Journal of Positive School Psychology
2022, Vol. 6, No. 3, 8482–8492

Enhancement Keylogger Application for Parental Control and Monitor Children's Activities

Mohamad Yusof Darus[1]; Muhammad Azizi Mohd Ariffin[2]

[1,2]Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA, 40450 Shah Alam, Selangor, Malaysia
Email: [1]yusof@fskm.uitm.edu.my, [2]mazizi@fskm.uitm.edu.my

Abstract

The Nowadays, keylogger has been used widely for malicious purposes, such as stealing passwords and credit card details. A keylogger also has benefits when used legally in terms of ethical purposes where parents can use a keylogger to monitor their children's activity on the Internet. However, the existing keylogger is overlooked because it lacks a screenshot function, webcam capture function, and persistence function. Besides that, the keyloggers mostly log all keystrokes typed on the target computer even though it is not an inappropriate word. Therefore, it is not convenient for parents to monitor everything typed by the children even though it is not an inappropriate word. Since online classes have been implemented in most schools because of the Covid-19 pandemic. Therefore, this project proposed an enhancement of a software-based keylogger with a screenshot function, webcam capture function, and persistence function for parents to monitor the children's online activities daily on the Internet. It is also logging only the inappropriate word typed on the target computer in a text file. This project methodology consists of 3 stages which are design, development, and testing stages. Based on the functionality test result, parents had received three attachments on the email when the software detected the inappropriate word typed on the target computer. The three attachments consist of a text file, a screenshot image, and a webcam capture image. Besides, the text file consists of the inappropriate word that has been detected by the software while the screenshot image displays the children's computer screen display in the form of .jpg format and the webcam capture image that displays the children's behaviors in a .png format. It can also keep the software executed in a hidden mode by enabling the persistence function even after the operating system is rebooting. To verify the effectiveness of the proposed software, this project gets feedbacks from 30 parents and based on the feedback it shows that this software is user-friendly and helps parent in monitoring their children's online activities. In conclusion, this software can help parents take a much better approach to today's monitoring needs, especially during this pandemic, where parents are busy working from home.

Key-words: Keylogger, Parental Control, Children Activities, Internet, Persistence Function.

I. INTRODUCTION

In this era of advanced technology, a variety of techniques have been developed by hackers to steal sensitive information from endpoint computers such as keyloggers. A keylogger is a tool that can automatically capture the keys typed on the keyboard. Captured records may include information regarding the document, passwords, user IDs, and other useful data (Shinde & Wanaskar, 2016). Therefore, an attacker may access confidential data in a protected database without a need to physically break into the house by using this approach (Creutzburg, 2017).

There are two types of keyloggers which are software and hardware keyloggers. Both of these keyloggers may have differences in how it applies, but it has the same functionalities, which is stored the captured data in a log file (Ahmed et al., 2014). Keylogger hardware is

similar to a USB flash drive that has to be inserted directly into the targeted device using the USB port to record the keystrokes, and the logging process started once the device boots. With the software-based keylogger, a user does not need to access the device after installation physically. Since it mainly has a log delivery feature, the software can automatically send logs to a specific destination, such as an email (Shinde & Wanaskar, 2016). The software keylogger intercepts data that travels between the keyboard and the operating system. It records the keystroke, stores them in a remote location, and then transmits them to the attacker (Ahmed et al., 2014).

The keyloggers can also be used legally such as parents can use this tool to record the children's online activities on a computer and monitor the children's social media conversation. Thus, parents able to take early action if the children are ever experienced with cyberbully (Ahmed et al., 2014). Furthermore, the cyber world can be dangerous to children, and parents should give extra attention to the children when using the internet.

With the current pandemic of covid-19 that has been affected globally, internet usage has become vital for both parents and children. Mostly, parents are work from home, everything has to be done from home (Fontanesi et al., 2020). Besides that, online learning has been implemented for the children to learn even from home and millennial main medium of learning is via Internet (Md Sabri et al., 2014). Therefore, parents have minimal time to monitor the children's online activities, especially when the children using a computer for online classes. Thus, parents able to use these tools to take a better approach to monitor the children's online activities on the internet.

Although most of the keylogger software has the function of logging keystrokes typed, thus it is not convenient since it logs all keystrokes even if the children did not type an inappropriate word. The lack of a screenshot function is also one of the limitations of most of the keylogger software since it is difficult for parents to monitor the website visited by the children without a screenshot function available. For example, the website URL visited by the children may not look suspicious, but it can contain an explicit picture or advertisement that is not supposed to be discovered by the children (Keijsers, 2016).

Besides, since an online class has been implemented in most schools because of the covid-19 pandemic, the children can do other things such as listening to music, watch inappropriate videos on YouTube, and not entirely focus on the online class. Therefore, without the webcam capture function available, parents can never realize what the children are doing when having online classes (Zaman & Nouwen, 2016). Moreover, as a muslim most parents must ensure that their children is accessing the appropriate we content (Ibrahim et al., 2009).

This paper aims to develop the keylogger by adding screenshot function, webcam capture function and persistence function. The proposed software will notify parents via the Telegram application that an inappropriate word is detected typed and the parent will receive an email.

II. LITERATURE REVIEW

Some related works and terminologies are presented here to appreciate the importance of integrating several features in the proposed keylogger.

A. Software Keylogger

The keyloggers are often used for debugging technical computer and business network problems. It has very appropriate uses in studying the interaction between the human and computer (Bayzid et al., 2019). Unlike content-filering software such as (Bin Mohamad Razali et al., 2019), keylogger is not design to filter or block content but rather continuously record needed data as logs. The software keylogger can records keystroke data as it travels through the keyboard interface and the operating system. Many types of software-based keyloggers can be classified, which are kernel-based keylogger, hypervisor-based keylogger, API-based keylogger, form grabbing-based

keylogger, and JavaScript-based keylogger as shown in Table 1.

Table 1 –Software-Based Keylogger Description

Keylogger Software	Functionality
Kernel-based	The malicious software system must operate either in kernel or user space. It takes much experience to build a key logger based on the kernel. The approach is both challenging to write and difficult to fight. Those keyloggers exist at the kernel level, making it difficult to identify them, particularly for user-mode programs that do not have root access—rootkit which intercepts the press key or keystrokes that pass through the kernel of the operating system.
Hypervisor-based	Keylogger residing or infecting the hypervisor to record all keystrokes sent to every virtual machine. Blue Pill is one such potential malware, which would be undetectable even though the malware algorithm is known to the public
API-based	A keylogger hooks keyboard APIs within an executed program to obtain events if the user presses a key to allow the keylogger to monitor it (Li et al., 2018). Windows APIs such as GetAsyncKeyState() and GetForegroundWindow(). These features are used to get keyboard events, mouse events, and current window names
Form grabbing based	A keylogger that captures data from web form until it is sent to the webserver. If the user clicks on the send button it will capture all the details on the web page (Sbai et al., 2018). This sort of keylogger stores data of the form until it is transmitted over the Internet.
JavaScript-based	To listen for and monitor keyboard events, a malicious JavaScript keylogger will be inserted into a specified website such as onKEyUp(). Stealing of credit card through web-based keylogger. Scripts could be inserted through various methods, including cross-site scripting, man-in-the-browser, man-in-the-middle, or remote website compromise.

B. Hardware Keylogger

Hardware keyloggers are computer parts that are installed between the keyboard and the Input/Output (I/O) port. All keystrokes are collected and either stored on the internal memory or transmitted via WIFI. Unfortunately, these devices can usually be seen through a computer's casual inspection and can be viewed every time a user uses a public computer (Echallier et al., 2017). There are three types of hardware-based keyloggers are Firmware-based, keyboard hardware, and video surveillance as shown in Table 2.

Table 2 –Hardware-Based Keylogger Description

Keylogger Software	Functionality
Firmware-based	On the BIOS level, these hardware-specific keyloggers log keystrokes. The computer must have physical or root-level access, as well as the software loaded into the BIOS must be generated for the specific hardware it will run on.
Keyboard hardware	Built between the keyboard itself and the target device. These devices are usually attached straight to the computer's connection and can only be seen if the user looks closely. They can be challenging to detect if the computer connections are not visible at the workstation. For example, keyloggers based on Universal Serial Bus (USB) will only be inserted into a USB port to accomplish the mission. Another example is by using the PC webcam to

	capture the users physical activities.
Video Surveillance	Video surveillance, which can be used to record passwords or PINs, could also be used in keyloggers. For example, a hidden surveillance camera on an ATM will allow an attacker to see a PIN or password entered.

C. Features of Keylogger

(Nadar et al., 2017) developed a keylogger software that provides features of capturing the computer screen monitor when the target user uses a mouse or joystick rather than a keyboard that can be saved in a log file. The log file can be viewed only by the owner of the keylogger. The proposed keylogger software also helps the user know all the sites accessed by the target user without their awareness. However, this keylogger only focusing on the mouse rather than the keyboard inputs.

Some of the reseachers developed the keylogger software with a feature where log file protection is invented by encrypting the log files (Li et al., 2018). Mostly, all log files in the keylogger are not encrypted and can be instantly exploited for malicious use. The system is helpful for ethical purposes in monitoring the activities of the target user without being detected on the internet. The author also introduces various prototypes, such as clipboard logging, screen capture, and keystroke logging features. This proposed keylogger is not suitable for monitor children's activities because parents need to decrypted the log files before reading the log files.

Another keylogger software is based on a user-space since implementing the user-space is much easier, and no special permission is required to execute the software (Sivarajeshwaran S & Ramya G, 2015). The keylogger software has other features, such as the software is running on a stealth mode without the knowledge of the target user. Other than that, the log file contains all the keystrokes typed by the target user, and a screen capture of the computer screen monitor can be sent through email, or it can be saved in a specific folder in a particular time interval set by the owner of the keylogger.

(Bhosale et al., 2016) was proposed the keylogger application that runs on Android smartphones. This software's main features are it will capture all the keystrokes typed by the target user on the mobile phone keyboard and automatically save the data in the log file of the mobile phones. The log file is then sent to the desired destination when the target user's mobile phones are connected to the Internet. The keylogger apps are also running in stealth mode, and it is not listed in the task manager. Besides that, another keylogger will trigger the user's mobile phone by sending push notifications whenever the webserver has a new log file (Witno & Rino, 2018). This keylogger using Cloud to Device Messaging (C2DM) is a server and cloud computing application. Nevertheless, this proposed keylogger focused to monitor employers' activities only and suitable for a business environment.

Most of the existing keyloggers lack a persistence function to let the software run again automatically if the computer is rebooting. Furthermore, does not provide a screenshot function of the target computer.

III. METHODOLOGY

A. Design Phase

The software design consists of a flowchart and logical design as shown in Figure 1 and 2.

Figure 1 –Flowchart for the user

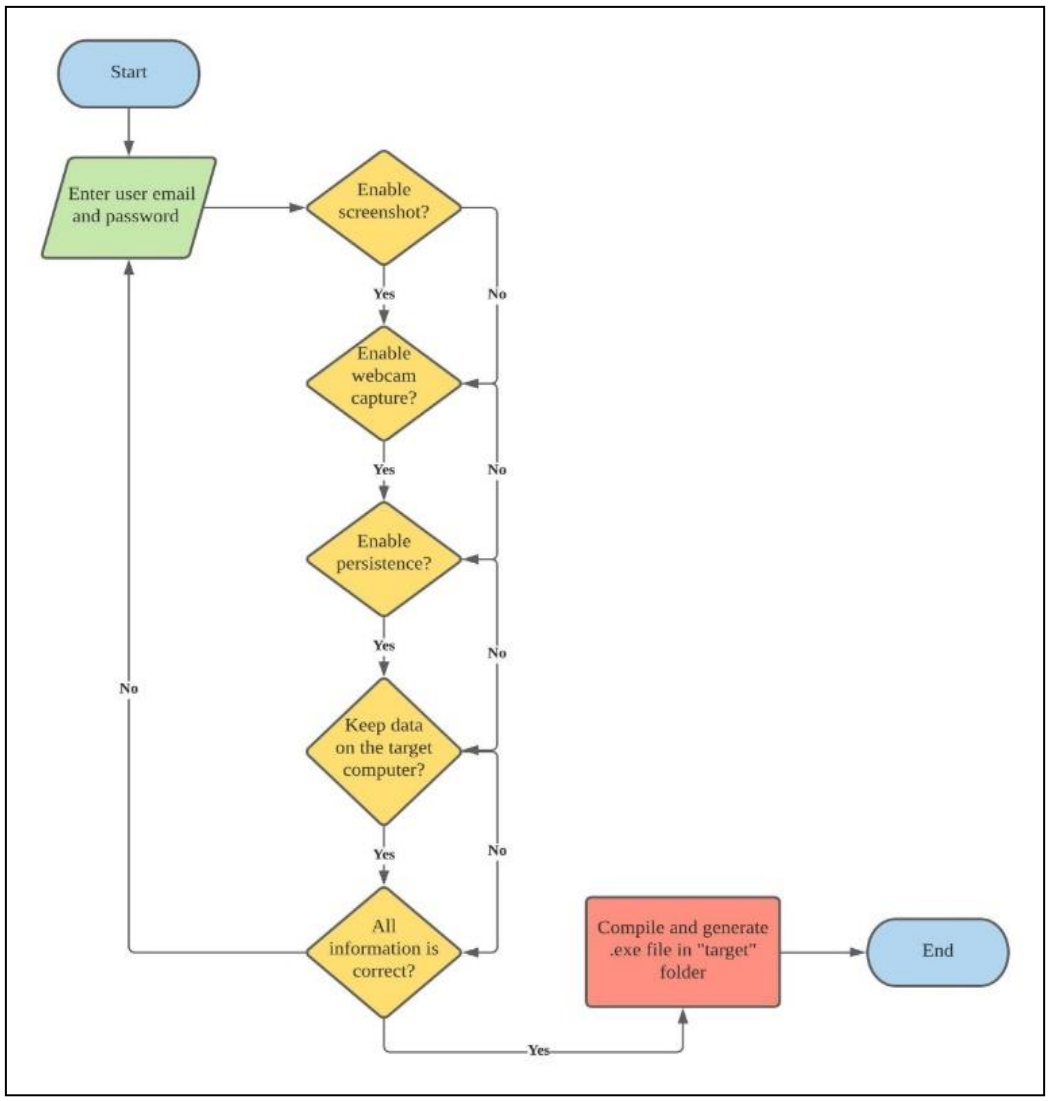


Figure 1 indicated that the user requires to enter an email and password. The user then needs to enable the four features, which is the screenshot function, webcam capture function, persistence function, and keep data on the target computer function to fully utilize the software. Next, if all of the user's information is correct, it compiled all of the information that the user has been entered and generated an execution file into a folder named "target". Lastly, the execution file is the one that the user needs to transfer and execute in the target computer.

Figure 2 – Logical design for the keylogger software

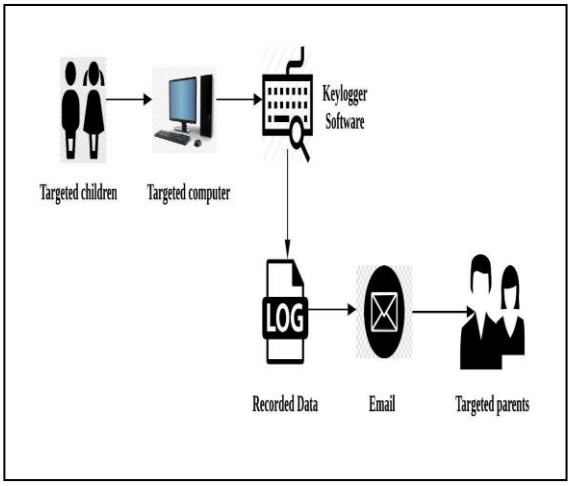


Figure 2 indicates that the keylogger software has been executed inside the target computer and running in a hidden mode. It also records

the inappropriate word typed on the target computer and sends it to the users' email along with other recorded data.

B. Development

The development phase begins to develop the keylogger software using the Sublime Text application. In this project, we developed the keylogger software in the Virtual Box. The Java language is used to write the code where it records the inappropriate word typed on the keyboard. It can also capture the current computer screen monitor and the webcam capture of the target computer and send it via email to the user and notify the user using a Telegram application. Figure 3 shows the example of the code for keystroke logging.

Figure 3 –Sample code for keystrokes logging

```
import java.text.DateFormat;
import java.text.SimpleDateFormat;
import java.util.Date;
import java.util.logging.Level;
import org.jnativehook.GlobalScreen;
import org.jnativehook.NativeHookException;
import org.jnativehook.keyboard.NativeKeyEvent;
import org.jnativehook.keyboard.NativeKeyListener;

public class Keylogger extends javax.swing.JFrame implements NativeKeyListener {

    private static DateFormat dateFormat = new SimpleDateFormat("yyyy-MM-dd");
    private static DateFormat dateFormatHour = new SimpleDateFormat("yyyy-MM-dd HH-mm-ss");
    private static String folder = "\\log(K)ey";
    private static String environment_variable_path = "APPDATA";
```

While the Figure 4 shows the example code for the screenshot function in the keylogger.

Figure 4 – Sample code for screenshot function

```
import java.awt.Toolkit;
import java.awt.image.BufferedImage;
import java.io.File;
import java.io.IOException;
import javax.imageio.ImageIO;

public class Screenshot {

    public static void TakeScreenshot(String filePath, String fileName) {
        try {
            Robot robot = new Robot();
            Rectangle screenRect = new Rectangle(Toolkit.getDefaultToolkit().getScreenSize());
            BufferedImage screenFullImage = robot.createScreenCapture(screenRect);
```

C. Functional Testing

For this project, the software's functionality is tested in the real environment, which is the windows 10 operating system. Figure 5 shows that the email received by the user with three attachments includes a text file, a screenshot image of the screen monitor, and a webcam capture image.

Figure 5 – Email received by the user

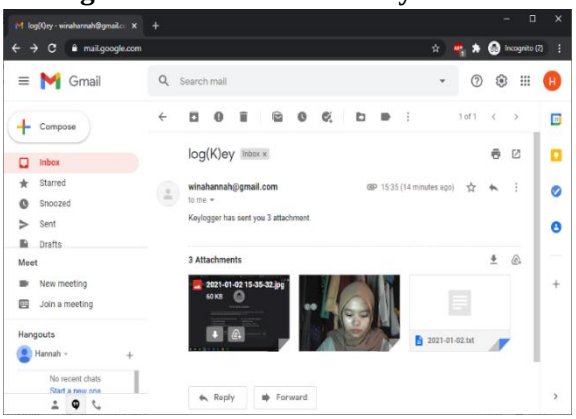


Figure 6 indicates the notification alert on the Telegram application received by the user. It states that the inappropriate word has been typed on the target computer and that the keylogger has detected it. It also informs the user to check the email as soon as possible to view the inappropriate word that has been detected, along with other enabled features such as screenshots image and webcam capture image.

Figure 6 – Notification received by the user on Telegram.

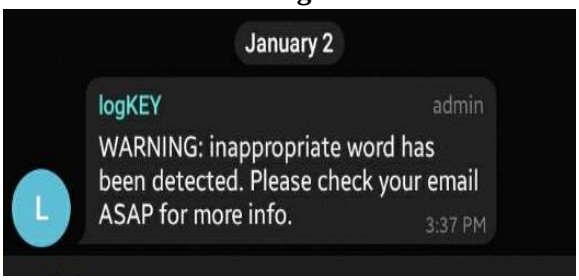


Figure 7 shows the recorded text file of the inappropriate word typed on the target computer, such as games, vapes, and drugs. This text file also indicates that the children have typed "games" two times on the Internet. The name of the text file indicates the date of the email sent to the user.

Figure 7 – A text file received by the user

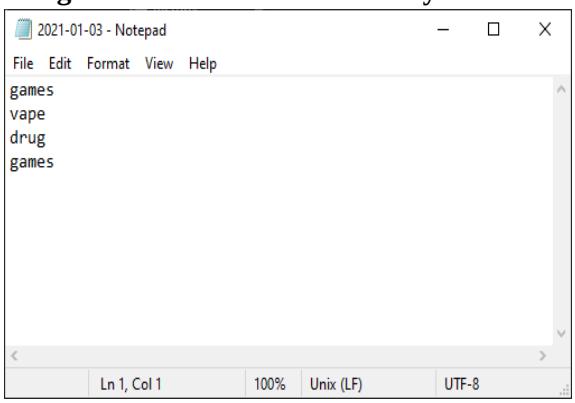


Figure 8 shows the screenshot image of the target computer display in .jpg format. The screenshot function provides the parents with a picture of the children's activities on the Internet when using the computer. It also shows capture the full ratio of the computer display. The screenshot picture's name indicates the date of the screenshot taken along with the time, which is on January 2nd in 2021, around 03:25 p.m.

Figure 8 – Screenshot image of the screen display

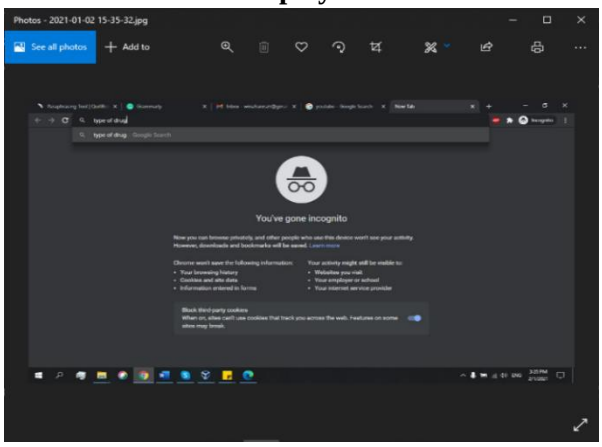


Figure 9 shows that the keyloggers software can detect the inappropriate word typed on a target. It is a screenshot image of the target computer screen display that reveals it has typed "how to buy cigarette," and the keyword that keyloggers recorded in the text file are " cigarette ". The screenshot picture's name indicates the date of the screenshot taken along with the time, which is on January 5th in 2021, around 02:35 p.m.

Figure9 – Screenshot image on Microsoft Edge browser

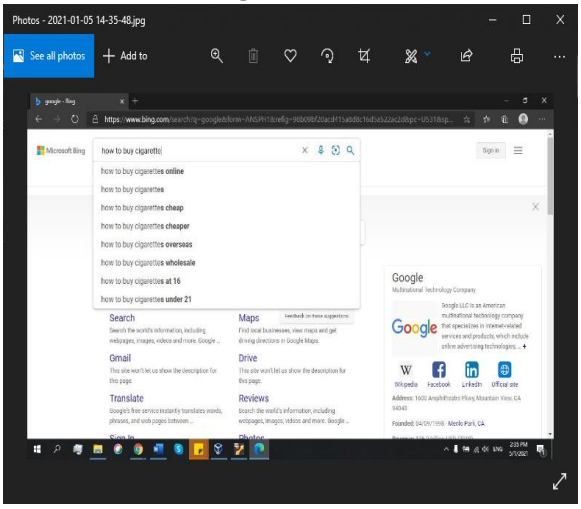
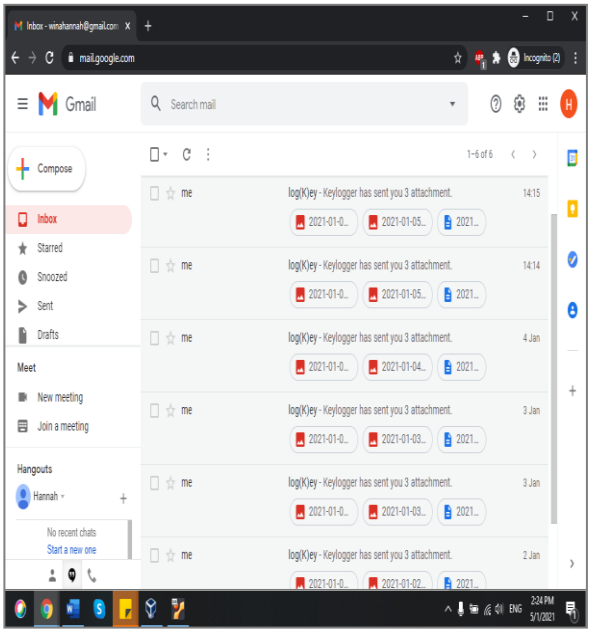


Figure 10 shows the email received by the parents on different dates, which is on January 2nd, January 3rd, January 4th, and January 5th of 2021. It also shows that the persistence function lets parents monitored the children's activity on the Internet daily without the need to execute the software every day on the target computer.

Figure 10 –Persistence of the keylogger software



IV. RESULT AND DISCUSSION

In this section, the analysis based on the question of the effectiveness of the proposed software. In this study, we recommended collecting 30 questionnaires from parents.

Figure 11 shows the result of a survey in which respondents were asked about their satisfaction with the software's reliability when using the software. From the pie chart, all of the respondents are satisfied with the software's reliability. Software reliability is defined as software that can fulfill its assigned role for the specified number of input cases in each context, considering that the hardware and the input are error-free.

Figure 11 –The reliability of the software

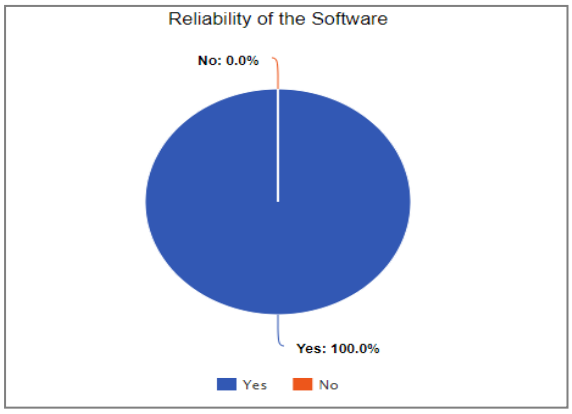


Figure 12 shows the result of a survey in which respondents were asked about their satisfaction with the software's effectiveness. From the pie chart, all the respondents are satisfied with the software's effectiveness when using the software.

Figure 12 –The effectiveness of the software

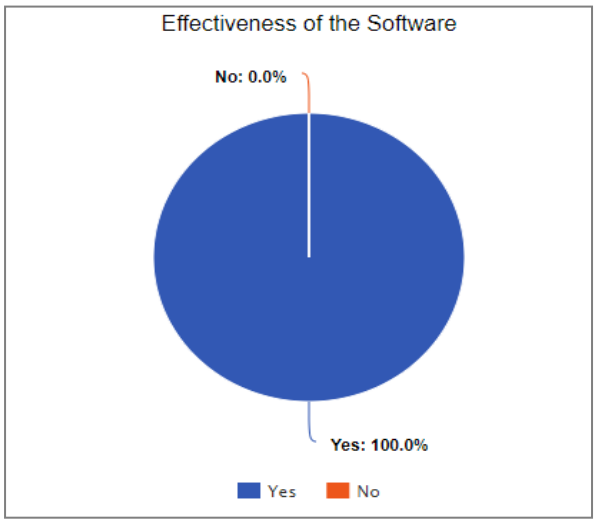


Figure 13 shows the result of a survey in which respondents were asked about their satisfaction with the software's ease of use. From the pie chart, all the respondents are satisfied with the software's ease of use. Ease of use is a crucial concept explaining how the target users can use the software easily.

Figure 13 –The ease of use of the software

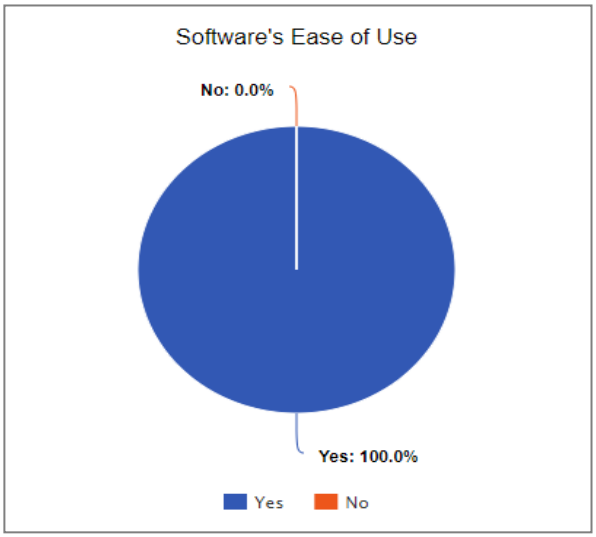


Figure 14 shows the result of a survey in which respondents were asked if they encounter any difficulties when using the software. The pie chart shows that 80 percent of the respondents do not face any problems while using the software, while 20 percent did encounter some problems when using the software.

Figure 14 – The difficulties found when using the software

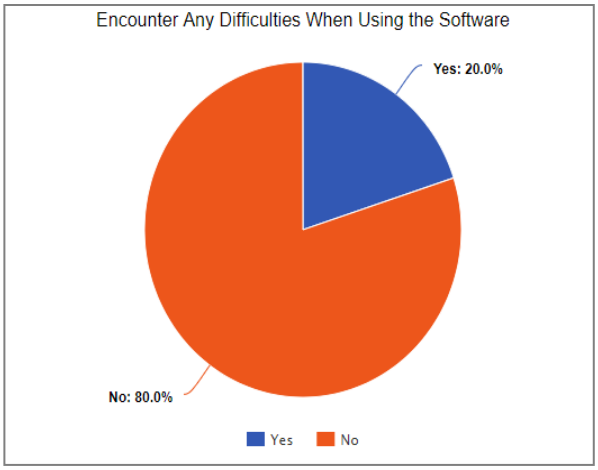


Figure 15 shows the result of a survey in which respondents were asked if the software interface is user-friendly or not. Therefore, the pie chart shows that 90 percent of the respondents choose a yes option where the software has a user-friendly interface, while 10 percent of the respondents said that the software does not have a user-friendly interface.

Figure 15 – User-friendly Interface

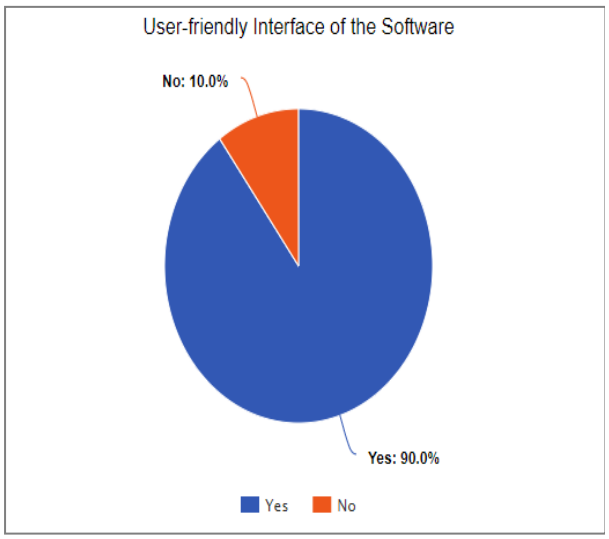


Figure 16 shows a survey in which respondents were asked if the software has helped parents monitor the children's online activities or not. Therefore, from the pie chart, all of the respondents are agreed that the software can help parents monitoring their children's activities when browsing the internet.

Figure 16 – The software helped parents monitor the children's online activities

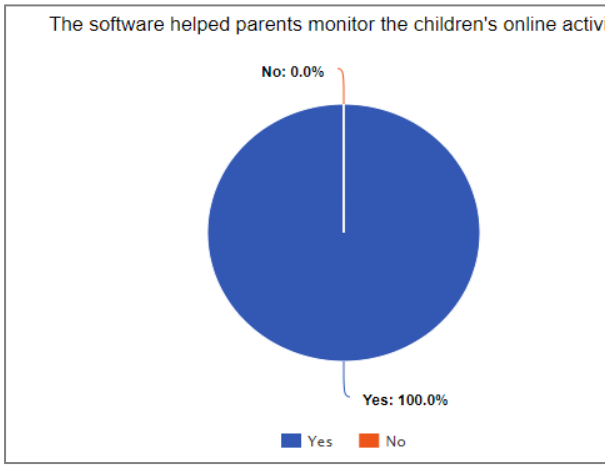
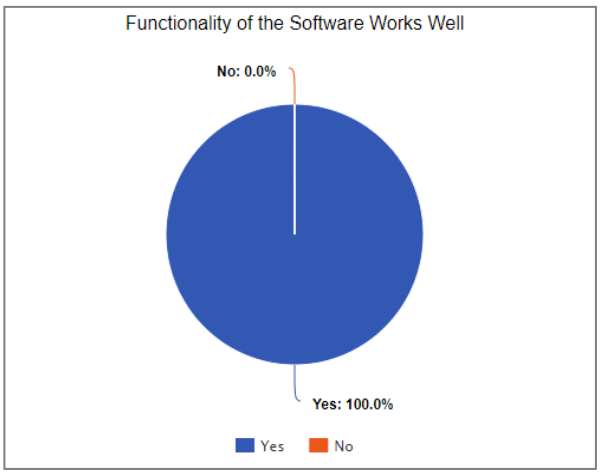


Figure 17 shows a survey in which respondents were asked if the software's functionality, which is the screenshot function, webcam capture function, and persistence function is working correctly or not. Therefore, from the pie chart, all of the respondents have tested the software's functionality and said that the software's functionality is working well.

Figure 17 – Functionality of the software



V. CONCLUSION

The parents will run this keylogger software to monitor the children's activities on the Internet. It is helpful in the current covid-19 pandemic, where most of the parents are working from home. Since parents are working remotely, it is difficult for the parents to monitor the children's activities while doing their works. Our proposed software has various features such as keystroke logging, screenshot function, and webcam capture function. More convenient features for parents are also offered by this software, which is the persistence and keep data on the target computer functions. Persistence is considered an excellent feature for the software, especially when the computer is rebooted because it does not require the parents to run the software every day on the children's computer.

The software can also be executed and run in a hidden mode without the children's awareness. Besides, by enabling the keep data on the target computer function, the recorded data is also stored in a specific folder at the children's computer. Therefore, parents able to view the recorded data again if the parents accidentally deleted the email given by the software since the email account now has a feature that can delete all emails received in a given amount of time set by the user.

Finally, this proposed software can detect inappropriate words typed in almost all browsers such as Google Chrome, Firefox, Microsoft Edge, and Internet Explorer as long

as the internet connection is working on the target computer. The software also has a feature that lets parents know when the email has been received by notifying them using a Telegram application. Therefore, parents do not have to check the email every time to see whether the keylogger has sent an email or not.

VI. ACKNOWLEDGEMENT

The authors would like to thank Universiti Teknologi MARA (UiTM) for providing Lestari SDG-Triangle Grant (600-RMC/LESTARI SDG-T 5/3 (142/2019)) to fund this research.

BIBLIOGRAPHY

1. AHMED, Y. A., MAAROF, M. A., HASSAN, F. M., & ABSHIR, M. M. (2014). Survey of Keylogger Technologies. International Journal of Computer Science and Telecommunications Journal Homepage: Www.Ijcst.Org, 5(25), 1–7. http://www.ijcst.org/Volume5/Issue2/p5_5_2.pdf
2. BAYZID, M., SHOIKOT, M., HOSSAIN, J., & RAHMAN, A. (2019). Keylogger Detection using Memory Forensic and Network Monitoring. International Journal of Computer Applications, 177(11), 17–21. https://doi.org/10.5120/ijca2019919483
3. BHOSALE, P., SAURABH HANCHATE, AJAY DASARWAR, & MOHAK INDURKAR. (2016). Keylogg - a Touch Based Key Logging Application. International Journal of Research in Engineering and Technology, 05(04), 12–15. https://doi.org/10.15623/ijret.2016.0504003
4. BIN MOHAMAD RAZALI, M. R., AHMAD, S., & DIAH, N. M. (2019). Collaborative filtering content for parental control in mobile application chatting. Bulletin of Electrical Engineering and Informatics, 8(4), 1517–1524. https://doi.org/10.11591/eei.v8i4.1634
5. CREUTZBURG, R. (2017). The strange world of keyloggers - an overview, Part I. Electronic Imaging, 2017(6), 139–148. https://doi.org/10.2352/issn.2470-1173.2017.6.mobmu-313
6. ECHALLIER, N., GRIMAUD, G., IGUCHI-CARTIGNY, J., PLACE, J., & JEAN-PHILLIPE, W. (2017). Virtual keyboard logging counter-measures using common fate's law. Csce.Ucmss.Com, 188–194. https://csce.ucmss.com/cr/books/2017/LFS/CSREA2017/SAM9731.pdf
7. FONTANESI, L., MARCHETTI, D., MAZZA, C., DI GIANDOMENICO, S. D., ROMA, P., & VERROCCHIO, M. C. (2020). The Effect of the COVID-19 Lockdown on Parents: A Call to Adopt Urgent Measures. Psychological Trauma: Theory, Research, Practice, and Policy. https://doi.org/10.1037/tra0000672
8. IBRAHIM, E. N. M., NOOR, N. L. M., & MEHAD, S. (2009). Trust or distrust in the web-mediated information environment (W-MIE) A perspective of online muslim users. Journal of Enterprise Information Management, 22(5), 523–547. https://doi.org/10.1108/17410390910993527
9. KEIJSERS, L. (2016). Parental monitoring and adolescent problem behaviors: How much do we really know? International Journal of Behavioral Development, 40(3), 271–281. https://doi.org/10.1177/0165025415592515
10. LI, L. S., FAUZEE, Z. M., ZAMIN, N., KAMARUDIN, N., SABRI, N. A., & AZIZ, N. S. N. A. (2018). An encrypted log file Keylogger system

for parental control. International Journal of Engineering and Technology(UAE), 7(2), 193–196. https://doi.org/10.14419/ijet.v7i2.28.12910

11. MD SABRI, S., HARON, H., JAMIL, N., & MIOR IBRAHIM, E. N. (2014). A Conceptual Review on Technological Intergenerational Knowledge Transfer. Journal of Computers, 9(3). https://doi.org/10.4304/jcp.9.3.654-667
12. NADAR, S., PATEL, T., GURAV, P., & RAUT, C. (2017). Xploiter-Keystroke Analyser. International Journal Of Engineering Sciences & Research Technology, 6(3), 305–308.
13. SBAI, H., GOLDSMITH, M., MEFTALI, S., & HAPPA, J. (2018). A survey of keylogger and screenlogger attacks in the banking sector and countermeasures to them. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 11161 LNCS, 18–32. https://doi.org/10.1007/978-3-030-01689-0_2
14. SHINDE, S., & WANASKAR, U. H. (2016). Keylogging : A Malicious Attack. International Journal of Advanced Research in Computer and Communication Engineering, 5(6), 285–289. https://doi.org/10.17148/IJARCCE.2016.5661
15. SIVARAJESHWARAN S, & RAMYA G. (2015). Developing Software Based Key logger and a Method to Protect from Unknown Key loggers. International Journal of Innovative Science and Modern Engineering (IJISME), 7, 2319–6386. http://www.xatrix.org/article2641.html
16. WITNO, S., & RINO, R. (2018). Monitoring Computer Activities with Cloud to Device Messaging (C2DM). Tech-E, 1(2), 35. https://doi.org/10.31253/te.v1i2.42
17. ZAMAN, B., & NOUWEN, M. (2016). Parental controls : advice for parents , researchers and industry. Eukidsonline, February, 1–9. https://www.researchgate.net/publication/301775592_Parental_controls_advice_for_parents_researchers_and_industry