J Inf Process Syst, Vol.13, No.3, pp.559~572, June 2017
https://doi.org/10.3745/JIPS.04.0033

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

Cyberbullying and a Mobile Game App? An Initial Perspective on an Alternative Solution

Manmeet Mahinderjit Singh*, Ping Jie Ng*, Kar Ming Yap*, Mohd Heikal Husin*, and Nurul Hashimah Ahamed Hassain Malim*

Abstract
Cyberbullying has been an emerging issue in recent years where research has revealed that users generally spend an increasing amount of time in social networks and forums to keep connected with each other. However, issue arises when cyberbullies are able to reach their victims through these social media platforms. There are different types of cyberbullying and like traditional bullying; it causes victims to feel overly self-conscious, increases their tendency to self-harm and generally affects their mental state negatively. Such situations occur due to security issues such as user anonymity and the lack of content restrictions in some social networks or web forums. In this paper, we highlight the existing solutions, which are Intrusion Prevention System and Intrusion Detection System from a number of researchers. However, even with such solutions, cyberbullying acts still occurs at an alarming rate. As such, we proposed an alternative solution that aims to prevent cyberbullying activities at a younger age, e.g., young children. The application would provide an alternative method to preventing cyberbullying activities among the younger generations in the future.

Keywords
Cyberbullying, Digital Etiquette, Intrusion Detection System, Mobile Application, Social Network

1. Introduction

With the emergence of information and communication technologies, the realm of offline and online life has lesser variances. Activities conducted in real life are now commonly expressed virtually. In fact, people are more active in the virtual space rather than real-life [1]. This has led to loads of inspiring technology that aimed at facilitating people in their daily chores and activities such as the Internet. The Internet offers applications such as e-commerce and mobile commerce that simplifies groceries whilst the social networks such as Facebook, Twitter and Instagram abridge physical distances between communicating users. Internet has made people stay put at home but they virtually able to move all over the globe in a single click. However, as with any technology, its usage can be for the common good or evil depending on the user. The Internet is among the most miss-used technology where the number of crimes (a.k.a. cybercrimes) are increasing yearly since its first introduction in 1990s. The seriousness of these crimes has led to the introduction of cyberlaws that is used to govern the security of the

Manuscript received March 10, 2016; first revision November 29, 2016; second revision February 9, 2017; accepted February 10, 2017.
Corresponding Author: Mohd Heikal Husin (heikal@usm.my)
* School of Computer Sciences, Universiti Sains Malaysia, Pulau Pinang, Malaysia (manmeet@usm.my, {pingjie.ng, karming89}@gmail.com, nurulhashimah@usm.my)

Internet (a.k.a. cybersecurity). Cybercrime is defined as a form of behavior mediated by networked technology that causes harm to users having access to the networked [2].

There are various types of cybercrimes that are specifically tied to applications in the internet. One of the most prominent cybercrimes that currently occurs is cyberbullying. Cyberbullying could be defined as a reflection of physical or verbal (traditional) bullying from a virtual perspective. The aforementioned aggressive behavior is transformed into aggressive online acts that are carried out using electronic means (such as sarcasm via status update, violation of privacy, etc.) by individuals or groups of people on another individual or group repetitively over time. This crime occurs more frequently as one of the heavily utilized services or application on the Internet is a social media or social networks platform. Platforms such as Facebook and Twitter provides an unrestricted way for users to express their opinions to a wider audience. As these platforms has a wide reach, such aggressive acts are able to executed from all over the world as easy as hitting the Enter key on the keyboard.

The statistics recorded in 2010 by the Cyberbullying Research Center [3] based on a sample taken for 10- to 18-year-olds from large school district in the Southern United States indicates that 20% of the sample have experienced cyberbullying in their lifetime and the remaining have experienced numerous cyberbullying acts in a period of 30 days. This clearly designates that the impact of cyberbullying drills down to the teenage whom are more familiar with emerging technologies more than the elder who may see these technologies as alien. In fact, Patchin and Hinduja [4] concluded that about one of every four teens has experienced cyberbullying, and about one of every six teens has done it to others. Hence, prevention measures are essentials to curb cyberbully especially looking at the impact on the teenage. The current approaches used in the United States is to emphasize on early education to prevent misused of technologies that would lead to cyberbullying. This approach is achieved by the introduction of a course in the primary schools called Digital Citizenship [5]. In this course, school children are exposed to appropriate conduct that they should observed while online and being aware on malicious bullying attempts imposed by their online mates onto themselves.

Cyberbullying has received a lot of attention from both the media and government sector. Compared to traditional bullying, cyberbullying is comparatively harder to detect and in most cases, the victims find it difficult to protect themselves from the heinous activity. Recently, there was a case in Malaysia where a woman driver turned into a road bully after a minor accident, became the victim of some vicious cyberbullying when her personal details were uploaded online by another motorist who witness the incident [6]. The public went started to abuse her even though the victim, an elderly man has forgiven her actions. There are a number of policies, preventive methods, empirical studies and analysis regarding cyberbullying in different countries conducted by different researchers. This paper is aimed at discussing the acts of cyberbullying that encompasses its definition and real-life sample cases related as well as the related preventive measures to the activity. Since, it has been highlighted that the most impacted age group are teenagers in our previous research paper [7], this paper would use the initial survey findings focusing on cyberbullying from that paper on the awareness of Malaysian children on the importance of digital etiquette collected in Malaysia. We then further propose an initial mobile digital etiquette game application as an early prevention approach to stem such negative act at its roots.

This paper outlines the background study of cyberbullying in Section 2 followed by the discussion on the related real-life cases in Section 3. In Section 4, a broad range of cyberbullying detection and prevention methods are highlighted. Whilst in Section 5, a different approach via game-based learning is proposed to educate children to better protect themselves in the cyberspace. Section 6 concludes the paper.

2. Background Study

The definition of cyberbullying is an extension of traditional bullying where "an aggressive act or behavior that is carried out using electronic means by a group or an individual repeatedly and over time against a victim who cannot easily defend him or herself" [8]. Traditional bullying is generally seen as an intentional behavior to harm a subject repeatedly where there is an imbalance of physical or mental power.

2.1 Difference between Traditional Bullying and Cyberbullying

Cyberbullying differs from traditional bullying in two major sections: repetition and power imbalance. From the context of repetition, the initial perpetrator does not always continue repeating a harmful act in cyberbullying. As an example, the sexting cases that lead to tragic incidents such as suicides of J. Logan and H. Witsell mention by Hinduja and Patchin [9], highlighted that the repetition harm was not only caused by the initial perpetrator but also by other individuals who repeated the act of the initial perpetrator (spreading nude photos and insults towards the victim). The power imbalance context in traditional bullying is defined where the victim is considered 'weak' in terms of physically or psychological; or it can also be considered as the virtue of numbers or popularity in a peer group context [8]. As such, the traditional definition of power imbalance is not appropriate in the context of cyberbullying as physical and psychological strength or even the virtue of numbers is necessary for the perpetration of cyberbullying. The two types of power imbalance that only occurs in cyberbullying but not within traditional bullying is the technical ability with ICTs (information and communications technology), and anonymity.

Cyberbullies are usually equipped with some knowledge of technical ability with ICT. However, technological skill is arguably a minor factor as mentioned by Slonje et al. [8] due to cyberbullying can occur even through simple texting. With the advent of social media platforms, dissemination of content over the Internet has become easier due to the sharing capability provided within various social network sites [9]. Anonymity in the sense of power imbalance is that the victim only knows someone out there is actively bullying them without having any clue regarding the identity of the actual perpetrator. In most cases, the victims are not aware of alternative ways of defending themselves against the anonymous perpetrator. Through the usage of social network or social media platforms, creating a new user account is as easy as creating a new email account. The case studies, which would be presented later in the paper, will highlight the simplicity of these factors.

2.2 Types of Cyberbullying

Griezel et al. [11] mentioned that bullying could be conducted in different forms. Traditional bullying can be broken down into three different forms: physical (e.g., punching), verbal (e.g., name calling), and social (e.g., rumor spreading); where cyberbullying consist of two forms: visual and text. Examples of visual and text are shown below:

- Sending nasty text messages, emails, and instant chat messages
- Forwarding confidential emails or instant text messages to other students
- Bombarding a student with hurtful text messages

- Setting up a public derogatory website or profile page about a student
- Using a mobile phone camera to video or photograph another student to embarrass them

Su and Holt [12] as well as Feinberg and Robey [13] define cyberbullying into more detail forms which includes flaming, harassment and stalking, denigration, impersonation, outing and trickery, and lastly exclusion. Most of cyberbullying related cases falls into one or more of the above categories [13]. The categories are highlighted by Feinberg and Robey [13] below:

- Flaming: Online fights using electronic messages with angry and vulgar language.
- Harassment and stalking: Repeatedly sending cruel, vicious, or threatening messages.
- Denigration: Sending or posting gossip or rumors about a person to damage their reputation or friendships.
- Impersonation and masquerading: Breaking into someone's e-mail account and using it to send vicious or embarrassing material to others.
- Outing and trickery: Engaging someone in instant messaging, tricking him or her into revealing sensitive information, and forwarding that information to others.
- Exclusion: Intentionally excluding someone from an online group.

This categorization of cyberbullying forms would be highlighted and shown in the next section.

2.3 Cyberbullying Cases

2.3.1 Sexting (harassment, outing, and trickery)

Jessica Logan [14], Hope Witsell [9] and Rehtaeh Parsons [15] were victims of sexting, which led all of them committing suicide after enduring pressure and depression due to the bullying they faced. There is still a lot of sexting victim and cases happen around this world. Their experience should be considered as serious and high profile cases in sexting. A simple way to define sexting is "the sending or receiving of sexually-explicit or sexually-suggestive images or video via a cell phone", this can also be extended to different kind of electronic media such as email, social network, instant messages application and also video chat [9].

Sexting is a combination of cyberbullying forms, which consist of outing and trickery where the perpetrator tries to get sexually explicit images or video from the victim. The perpetrator would then share and spread out that sensitive content to others. The issue with sexting is that there is no security checking and detection in the internet. Freedom of speech on the internet has allowed users to post anything they want without much restrictions. The act of sharing nude photos on the internet via social networks is not heavily controlled under the law enforcement as compared to porn websites. Currently, there are no effective method of tracing the photo or video posted in social network or internet; whether the file is duplicated, downloaded, and shared by others without the permission of the owner itself.

2.3.2 Privacy context-user anonymity (harassment, impersonation, and masquerading)

Bullycide is a term used to refer victim that suicides due to bullying whether in person or through social media. The case highlighted in this section involves a 13-year-old young girl named Megan Meier from Missouri. It begins when she gets to know a 16-year-old boy named Josh Evans through MySpace.

On one particular day, she received a message from Josh that says: "I don't know if I want to be friends with you anymore because I've heard that you are not very nice to your friends." [16]. Bulletins about her was posted which led to her harassment by her schoolmates. In October 2006, her parents found her hanged in her closet and rushed her to the hospital but it was too late. She died on the following day.

Through the police investigation, it was found that the boy Josh was actually a fake identity created by Lori Drew, who is the mother of Megan's former friend, Sarah. Drew claimed that the reason she did this is to use the contents of the email conversations she had with Megan to shame her as retribution for spreading gossips about her daughter Sarah. User anonymity is a privacy issue related to user authenticity in social networks. Users are able to create multiple accounts by utilizing different email addresses. In addition to being anonymous, pseudonomity is an issue as well where emails are used as a mean to hide the identity of the sender. The concealment of user identity that is meant to protect user identity and preserve user privacy could be harmful from a social media context. Bullies could utilize these fake accounts to denigrate and flame victims. There were also users masquerading as another individual to make unusual request such as sexual encounters.

2.3.3 Workplace cyberbullying (denigration, harassment, and exclusion)

Cyberbullying is not just an issue among teens or children. Many adults also experience some form of cyberbullying while at work. Such a situation occurs more commonly in the recent years as more social network platforms are utilized within a business environment [1]. A joint research conducted in 2012 by the University of Nottingham and University of Sheffield with 320 respondents, found that "around eight out of ten employees had experienced bullying behaviour…at least one occasion in the previous six months" [17]. Cyberbullying within the workplace usually occurs at a more subtle level and remain undetected for some time the victims are more prone to keeping quiet on the fear of losing their jobs [18]. Current research highlights that there are three standard characteristics that is usually linked to workplace cyberbullying [19]: (i) it is persistent, (ii) frequent, and (iii) entails a power imbalance.

Some of the examples of cyberbullying within the workplace include withholding information among employees, spreading rumors or gossip and harassment via email or social networks [20]. Workplace cyberbullying can negatively affect not only the individual or victim but also lead to an increase of employee turnover and decrease the commitment of employees within an organization [21]. One of the researcher from the study also highlighted that "those that had experienced cyberbullying tended to have higher mental strain and lower job satisfaction". This is due to the impact of cyberbullying being seen by a wider audience compared to offline bullying [22]. Indirectly, the victims of cyberbullying could also face hostile reactions and ridicule from their colleagues.

3. Existing Cyberbullying Detection Approaches

The issue of cyberbullying within the social network needs to be tackled proactively. Any form of cyberbullying act involves two parties, which is the victim and the bully. To-date, there are two approaches in tackling cyberbullying act which is preventing the act from occurring in the first place and detecting the act once a bully message has been generated. As prevention is more effective than detection, the need for both mechanisms in placed is undoubtly important.

Intrusion Prevention System (IPS) is utilized as the 'first line of defense' and able to actively prevent intrusions that are detected through several approaches: sending an alarm notification to the appropriate authority, resetting connections or even blocking the offending IP address [23]. Another means for prevention system is through utilization of user training and guidelines to instill ethical usage of social networks [24]. If the IPS fails to do the required actions, the Intrusion Detection System (IDS) would attempt to detect the said intrusion. The detection system is capable of detecting any keywords used which depicts the nature of the bully or the act of bullying [25,26]. By identifying intrusions through misuse (well-defined attacks / specific actions being performed on specific objects with known weak points), anomaly (activity deviations from what is considered normal usage patterns) or hybrid (a combination of both misuse and anomaly intrusions), IDS systems are able to detect any form of bullying activity [27].

The main feature used in detecting such acts is through the identification of immoral (areas that are considered evil or wrong according to theory of ethics) and amoral (exhibiting indifference to codes of society) keywords [28]. Two examples of an IDS are the SybilRank by Cao et al. [29] and Information Distiller, Profile Hunter and Profile Verifier by Kontaxis et al. [30]. SybilRank uses an early-terminated random walk starting from a non-Sybil node and rank nodes in this social graph according to degree-normalized probability. This solution will screen out low-ranked nodes as potential fake user. In their paper, Sybil refers to the likelihood that the user is a fake account.

The Information Distiller, Profile Hunter and Profile Verifier Detection of social network profile cloning method as proposed in Kontaxis et al. [30] consists of three functions. Information distiller would extract information from legitimate social network profiles. Rare or user-specific information pieces will be labelled as the user- identifying terms and used to create a user-record through the detection system. This record will pass on to the next system component, Profile Hunter that will utilize the records to locate related social network profiles that may potentially belong to the user. The last component of this solution processes the profile-records and checks the similarity of those profiles with a user original profile. The similarity score along with those profiles will be listed which can be used by the social network providers to remove any duplicated profiles.

However, even with the development of both IPS and IDS approaches, cyberbullying acts seems to occur consistently and more widely. It should be noted that the existing approaches are more focused on early detection of cyberbullying activities where the users are at an older age [31,32]. It has been noted that such activities could be prevented if an early prevention approach or method could be implemented [13,22]. As such, the direction of this paper is not focus in text mining or detection system in depth but more on the early prevention of such acts.

4. Proposed Cyberbullying Prevention via Mobile Digital Etiquette Application

Early empirical studies has indicated that the act of bullying is a gradual evolving process, which involves indirect and discreet approaches [33]. The causes of bullying stems from two main issues: (1) the role of the personality of the victims or bully perpetrator and (2) the role of psychosocial factors. These issues include somatic symptoms, social problems, thought problems, aggression and externalizing problems exhibited mainly by the perpetrator [31]. Victims of bullying on the other hand, have been

found to differ in terms of personality such as being oversensitive, having low self-esteem and feelings of anxiousness in social settings [33]. These traditional bullying causes are made worse as social media platforms are heavily utilized especially among the younger generation [34]. Thus, cyberbullying has a far-reaching impact and audience.

As highlighted by Slonje et al. [8] and the European Network and Information Security Agency [35], educational training on ethics is essential among users where such training could be viewed as a prevention method. As most of the cyberbullying activities are targeted towards children below 7 years old as shown in relevant works [36,37], we decided to focus on a particular age group in order to prevent future cyberbullying activities. We focused on Malaysian primary school students as the number of cyberbullying cases within Malaysia are increasing exponentially as more young children are exposed to the online environment [38,39]. Our initial research [7] has found that children between the ages of 7- to 12-year-olds are not usually aware of good online etiquettes. Our questions developed for our initial research was based around what is considered as online social norms [40]. Most of the students from our initial research only accessed digital etiquette training while they were at school that could be due to specific class syllabus in their school that promotes such training. A majority of the current game-based learning applications are based on the PC platform with limited online mobile accessibility [41,42]. With the current number of mobile devices usage among the younger generation, it was more suitable to develop a mobile based application as there is a low number of applications for digital ethics training especially on the Android platform [43]. Our initial application is aptly called Mobile Digital Etiquette Game (MDEG) trains primary school children through scenario-based questions, which would be more suitable for their age. The students are also tested on their understanding through a combination of questions such as true/false and multiple-choice questions. The game application would consist of three sections as shown in Table 1 whilst the system architecture is shown in Fig. 1. Such an application would provide another alternative method in preventing cyberbullying activities in the future.

Table 1. Proposed application sections for MDEG

	Aim	Proposed approach
Learning/Training section	To provide sufficient and clear training for the user on good online netiquette. Explanations would be designed to introduce ethical jargons slowly at the same time focusing on simple scenarios.	The learning would consist of three levels game-based learning that encompasses three popular games for children. These games are the Mix & Match Challenge, The Snake & Ladder and Scrabble. Each of these would be designed with situation case studies (topics) where related online etiquettes are highlighted.
Exam/Test section	To test the understanding of the user on online netiquette in a fun approach.	The questions in this section would utilized a variety of question formats such as True/False and multiple choices in order to capture the user's attention. This section would use the badge reward system in order to to promote a sense of achievement for the user upon completing the questions. A timer would be utilized for a sense of competitiveness that are normally exist within games. The user would be scored at the end of the section.
Score section	To provide a benchmark indicator for the user.	The user is able to review their previous score. We are proposing that this section would highlight some of the mistakes that the user has done with the exam questions. Such approach would improve the user's understanding on online netiquette.

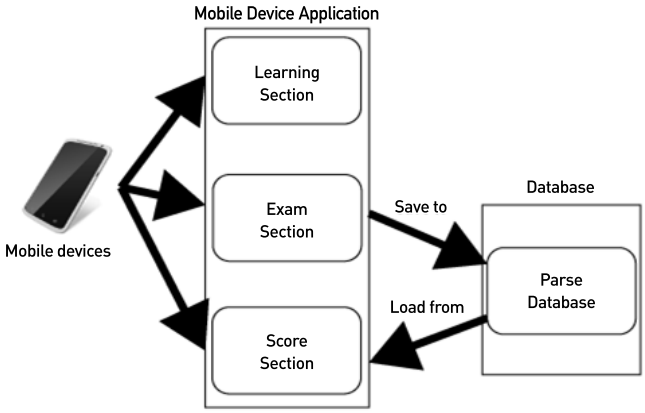

Fig. 1. System overview of the MDEG application.

The application is divided into three main sections mainly called (1) Learning/Training section where the information on good online netiquette is provided via simple scenarios that the users could easily follow; (2) Exam/Test section is the area that the understanding of the users are tested based on the topics taught in the first section; and lastly (3) Score section. This section provides additional information on the test results that the users have undertaken. These three sections were designed according to the recommendation of a flipped classroom approach where the students are provided with a participative learning environment that "seeks to engage students in an authentic problem solving and self-directed learning" [32,44]. Table 1 highlights the aims of the relevant sections as well as our proposed approach.

The main essence of the MDEG application would be directed towards tackling the issue of cyberbullying and educating target users on good practices in curbing the cyberbullying issue at an early stage. Enhancement of the cyberbullying method used here is at the level of prevention rather than detection. The outcome of this proposed application will become the initial step in designing a better application module of both prevention and detection in the near future.

5. Interface Design and Initial Testing

5.1 Interface Design

As part of this initial proposed development, we have designed the interface in a homogenous manner. The interfaces are separated into the three different sections as highlighted in Table 1. Fig. 2 shows the main interface of our proposed application. The user can invoke the option function or start the game function.

When the user selects the 'Start' option, they will be presented with the three main sections as depicted in Table 1. Fig. 3 highlights the 'Start' menu interface. User could select the sections that they would like to access: learning, exam or score.

As mentioned, one of the games that we have proposed in our application is the Snake & Ladder game. For the game, a virtual character is shown on the screen. It will begin from the start point where users would be asked a random question which is based on the training information provided in the

application. The overall logic of the game dictates that if the question is answered correctly, the virtual character will move forward based on a randomly generated number of tiles while an incorrect answer would lead to the character to moving backwards based on the random tiles. Fig. 4 highlights the overall board for the Snake and Ladder game.

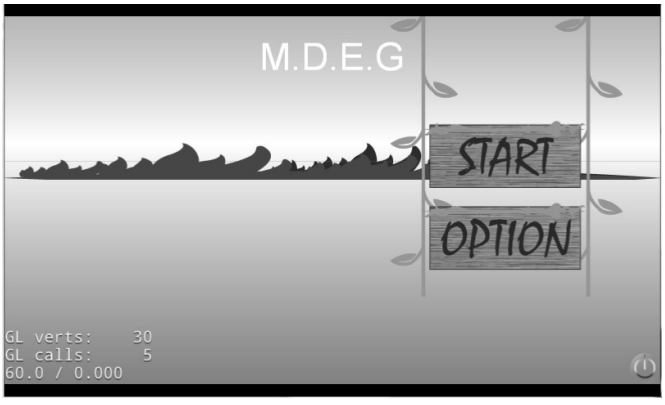

Fig. 2. Main menu interface.

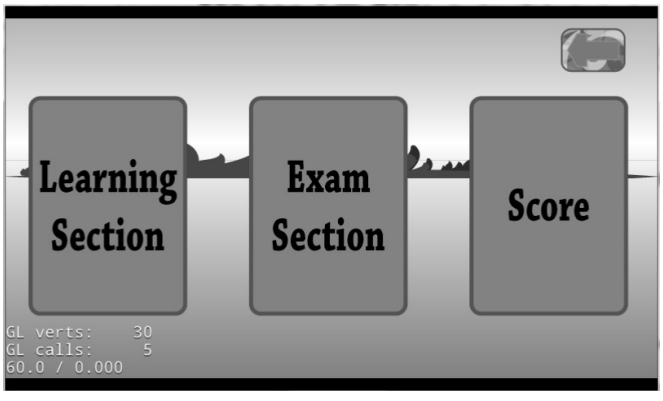

Fig. 3. Start menu interface.

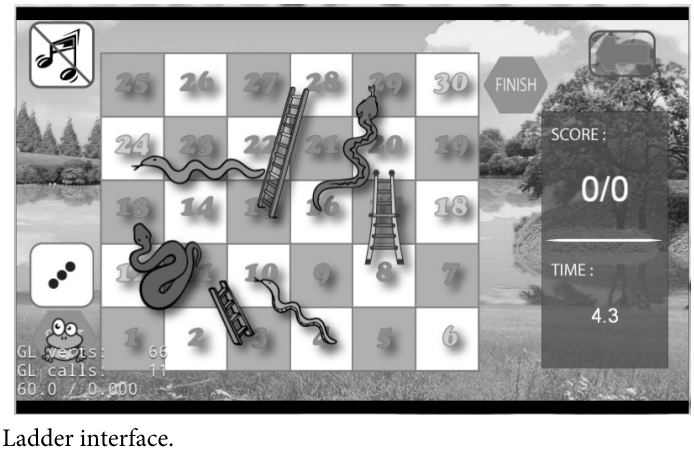

Fig. 4. Snake and Ladder interface.

5.2 Initial System Testing

As this is a newly developed system, we have conducted an initial unit testing to ensure that all the relevant components are working effectively. Tables 2 and 3 highlights some of the testing that we have conducted on the proposed application.

Table 2. Test case 1

Use case/ scenario	Test case	Initialization	Test input	Expected result	Test procedure
SA-0001	SA-0001	Avatar movement	-	Avatar moves tile by tile.	Avatar reached the destination with shortest distance path
SA-0002	SA-0002	Time display	Generates the time from the system.	Time will display in second with 1 decimal place.	Shown in floating point form with long decimal places.
SA-0003	SA-0003	Detection of the avatar when falls in trap tiles.	-	The check trap function is only carry out once per the avatar current location	Multiple times of testing with each trap in the board.
SA-0004	SA-0004	Failed to bounce back from victory tiles	-	The extra movement of frog will be bounce back from the victory tiles.	Multiple times of testing with different dice number.

Table 3. Test case 2

Use case/ scenario	Test case	Initialization	Test input	Expected result	Test procedure
SB-0001	SB-0001	Failed to flip the card back to close if the pair is not matched.	-	The cards will flip back to close if the pair is not matched.	Multiple times of testing with the different location of the card from the application.
SB-0002	SB-0002	Failed to maintain the card as open status if the pair is matched.	-	The cards will stay open if the pair is matched.	Multiple times of testing with the different location of the card from the application.
SB-0003	SB-0003	Failed to proceed to next question after all pairs are matched.	-	Will proceed to next question or show success message if all pairs are matched up.	Multiple times of testing with the different location of the card from the application.
SB-0004	SB-0004	Failed to kill all cards after the question is done.	-	All the previous question cards will be removed when proceeding to next question.	Multiple times of testing with the different location of the card from the application.

Further testing would be implemented specifically on the user testing once the application has been fully developed. The development of this application would enable the target users specifically among the younger generation to be more equipped with basic digital ethics knowledge. By implementing a game based training, it could attract the younger generation by tapping into their interest with games while providing sufficient information on different digital ethics topic such as cyberbullying, plagiarism and digital etiquette. The incentive of employing games application as a mean to strengthen awareness on the risk of cyberbully and educate students in understanding the cyberbully pheonema as whole. Overall, the main findings of this research shows that digital ethics training could be provided in a game based application by designing the interfaces to suit the target demographic. Beside that, further user evaluations would be beneficial in enhancing the application

6. Conclusion and Future Work

Throughout the literature review, there are findings that cyberbullying comes in different kinds of form. Cyber bulling is a serious issue as it affects not only individuals but also the wider community such as business organizations. There are no definite ways to prevent cyberbullying but there are approaches that can be undertaken to reduce the rate of cyberbullying acts. The advancement of technology and the mobility of mobile devices also allows cyber bullies to attack their victim anytime and anywhere. Therefore, the solutions within this paper are catered to address the issues in social media platforms, as these portals are the current main channel for cyberbullying activities. Some of the solutions are complicated to be implemented due to the complexity of the algorithm and legal acts such as the freedom of speech. The lack of policies and legal laws that could tackle such cyberbullying activities effectively also could complicate the existing solutions. As such, by tackling the issue at an early stage especially among the younger generation, cyberbullying activities could be prevented.

For our future work, we aim to improve our digital etiquette application so it could cover a wider range of users such as teens and adults. Such enhancement would require further examination into the usage behaviours and level of understanding among those users.

References

[1] R. Hanna, A. Rohm, and V. L. Crittenden, "We're all connected: the power of the social media ecosystem," *Business Horizons*, vol. 54, no. 3, pp. 265-273, 2011.

[2] D. S. Wall, *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge, MA: Polity Press, 2007.

[3] S. Hinduja and J. W. Patchin, "Bullying, cyberbullying, and suicide," *Archives of Suicide Research*, vol. 14, no. 3, pp. 206-221, 2010.

[4] J. W. Patchin and S. Hinduja, *Cyberbullying Prevention and Response: Expert Perspectives*. New York, NY: Routledge, 2012.

[5] M. Ribble, *Digital Citizenship in Schools*, 2nd ed. Eugene, OR: International Society for Technology in Education, 2011.

[6] D. Murad, N. H. Rodzi, and T. Avineshwaran, "Angry woman driver becomes cyberbullying victim," 2014 [Online]. Available: http://www.thestar.com.my/News/Nation/2014/07/17/Road-rage-leads-to-outrage-Angry-woman-driver-becomes-cyber-bullying-victim/.

[7] N. A. Rahman, N. S. Razali, S. A. Mohd Ali, N. H. Ahamed Hassain Malim, M. H. Husin, and M. M. Singh, "Digital etiquette: educating primary school children via mobile game application," in *Proceedings of the 7th Knowledge Management International (KMICe2014)*, Langkawi, Malaysia, 2014.

[8] R. Slonje, P. K. Smith, and A. Frisen, "The nature of cyberbullying, and strategies for prevention," *Computers in Human Behavior*, vol. 29, no. 1, pp. 26-32, 2013.

[9] S. Hinduja and J. W. Patchin, "Sexting: a brief guide for educators and parents," 2010 [Online]. Available: http://cyberbullying.org/sexting-a-brief-guide-for-educators-and-parents-2.

[10] M. H. Husin, G. Deegan, and N. Evans, "Social twins: Enterprise 2.0 and Government 2.0," *European Journal of ePractice*, vol. 2012, no. 17, pp. 51-67, 2012.

[11] L. Griezel, R. G. Craven, A. S. Yeung, and L. R. Finger, "The development of a multi-dimensional measure of cyber bullying," in *Proceedings of Australian Association for Research in Education*, Brisbane, 2008.

[12] C. Su and T. J. Holt, "Cyber bullying in Chinese Web Forums: an examination of nature and extent," *International Journal of Cyber Criminology*, vol. 4, no. 1-2, pp. 672-684, 2010.

[13] T. Feinberg and N. Robey, "Cyberbullying: intervention and prevention strategies," *National Association of School Psychologists: Communique*, vol. 38, no. 4, pp. 22-24, 2009.

[14] D. Siegle, "Cyberbullying and sexting: technology abuses of the 21st century," *Gifted Child Today*, vol. 33, no. 2, pp. 14-65, 2010.

[15] P. Newton, "Canadian teen commits suicide after alleged rape, bullying," 2013 [Online]. Available: http://edition.cnn.com/2013/04/10/justice/canada-teen-suicide.

[16] N. M. Aune, "Cyberbullying," 2009 [Online]. Available: http://www2.uwstout.edu/content/lib/thesis/2009/2009aunen.pdf.

[17] L. Brooke, "Punched from the screen: workplace cyber bullying becoming more widespread," 2012 [Online]. Available: http://www.nottingham.ac.uk/news/pressreleases/2012/november/punched-from-the-screen---workplace-cyber-bullying.aspx.

[18] M. S. Hershcovis, "Incivility, social undermining, bullying…oh my!: a call to reconcile constructs within workplace aggression research," *Journal of Organizational Behavior*, vol. 32, no. 3, pp. 499-519, 2011.

[19] K. Krombholz, D. Merkl, and E. Weippl, "Fake identities in social media: a case study on the sustainability of the Facebook business model," *Journal of Service Science Research*, vol. 4, no. 2, pp. 175-212, 2012.

[20] C. Privitera and M. A. Campbell, "Cyberbullying: the new face of workplace bullying?" *CyberPsychology and Behavior*, vol. 12, no. 4, pp. 395-400, 2009.

[21] M. Hutchinson, M. Vickers, D. Jackson, and L. Wilkes, "Workplace bullying in nursing: towards a more critical organisational perspective," *Nursing Inquiry*, vol. 13, no. 2, pp. 118-126, 2006.

[22] R. M. Kowalski, G. W. Giumetti, A. N. Schroeder, and H. H. Reese, "Cyber bullying among college students: evidence from multiple domains of college life," in *Misbehavior Online in Higher Education*. Bingley: Emerald Publishing Group, 2012, pp. 293-321.

[23] X. Zhang, C. Li, and W. Zheng, "Intrusion prevention system design," in *Proceedings of the 4th International Conference on Computer and Information Technology*, Wuhan, China, 2004, pp. 386-390.

[24] S. Zhang and D. Leidner, "Workplace cyberbullying: the antecedents and consequences," in *Proceedings of 20th Americas Conference on Information Systems*, Savannah, GA, 2014.

[25] D. E. Denning, "An intrusion-detection model," *IEEE Transactions on Software Engineering*, vol. SE-13, no. 2, pp. 222-232, 1987.

[26] J. S. Sherif and T. G. Dearmond, "Intrusion detection: systems and models," in *Proceedings of 11th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises*, Pittsburgh, PA, 2002, pp. 115-133.

[27] M. Ptaszynski, P. Dybala, T. Matsuba, F. Masui, R. Rzepka, and K. Araki, "Machine learning and affect analysis against cyber-bullying," in *Proceedings of the Linguistic and Cognitive Approaches to Dialog Agents Symposium*, Leicester, UK, 2010, pp. 7-16.

[28] P. Norberg, "I don't care that people don't like what I do: business codes viewed as invisible or visible restrictions," *Journal of Business Ethics*, vol. 86, no. 2, pp. 211-225, 2009.

[29] Q. Cao, M. Sirivianos, X. Yang, and T. Pregueiro, "Aiding the detection of fake accounts in large scale social online services," in *Proceedings of the 9th USENIX conference on Networked Systems Design and Implementation*, San Jose, CA, 2012.

[30] G. Kontaxis, J. Polakis, S. Ioannidis, and E. P. Markatos, "Detecting social network profile cloning," in *Proceedings of 2011 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*, Seattle, WA, 2011, pp. 295-300.

[31] Y. S. Kim, B. L. Leventhal, Y. J. Koh, A. Hubbard, and W. T. Boyce, "School bullying and youth violence: causes or consequences of psychopathologic behavior?" *Archives of General Psychiatry*, vol. 63, no. 9, pp. 1035-1041, 2006.

[32] S. F. Page, "Innovative schools in Michigan," 2015 [Online]. Available: http://files.eric.ed.gov/fulltext/ED558046.pdf.

[33] S. Einarsen, "The nature and causes of bullying at work," *International Journal of Manpower*, vol. 20, no. 1, pp. 16-27, 1999.

[34] R. N. Bolton, A. Parasuraman, A. Hoefnagels, N. Migchels, S. Kabadayi, T. Gruber, Y. K. Loureiro, and D. Solnet, "Understanding Generation Y and their use of social media: a review and research agenda," *Journal of Service Management*, vol. 24, no. 3, pp. 245-267, 2013.

[35] European Network and Information Security Agency, "Cyber-bullying and online grooming: helping to protect against the risks," 2011 [Online]. Available: https://www.enisa.europa.eu/publications/Cyber-Bullying%20and%20Online%20Grooming.

[36] R. Dredge, J. Gleeson, and X. P. Garcia, "Cyberbullying in social networking sites: an adolescent victim's perspective," *Computers in Human Behavior*, vol. 36, pp. 13-20, 2014.

[37] S. Park, E. Y. Na, and E. M. Kim, "The relationship between online activities, netiquette and cyberbullying," *Children and Youth Services Review*, vol. 42, pp. 74-81, 2014.

[38] A. Anandarajah, "Cyber bully" 2004 [Online]. Available: http://www.cybersecurity.my/en/knowledge_bank/news/2004/main/detail/904/index.html.

[39] Malaysian Communications and Multimedia Commission, "MCMC's 2011 Annual Report," 2012 [Online]. Available: https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/SKMM_11eng.pdf.

[40] C. Shih, "The new social norms," in *The Facebook Era: Tapping Online Social Networks to Market, Sell, and Innovate*, 2nd ed. Boston, MA: Pearson Education, 2011, pp. 31-44.

[41] BrainPOP "Digital etiquette game," 2012 [Online]. Available: http://www.brainpop.com/technology/computersandinternet/digitaletiquette.

[42] Carnegie Cyber Academy, "Betty's netiquette quiz," 2012 [Online]. Available: http://www.carnegiecyberacademy.com/funStuff/netiquette/netiquette.html.

[43] C. Chou and H. Peng, "Promoting awareness of Internet safety in Taiwan in-service teacher education: a ten-year experience," *The Internet and Higher Education*, vol. 14, no. 1, pp. 44-53, 2011.

[44] L. Abeysekera and P. Dawson, "Motivation and cognitive load in the flipped classroom: definition, rationale and a call for research," *Higher Education Research & Development*, vol. 34, no. 1, pp. 1-14, 2015.

Manmeet Mahinderjit Singh http://orcid.org/0000-0001-8081-5223

She is currently serving as an Information Security lecturer in the School of Computer Sciences, Universiti Sains Malaysia. She received Ph.D. degree in Data Security from The Universiti of Queensland, Australia in 2012. She received M.Sc. in Computer Science (Distributed Security) and B.CompSc (Hons) in Computer Science (major program) from the University Sains Malaysia in 2001 and 2006, respectively. Her research interests include trusted models & systems (messaging, social media, location aware systems); sensors network security (wearable technology, RFID/NFC, ambient intelligence systems, mobile crowdsensing); data mining security (intrusion detection techniques, alert management, cost-sensitive systems) and CyberCrime (BYOD, advanced persistent threat attack-security policies models & analytical tools).

Ping Jie Ng

He received B.Sc. degree in School of Computer Science, majoring in Distributed Systems and Security from University Sains Malaysia, Penang in 2014. His current interests in the field of security has been a major factor in designing research in the topic of cyberbullying.

Kar Ming Yap

He received B.Sc. degree in School of Computer Science, majoring in Distributed Systems and Security from University Sains Malaysia, Penang in 2014. His current interests in the field of security has been a major factor in designing research in the topic of cyberbullying.

Mohd Heikal Husin http://orcid.org/0000-0002-3667-3894

He is an Information System lecturer in the School of Computer Sciences at the Universiti Sains Malaysia in Pulau Pinang, Malaysia. He has published in local conferences as well as international conferences on the topic of social media usage and effective policy development within organizations as well as effective technology adoption approaches. He holds a Bachelor of Multimedia Computing from INTI International University (formerly known as INTI College Malaysia), a Master in e-Commerce and a Ph.D. in IT from the School of Computer and Information Science at the University of South Australia. His current research interests includes Government 2.0, Enterprise 2.0, social networking and ICT education.

Nurul Hashimah Ahamad Hassain Malim

She received her B.Sc. (Hons) in computer science and M.Sc. in computer science from Universiti Sains Malaysia, Malaysia. She completed her Ph.D. in 2011 from The University of Sheffield, United Kingdom. Her current research interests include high-performance computing, chemoinformatics, bioinformatics, data analytics and sentiment analysis. She is currently a senior lecturer in the School of Computer Sciences, Universiti Sains Malaysia, Malaysia.