Parental Control System for Children on Wireless Network

Wan Hazimah binti Wan Ismail
Malaysian Institute of Information Technology
Universiti Kuala Lumpur, Malaysia
wanhazimah@unikl.edu.my

Herny Ramadhani Mohd Husny
Malaysian Institute of Information Technology
Universiti Kuala Lumpur, Malaysia
herny@unikl.edu.my

Ahmad Syahman bin Mamat
Malaysian Institute of Information Technology
Universiti Kuala Lumpur, Malaysia
syahman922@gmail.com

Norhaiza Ya Abdullah
Malaysian Institute of Information Technology
Universiti Kuala Lumpur, Malaysia
norhaizaya@unikl.edu.my

***Abstract*— Today's teenagers, and school age children are getting more and more technologically sophisticated, very often outpacing what their parents know about these high-tech gadgets. While for some kids that actually means that they are learning computer languages, creating websites, and even building robots, most others are simply using today's technology to watch videos on YouTube and play MMORPGs (massively multiplayer online role-playing games) or they are talking on their cell phones and sending text messages. Unfortunately, many of the things kids can do online and with their cell phones can lead to a lot of trouble if they are not monitored. From watching porn and other inappropriate video and websites to sexting (sending inappropriate text messages or photographs) and chatting with predators, new technology can lead to new problems. Cell phones and the internet have even led to new ways for kids to be bullied or cyber bullying. That does not have to mean that kids cannot have a computer or cell phone, but we should learn about parental controls that can help protect them as they use the latest high-tech gadgets. The aim of this project is to develop the parental control system that able to monitor the children's behavior and to block the inappropriate website. This system also has time management to manage the surfing time access the internet.**

Keywords — Parental Control System, Web Filtering

I. INTRODUCTION

Modern life has become easier and the people of the world have to thanks to the immense contribution of the internet technology for communication and information sharing. There is no doubt that the internet has made our life become easier and more convenient. We can use the internet to communicate with people around the world, doing business by using the internet, make new friend and know different cultures, searching information, studying and others.

The internet also allows people to communicate with each other from any location. With the internet, people no need to go to the other location, it just only can communicate using social media such as Facebook, Twitter, WhatsApp and others. By using this medium, we can save our money from spending too much cost to go the location just only to communicate to the people.

However, the internet also has some disadvantages. For example, some people use the internet to communicate with wrong people such as for drug dealing, gambling, sexual harassment and racism. Furthermore, the use of the internet by wrong people can lead towards bad culture in communicating with each other, such as the use of bad languages which can be seen nowadays most in the games chat. While the internet provides good information to the users, the internet also has a dark side where it is also filled with lots of negative and inappropriate content such as pornography, racism and defamation [1].

Hence, this project aims to overcome the problem by constructing a parental control system using Raspberry Pi and act as a wireless router that allow parents to prevent their children from accessing unsuitable Internet content. It acts as a filter, authorized to surf into harmless pages, but blocking certain sites that may be inappropriate for children. Laptops, smart phones, and tablets connect to the wireless router will be filtered with Raspberry Pi's web filter when children surfed the internet. This system also intercepts blacklisted content websites such as porn, gamble, drugs, and prostitutes if they try to access them. For example, our children try to search explicit word such as 'sex' on a search engine, list of websites will appear on the browser, but they unable to access that website as it is blocked by Raspberry Pi's web filter. Besides that, this system able to limit the access time of internet usage for our children when they surf the internet. Parents also able to set the time when will their children able to access the internet.

II. TYPE OF WEB FILTERING

Filters can be implemented in many different ways by software on a personal computer, via network infrastructure such as proxy servers, DNS servers, or firewalls that provide Internet access. No solution provides complete coverage, so most companies deploy a mix of technologies to achieve the proper content control in line with their policies. For example, businesses often block social networking sites to prevent employees from wasting time. Parents are required to block pornography to protect children online and many organizations

block malicious websites that host exploits and malware [2]. Below are the some of filtering's techniques of the parental control system:

A. Browser-based Filters

Browser-based types of web filters are typically extensions, applications or add-ons that can be installed and used with a particular web browser. While not the most thorough filter, these types of web filters are widely available and are very convenient for users [3].

B. Search Engine Filters

Search engine types of filters sift out unsuitable content from the results a user sees when looking up information through a search engine. Some search engines have this feature built into their user interface. Google and Bing have Safe Search options for those who want to filter out inappropriate content in their search results. Both of these search engines have Safe Search on as a default, but one does not need administrative privileges to turn these filters off [4]. Search engine filters can also be easily circumvented if the user knows the URL of the site they are trying to access or if they use another search engine that does not have a similar filter.

C. Client-side Filters

Client-side filters are filtering programs installed on the device an employee or student uses. Such filtering programs typically have to be installed and configured on each individual device, making these types of web filters more time consuming to install than others. While these types of web filters may be ideal for a small business, larger businesses may not want to deal with the hassle of setting up this type of web filter on more than a few computers. These types of web filters can also be easily circumvented by those who have administrative privileges since these types of web filters are often directly installed on the device and not controlled by a central program [4].

D. Content-limited ISPs

Content-limited ISPs are internet service providers who block off specified websites from all who subscribe to the ISP's service. Typically found in countries who censor content on the web, these types of web filters are gradually making their way to countries around the world. Virgin Media, for example, is an ISP that used this type of web filtering to block the Pirate Bay from subscriber access. While these types of web filters are not yet widely available, they may be in the future [4].

E. Network-based Filters

The next type of web filtering is called network-based web filtering. Network-based types of web filters are typically implemented in either the transport or application layers of a network. These types of web filters are set up as either a web proxy or a transport proxy to guard the network. They serve as the middleman between outgoing requests and incoming information. They also usually guard the individual IP addresses of all of the workstations on the network by only displaying the IP address of the filter to outside users [5].

III. Existing Parental Control Software

A. Safe Eyes

Safe Eyes is an award winning Internet parental control program that just got better. Safe Eyes Parental Control Software has been released and this software allows parents to further increase their control over computer and internet activity. This parental control program gives the user complete control over what kids do while they are online. Safe Eyes allows a parent to monitor, restrict and block internet activity all in one package. A parental control program for a computer allows parents to totally control and monitor all aspects of computer and internet activity. This is a great program for the youngest of Internet users, as it will block 35 categories of website content, as we deem appropriate. The Safe Eyes Internet parental control program allows user to control the time our kids spend on the internet. We know they spend way too much time online when they could be doing something more productive. We have total control over the time they spend on the internet. The subscription fee for 3 PCs is $49.95 per year [6].

B. KidsWatch

KidsWatch is a comprehensive tool to help safeguard our family from inappropriate content on the Internet. The service features several tools and blockers designed to both track and block content through our computer, as well as manage our kid's time spent online. KidsWatch blocks thousands of websites and key phrases in search results. It has over 60 different categories to choose from when selecting which type of content we want to block access from (e.g. Adult, Porn, Hate Speech and Violence). With KidWatch's time management tool, setting time limits on computer usage is easy and effective.

This tool allows user to set specific blocks of time for when our child is able to access the computer, Internet usage, gaming websites or instant messaging. With the chat session monitor, we will be able to monitor our child's chat or instant messenger conversations with anyone on Facebook, Twitter, Yahoo!, Skype, Tumblr, Instagram and YouTube. If our child is using an instant messenger outside of these, KidsWatch will not monitor the conversations, but we do have the option to entirely block access to that service. KidsWatch has 2 packages which are Time Management plan and Professional plan. The subscription fee for Time Management plan is $29.95 per year and Professional plan is $49.95 per year [7].

C. Net Nanny

Families can use Net Nanny to protect their children from pornography, online predators, cyberbullying, and other threats that compromise online safety. Net Nanny's award-winning technology filters, monitors, and blocks unsafe materials while allowing teenagers' access to the Internet. Unlike other parental controls that simply block a list of web sites, Net Nanny's dynamic filter scans and analyses each web site to determine if it is appropriate for your child, based on your unique customization. It can even mask profanity, but let the site pass, ensuring teenagers are protected while they navigate the Internet. The subscription fee for 1 device is $39.99 per year.

For additional computer or device will be charged $19.99 per year [8].

D. Cyber Patrol

While "parental controls" in a product name typically suggests home use, the comprehensive and flexible CyberPatrol Parental Controls ($39.95 per year direct) is equally suited for schools, libraries, or workplace settings. It even includes configuration themes for those specific environments. CyberPatrol blocks inappropriate Web sites, schedules Internet access, control programs, filters objectionable words from instant messages, and monitors Web-surfing activity [9]. It is good at what it does. About the only significant features it lacks are in the remote notification and management area.

IV. COMPARISON OF PARENTAL CONTROL SOFTWARE

The Internet is always on, but parents cannot always be around to see what their children are looking at. That's why there's need parental control software. Parental control software helps parents, guardians, and other computer administrators monitor and set limits on online activity [10]. There are so many parental control software that is available in the market, but they are not meeting the customer requirement on the criteria or features that the market offers. Below is the summary of some feature of the parental control software:

TABLE I. Comparison of Parental Control Software

Software	Cost	Programs Monitored	Special Features	Reports /Alerts
Safe Eyes	$49.95/yr for 3 PCs	Internet Explorer, Firefox; Instant messenger (Yahoo!,AIM, MSN, ICQ)	Multiple levels of blocking severity; Some ability to block program access	Daily or weekly reports; instant email, text or phone alerts for violations
Kids Watch	$29.95 for Time Management plan OR $49.95 for Professional plan	Windows Internet browsers, Facebook, Myspace, Yahoo and MSN	Time management, instant message monitoring, block sites and programs	Searchable web history email reports, messaging email alerts
Net Nanny	$39.99/yr AND $19.99/yr additional computers/ devices	Internet Explorer, Firefox, Chrome, Safari	Profanity masking; ratings-controlled gaming; picture, forum, blog controls	Searchable web history reports; customizable real time cell phone/email alerts
Cyber Patrol	$39.95/yr for 3 PCs	IE, Firefox	IM-level profanity masking	Web history reports
Kidsafe	One-time payment $50.35. No subscription fee	Support all web browser and IM	User-access level management and time management	Web log history

As we can see, the existing parental control software has a subscription fee per year to subscribe the software and program monitored not support all web browsers but proposed parental control have more advantage which is supporting many web browsers in a software. The proposed parental control also can save our money, which is only one-time payment to setup the software. The majority of parental control software support blocking pornography feature.

V. SYSTEM ARCHITECTURE

The systems architecture process is where the concepts that will be the backbone of the actual system are developed. It is a conceptual model that describes the structure and behavior of the proposed system.

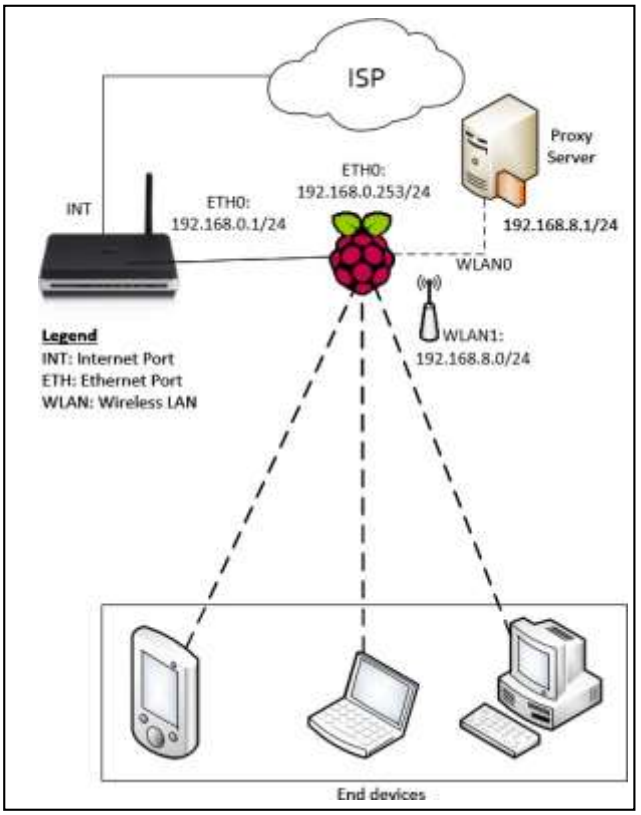

Fig. 1. System Architecture Diagram

Fig. 1 shows the system architecture diagram for Parental Control System. As we can see, there are two types of

connections are shown on the diagram. First, the connection between Raspberry Pi (ETH0) and home router (ETH0) are using physical cable and the other using Wireless connection. The physical cable that is being used is CAT5E cable. For local connection we used Ethernet Port (ETH0) to connect the devices while to connect home router with ISP we used Internet Port (INT).

VI. PROTOTYPE / PRODUCT DEVELOPMENT

The development of this project started with the installation Rasbian OS on Raspberry Pi. This is an earlier process before we write and run the code into Raspberry Pi. After that, we configured the static IP for Raspberry PI acts as a router. Next stage, we also created the wireless access point for a connection user access to the internet. Then, we configured the squid acts as a proxy server. Next, we configured Apache, MySQL, PHP, and phpmyadmin.

A. Login Page

Fig. 2 below shows the login page of the prototype system. For first time login, user needs to ask the administrator for registration an account before they able to access the internet. The detail information must be provided by users such as username, full name and password for ease of use of administrator to create a new account. User unable to access the Internet if they not login into the system.

Fig. 2. Login Page

B. Add User Page

Firstly, user need to get the username and password before they able to surf the internet. So, user request an administrator to create a new account for them. Only administrator able to add and modify user account. Each user can surf the internet within a limited time in a session that is fixed by the administrator. After a session is expired, the user will unable to access the internet and need to request a new session again from the administrator. Fig. 3 shows the add user page of the prototype system.

Fig. 3. Add User Page

C. Log Viewer Page

Fig. 4 shows the log viewer page after administrator success to login. This page shows the user being logged into the system. When user login into the system, some information being displayed such as IP address, user, permission, login from and login expiry.

Fig. 4. Log Viewer Page

D. Add New Rules

Fig. 5 shows the tab to add new rules into the system. The administrator can manage the rules by adding the specific website URL into adding host option and ability to select which group is affected by that rule. The administrator also has an option to set the access time for surfing the internet.

Fig. 5. Add New Rule Page

E. Add Blacklist Website

Blacklisting the website is one of the main functions of this system. When an administrator blacklisted the website, the system should deny the access to reach the website by user-access level. For example, an administrator only blacklisting the website for kids only. So the kid's group unable to access the website. It is because the proxy server filters all traffic through the website URL. Fig. 6 shows the example of a rule that the system has been blocked user to access the website.

Fig. 6. Example of Rules

Fig.7 shows the example of list rules that has been managed by an administrator. As we can see, the administrator does not allow kid's group access the Facebook URL.

Fig. 7. List Rules Page

Fig. 8 shows the Kidsafe log that Facebook URL has been blocked by a system. The proxy server has been rejected user access the Facebook URL.

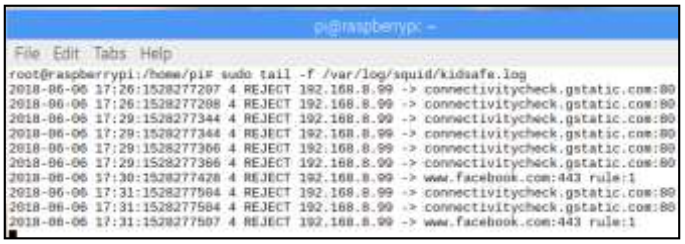

Fig. 8. Kidasfe Log

VII. TESTING AND RESULT

In software testing, the behavior of the whole system is tested as defined by the scope of the development project. It may include tests based on risks and requirement specifications, use cases, or other high level descriptions of application behavior, interactions with the operating systems and system resources. Software testing is most often the final test to verify that the system to be delivered meets the specification and its purpose.

A. User Registration Module

Table 2 shows the test case of the user registration module. This testing has been performed by the developer using an administrator account.

TABLE II. User Registration Module

Test ID	TID01
Description	Add new user into the system
Test type	Positive
Precondition	Developer must login as an administrator account
Input definition	• Administrator enters username and password • Administrator clicks "Login" button • Administrator clicks "Users" tab • Administrator clicks "Add new user" button

	• Administrator insert the user information • Administrator clicks "Save" button
Output definition	Administrator gets message "New user added". System gets new user.
Remark	The registration a new user has been successful.

B. User Authentication Module

Table 3 shows the test case of user authentication module. This testing has been performed by the developer using a normal user account.

TABLE III. User Authentication Module

Test ID	TID02
Description	Checking the user authenticate login
Test type	Positive
Precondition	User must login with the valid username and password
Input definition	• User enters username and password • User clicks "Login" button
Output definition	User gets message "Welcome" on top browser. User able to manage their account by itself.
Remark	User successfully login into system with the valid username and password

C. Time Control Management Module

Table 4 shows the test case of the time control management module. This testing has been performed by the developer using an administrator account.

TABLE IV. Time Management Module

Test ID	TID03
Description	Manage time for user to access the internet
Test type	Positive
Precondition	Developer login as administrator
Input definition	• Administrator enters username and password • Administrator clicks "Login" button • Administrator clicks "Users" tab • Administrator clicks "List of Users" button • Administrator clicks one of username • Administrator insert the number for login expiry • Administrator clicks "Save"
Output definition	Administrator can control time management of user access the internet.
Remark	User unable to access the internet after the session expired

D. User Log Management Module

Table 5 shows the test case of the time control management module. This testing has been performed by the developer using an administrator account.

TABLE V. User Log Management Module

Test ID	TID04
Description	Track user login into the system
Test type	Positive
Precondition	Developer login as administrator
Input definition	• Administrator enters username and password • Administrator clicks "Login" button • Administrator clicks "Log viewer" tab button
Output definition	Administrator can view the history of user login into the system
Remark	Administrator successfully view the log viewer.

E. Rules Management Module

Table 6 shows the test case of rules management module. This testing has been performed by the developer using an administrator account.

TABLE VI. Rules Management Module

Test ID	TID05
Description	Manage the rules such as add blacklist website
Test type	Positive
Precondition	Developer login as administrator
Input definition	• Administrator enters username and password • Administrator clicks "Login" button • Administrator clicks "Rules" tab • Administrator clicks "Add rule" tab • Administrator insert the website URL • Administrator clicks "Add rule" on bottom button
Output definition	Administrator can view the history of user login into the system
Remark	Administrator successfully view the log viewer.

F. Security Testing Module

Table 7 shows the test case for checking security login for this system. This testing has been performed by the developer.

TABLE VII. Security Testing Module

Test ID	TID06
Description	Checking security login whether secure or not
Test type	Positive
Precondition	Run SQLMap on Kali linux
Input definition	• Open Kali Linux • Go to terminal • Enter this command "sqlmap –u "http://192.168.2.2/kidsafe/" –-dbs –level=5 –-risk=3"
Output definition	The testing result shows the system is not able to injectable.
Remark	The login system is not able to injectable.

Based on all the test case above, all the results will be compiled in the Table 8 below:

TABLE VIII. Summary of the Results

Test ID	Module	Description	Expected Result	Result
TID 01	User registratio n by administra tor	Add new user into the system	Administrator successfully added new user into the system	Pass
TID 02	User authentica tion	Login phase that's authenticat e user	System able to verify valid user on authentication login	Pass
TID 03	Time control manageme nt	Manage time for user access the internet	Administrator able to manage time for user while accessing internet	Pass
TID 04	User log manageme nt	Track user log in into the system	Administrator able to view the record of user log	Pass
TID 05	Rules manageme nt	Manage the blacklist website	Administrator able to manage the rules	Pass
TID 06	Security Testing	Checking security login	The system is not able to injectable	Pass
TID 06	Security Testing	Checking security login	The system is not able to injectable	Pass

As a summary, all functionality and testing are well functioning. Furthermore, the expected result from the outcome of this testing phase are satisfied. The actual result meets the objective and the testing gains good results meet the expectation.

VIII. CONCLUSION AND RECOMMENDATION

In conclusion, every Parental Control Software is unique on its own and provides parents with the basic security to keep their children safe from the harmful content present online. Whether it's web filtering, time usage limit or blocking inappropriate website, every application helps us in one way or another. The prototype also has been tested to ensure the system works successfully. However, the test result shows the system have met the project goals.

This project has been successfully developed and implemented. However, it can be improved targeting more advanced and better system in the next stage of research. For future improvement, the system need to add One Time Password (OTP) to authorize legitimate user only for security purpose. The user must enter the correct pin number OTP to login the system. For another recommendation is to implement this system at school where it can control the student's activity when they access the internet, but it is requiring a powerful device to support more user.

REFERENCES

[1] Cioffi, C., Pagliarecci, F., & Spalazzi, L. (2009). An anomaly-based system for parental control. *Proceedings of the 2009 International Conference on High Performance Computing and Simulation, HPCS 2009*, 193–199.

[2] Santisarun, P., & Boonkrong, S. (2015). Social network monitoring application for parents with children under thirteen. *2015 7th International Conference on Knowledge and Smart Technology (KST)*, 75–80.

[3] Fitzpatrick, J. (2014). Five Best Content Filtering Tools. Lifehacker. Retrieved from https://lifehacker.com/5312820/five-best-content-filtering-tools

[4] Calyptix. (2016). Types of Web Filters and How They Can Work for Your Clients. Retrieved from https://www.calyptix.com/top-threats/types-of-web-filters-and-how-they-can-work-for-clients/

[5] Prakash, B. (2014). Web Content Filtering: Inline Versus Endpoint-Based Filtering. Security Intelligence. Retrieved from https://securityintelligence.com/web-content-filtering-inline-versus-endpoint-based-filtering/

[6] Dave, R. (2013). Internet Monitoring Software. Retrieved from https://promos.mcafee.com/offer.aspx?id=550332

[7] KidWatch Review. (2018). Retrieved from https://www.nextadvisor.com/parental_controls/kidswatch_review.php

[8] Neil, J. R. (2018). ContentWatch Net Nanny 7. Retrieved from http://sea.pcmag.com/contentwatch-net-nanny-7/19380/review/net-nanny

[9] Neil, J. R. (2008). CyberPatrol Parental Controls 7.7. Retrieved from https://www.pcmag.com/article2/0,2817,2334004,00.asp

[10] Ghosh, A. K., & Wisniewski, P. (2016). Using a value sensitive design approach to promote adolescent online safety on mobile platforms. *Proceedings - 2016 International Conference on Collaboration Technologies and Systems, CTS 2016*, 593–596.