullying data on SNS via each part and module, and allowing rapid and accurate phased responses.

REFERENCES

1. http://www.sjbnews.com/news/articleView.html?idxno=623166.
2. K. L. Mason, “Cyberbulling: A preliminary assessment for school personnel”, Psychology in the Schools, 45(4), 2008, pp. 323-348. https://doi.org/10.1002/pits.20301.
3. J. W. Patchin, S. Hinduja, “ Assessing Concerns and issuse about the meditation of technology cyberbullying”, Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 2(2), 2008, pp. 1-12. https://cyberpsychology.eu/article/view/4214/3256.
4. J. W. Patchin, S. Hinduja, “ Bullies move beyond the schoolyard: A preliminary look at cyberbullying”, Journal of Youth Violence & Juvenile Justice, 4(2), 2006, pp.148-169. https://doi.org/ 10.1177/1541204006286288.
5. P. K. Smith, J. Mahdavi, M. Carvalho, S. Fisher, S. Russell, N. Tippett, “Cyberbullying: its nature and impact in secondary school pupils”, Journal of Child Psychol Psychiatry, 49(4), 2008, pp.376-385. https://doi.org/ 10.1111/j.1469-7610.2007.01846.x.
6. R. Slonje, Smith, .P. K. Frisen, A. “The nature of cyberbullying and strategies for prevention”, Journal of computer in human behavior, 29, 2003, pp. 26-32. https://doi.org/10.1016/j.chb.2012.05.024.
7. D. Olweus, Sweden. In Smith, P. K, Morita, Y, Junger-Tas, J, D. Olweus, r. R. Catalano, P. Slee, (1999) (Eds), The Nature of School Bullying: A Cross-National Perspective. London & New York: Routledge; 7–27, 1999a.
8. Ika Yunida Anggraini, Sucipto Sucipto, Rini Indriati, “Cyberbullying Detection Modelling at Twitter Social Networking”, Journal of Informatika, 6(2), 2018, pp. 113-118. https://doi.org/ 10.30595/juita.v6i2.3350
9. S. Y. Choi, “A study of the review of research on cyberbullying and Its responding strategy”, Journal of Communications of the Korean Association of Computer Education, 17(6), 2014, pp. 35-48. http://www.earticle.net/Public/Detail/1/1388/2657?code=1230577.
10. Y. O. Cho, “The Impact of Cyber Bullying Victim Experience and the Influence of Mediating Effect of Depression on Delinquent Behaviors”, Journal of Korean journal of youth studies, 20(10), 2013, pp. 117-142. http://www.riss.kr/search/detail/DetailView.do.
11. National Information Society Agency, A Survey on the actual cyberbullying in 2017, 2017.
12. Korea Communication Commission, Nation Information Society Agency. A Cyberbullying Survey in 2018. NIA, 2018.
13. C. H, Liew, D. V. Kasturi, “Cyberbullying Detection System on Twitter”, International Journal of Information System and Engineering, 1(1), 2005, pp. 1-11. https://doi.org/10.24924/ijise/2015.04/v3.iss1/36.47

AUTHORS PROFILE

Sei-Youen Oh, I got my Ph.D. in Criminology at Dongguk University(Title of thesis: A Study of police response to domestic violence, 2009). I am currently a professor of police administration at Semyung University. My research interests are convergence research between IT, criminology and police science. Recently published papers are “A study on preventive system against recidivism of retaliatory crime using IoT-based smart watch”(2018). “A Comparative Study on AI-based Anti-terror Crime System”(2019), etc.