Website Defacement Detector

by

Mohammad Sharul Mizwan Bin Md Salleh

Dissertation report submitted in partial fulfillment of
the requirements for the
Bachelor of Technology (Hons)
(Information and Communication Technology)

MAY 2013

Universiti Teknologi PETRONAS
Bandar Seri Iskandar
31750 Tronoh
Perak Darul Ridzuan

CERTIFICATION OF APPROVAL

Website Defacement Detector

by

Mohammad Sharul Mizwan Bin Md Salleh

A dissertation report submitted to the
Information and Communication Technology Programme
Universiti Teknologi PETRONAS
in partial fulfillment of the requirement for the
BACHELOR OF TECHNOLOGY (Hons)
(INFORMATION AND COMMUNICATION TECHNOLOGY)

Approved by,

_____
(Pn. Norshuhani binti Zamin)

UNIVERSITI TEKNOLOGI PETRONAS

TRONOH, PERAK

May 2013

CERTIFICATION OF ORIGINALITY

This is to certify that I am responsible for the work submitted in this project, that the original work is my own except as specified in the references and acknowledgements, and that the original work contained herein have not been undertaken or done by unspecified sources or persons.

_____

MOHAMMAD SHARUL MIZWAN BIN MD SALLEH

TABLE OF CONTENTS

ABSTRACT

It is undeniable that website has become an important element in the life of nowadays generation. As the website become more sophisticated, likewise the security threats that the website poses. One of them is website defacement in which unauthorized person changes the visual appearances of the website for various intention. Some are only for fun and hacking skill-testing, but worst case, it can be cause further severe security damages. It can be said that website defacement can causes security threats to a website and also can damage the reputation of the website owner. This is very bad especially for businesses-website because the website portray their public face. Usually, website administrator or website owner get the information about their website being deface too late, making public already see the messages or images on their defaced website which can humiliate and lower down their reputation. That is why, a website defacement detector is a must to be developed to monitor the website at a specific time interval and alert the website admin through email as soon as the system detected any unauthorized changes. Therefore, the target user for this application is the website admin and website owner. The approaches that will be implemented in this project are whether anomaly detection technique or hash tags comparison technique. The approach is not yet decided as this research study is yet to test on both approaches. Besides that this research study has conducted data collection such as interview, document studies and website defacement patterns observation. The results will help this research study to further develop a system that fulfills the requirements that a website admin or website owner might ask.

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

1.1 Background of Study

In this information age, people nowadays cannot live without the internet. The World Wide Web has become part of people's life and they want to get connected to the internet almost all the time for socialization, works and etc. People are connected to each other in the internet by the mean of websites or mobile applications.

Although most of the generations nowadays are familiar with websites, but to make this research study more understandable, a basic technical definition of what is a website must be provided. A website is collection of webpages that is coded using Hypertext Markup Language (HTML/XHTML) served from a single web domain, hosted on at least one web server and the websites can be accessed via network such as the internet through Uniform Resource Locator (Wikipedia, n.d.)[1]. The HTML source code of the website that is written by the developer of the website will be placed on a server so that the website can be accessed by the public using an internet address which is the URL of the website.

The first website ever created was done by Tim Berners-Lee, a British physicist who invented the CERN website in the year 1989 in a project called World Wide Web (WWW) intended for the information sharing between physicists around the world (CERN, n.d.). But, according to CERN (n.d.) [2] the WWW project was made available

[1] Wikipedia. (n.d.). Website. Retrieved June 15, 2013, from Wikipedia: http://en.wikipedia.org/wiki/Website

[2] http://info.cern.ch/

for the public to use the technology on royalty free basis on 30 April 1993. This is the beginning where the websites started to grow rapidly as people started to build their own websites and based on CERN statistics, by 2013, there are estimated about 630 million websites available online. From the value portrayed, it is clear that online world has become part of people's life and all the created websites is the mean to achieve what they want and to ease their lifestyle in socials, politics, economics and etc.

The existence of website has changes the way people lives nowadays. The advancement in technology with the creation of the website has made the mean of communication and transaction to be easier and much faster as compared to conventional and traditional way. But, there will always be security threats poses in line with the advancement of technology. As technology grows, the security threats will also grow. A website is vulnerable to various security threats and one of the threats is hacking activity intended to deface the website for various intention.

According to Hollander (n.d.) in his research paper about website defacement, he states that the occurrence of website defacement is when unofficial intruders alter a website maliciously through techniques of substituting or inserting provocative and offending data to the website. Surprisingly, Hollander (n.d.) mentioned, web defacement is quite common as 19 percent reported that their website has been misused and suffered from unauthorized access with additional 32 percent saying that it is not in their knowledge whether their website has been tampered or not.

Based on MyCERT (n.d.)[3], website defacement is the attack or attempt to change a website visual appearance and generally, website defacement is considered a kind of electronic graffiti for fun and skill testing but recently, it has become the mean to spread messages for political reasons by the cyber protesters with political agenda.

Defacement of website did not just stop at only mean to spread political issues but a more severe attack can be conducted through website's defacement. Example as Catbird (n.d.) states in their website that mentioned, "Web site defacement refers to

[3] http://www.mycert.org.my/en/resources/incident_handling/main/main/detail/756/index.html

an attack that alters the content of your website with potentially offensive or erroneous graphics and text or, even more serious, places imperceptible code on your site which is activated when a user access it, often triggering a download of malicious code onto the user's hard drive which may subsequently be controlled by a hacker remotely". This show how serious website defacement can get and a countermeasure to avoid this problem from prolonging must be taken.

1.2 Problem Statements

The problem statements are as discussed below:

1.2.1 Security Threats

Website defacement can be caused by various reasons for the attacker to deface the website based on their personal agenda. Due to that, according to MyCERT (n.d.), website defacement has become more than just a mere electronic graffiti because hacker usually use the defacement as a milestone to start various more serious security threats such as botnets, phishing, spams, malware hosting and many more illegal activities. The detection and protection of website from defacement is a must as to avoid the possible vulnerability that the website may possess. "On certain extent, you will never know your web application was compromised as no defacement on any page identified" (MyCERT, n.d.).

1.2.2 Reputation Damage

Defacement of website can also damage the image of the company or organization that the website portrays. According to Catbird (n.d.)[4], a website is the company or organization face to the public and any illegal changes done to the website will severely damage the company's reputation and the relationship with their valued customer. This is because, a hacked website will show that their security mechanism is weak and sometimes, messages appeared on the defaced website is intended to humiliate the owner of the website. The customer can lose their trust on the security

[4] http://www.pharmingshield.com/pharmingshield/website-defacement.php

of the website of the company and the company can lose their current and potential customers.

1.3 Objective and Scope of Study

In the cyber world, there are many websites that can be accessed publicly and some people might manage more than one website at a time plus they are not monitoring the website for 24 hours a day due to human limitation that need to eat, rest and etc. It is hard to monitor a website from defacement 24 hours a day. Therefore, the objective of this research is:-

- To automatically detect unintentional or unauthorized changes in the monitored website.

There are many types of defacement such as defacement of currency, character, image and many more. But this research will be focusing on revising and improving the algorithm to detect any changes done in a website and develop an open source system to automatically detect unauthorized changes in a website and inform the appropriate person in charge of the changes so that appropriate action can be taken.

Existing defacement detectors that the literature found are Site24x7[5], Binary Canary[6] and Nagios XI[7]. Unfortunately, some of them are not publicly available. The users of the system must pay a certain amount of money to use it and the focus of this research study is to develop a matching system but can be available for free of charge.

[5] http://www.site24x7.com/monitor-webpage-defacement.html
[6] http://binarycanary.com/en/default.cfm
[7] http://www.nagios.com/solutions/website-defacement-detection

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

Artificial Intelligence (AI) is the major concept that is being integrated in this research study. According to Wikipedia (n.d.)[8] as referred to McCarthy (2007), the term AI was first coined by McCarthy (1956) at Dartmouth Conference and McCarthy define AI as "the science and engineering of making intelligent machines". Nilsson (2009) agrees that AI might lack of true definition that is agreed upon everyone but he suggest that AI is "activity devoted to make machines intelligent, and intelligence is that quality that enables an entity to function appropriately and with foresight in its environment".

Besides that, Russel and Norvig (1995) in Artificial Intelligence: A Modern Approach textbook has extracted the AI definitions from eight textbooks and come to derived that AI is a system that think and act rationally like a human. On top of that, Dobrev (2004) in his research to give a formal definition of AI suggest informally that AI is a program that do not know anything but can learn and "AI will be such a program which in an arbitrary world will cope not worse than a human". Based on the definitions provided, all four authors agrees that AI is a technology to develop a system or machine that can possess human ability to act and behave rationally and can learn by themselves accordingly. That is why this research project is implementing AI as it major concept as to integrate the intelligence into the system that are going to be developed to detect website defacement, to develop an intelligent system that can automatically detect unauthorized changes in monitored website.

[8] http://en.wikipedia.org/wiki/Artificial_intelligence

One of the branches of AI is data mining According to Han and Kamber (2006), data mining can be simply-defined to refer to the extraction or 'mining' information or knowledge from enormous quantity of data and the actual term is misnomer. Often, people consider data mining as the synonym for Knowledge Discovery from Data (KDD) but there exist some other views that said that data mining is an essential analysis steps in KDD process (Han & Kamber, 2006). KDD main concerns is to acquire new, valid and useful knowledge from sets of data and according to Kroeze et al., (2004) as referred to Berson and Smith (1997) maintain that, "'in the case of large databases sometimes users are asking the impossible: "Tell me something I didn't know but would like to know". This shows that it is hard to obtain new knowledge from large sets of data. That is why data mining is the essential analysis steps in KDD process which intelligently extract data patterns to be observed, evaluated and presented in the next steps of KDD. The same concept will be implemented in the system that will be developed in this research study.

According to Wikipedia (n.d.)[9], "the actual data mining task is the automatic or semi-automatic analysis of large quantities of data to extract previously unknown interesting patterns such as groups of data records (cluster analysis), unusual records (anomaly detection) and dependencies (association rule mining)". The data analyzed through the process can be considered as a result or summary of the input and it can be used for further analysis and study. In simple word, data mining gathers and uses the information from the past data to analyze the result of a problem that may arise (Wikipedia, n.d.)[10].

Data mining has six common classes of task which are anomaly detection, association rule learning, clustering, classifications, regression, summarization and sequential pattern mining. But this research study focus on the anomaly detection (Davanzo et al., n.d.), and hash code (Kanti et al., 2012). The mentioned approaches will be studied in order to gain valuable information and knowledge on how to detect and develop a system to automatically detect website defacement.

[9] http://en.wikipedia.org/wiki/Data_mining
[10] http://en.wikipedia.org/wiki/Data_mining

2.2 Website Defacement

Website defacement as stated in Chapter 1 of this research study and as stated by Davanzo et al., (n.d.) is "unauthorized modifications to a web site". This means that website defacement is an attempt of other person which have no authorize access to the website to change illegally the source code of the website in order to change the visual appearance of a website and often this is done by hacker or cracker to test their skills and as an act of electronic graffiti.

But, according to MyCERT (n.d.)[11] the website defacement recently is not just an act of electronic graffiti but in is also done for political agenda intention and it can become worse as stated by CatBird (n.d.)[12] which mentioned in their website that website defacement can be an act to change the source code of a website and insert "potentially offensive or erroneous graphics and text or, even more serious, places imperceptible code on your site" which can download malicious code into hard disk of someone accessing the defaced website. This makes the person's data and personal information to be vulnerable to the hacker that installs the malicious code remotely. Furthermore, Kanti et al., (2012) also agreed that website defacement is an attack to modify the appearance of a website visually and website defacement is occurring when "a hacker changes the page of a website to something other than what was originally there".

By all three definitions of website defacement, it can be concluded that website defacement is an attack to change the website visual appearance but it can lead by many other intentions and causes further severe attack which is dangerous to the owner of the defaced website and also the person accessing the defaced website. There are many recent cases involving website defacement and it is still a puzzle when website defacement was first start but many researchers have done researches regarding web defacement as to contribute valuable knowledge into the website defacement field and thus encouraging the development of tools to detect website defacement and avoid further security threats.

[11] http://www.mycert.org.my/en/resources/incident_handling/main/main/detail/756/index.html
[12] http://www.pharmingshield.com/pharmingshield/website-defacement.php

2.3 Existing Cases of Website Defacement

2.3.1 Global Website Defacement Cases

Many cases involving website defacement done by hacker for political or individual interest and intentions can be found on the internet. Some of it as stated by Baloch (2013)[13] in an online newspaper article, Indian hacker who acknowledge themselves as 'NIGh7 F0x' has attacked and deface the homepage of The Election Commission of Pakistan's website and the attack is done at the peak traffic when people is busy visiting the website to know latest info regarding the election and the attack has cause the website to be not available to be accessed. This is clearly done for political agenda of the hacker.

In other case, The Human Rights Commission of Pakistan's website has been hacked by United Arab Emirates (UAE)'s hacker who claimed themselves as 'Gh()sT HAXOR- BOZZERROR' and then the website has been counter hacked by Pakistan Cyber Army (PCA). The intention is unclear but there is a threat given by UAE hacker and warning to never hack UAE website or server through this warning message: *"Never touch UAE ./Web or cyber or we will burn every web on your server"* and *"This is just a warning message to all newbie hackers don't step into Khaleej systems"* (Desk, 2013)[14]. The screen shot of this event is as follow:

[13] http://tribune.com.pk/story/528721/ecp-website-defaced-by-indian-hacker/
[14] http://tribune.com.pk/story/512891/hrcp-website-taken-down-by-hackers/

Figure 2.1: Defacement done by UAE hackers to Pakistan's website

Figure 2.2: The counter-attack done by PCA towards UAE defacement

Desk (2013)[15] also reported in The Express Tribune that Pakistani hacker that identify themselves as 'CyberHax0rs' has hacked Pakistan Telecommunications Company Limited (PTCL) just for fun.

Figure 2.3: The defacement done by 'CyberHax0r' for fun

CBCNews (2013)[16] also reported that National Public Radio (NPR), a non-profit broadcaster for US has been hacked by hacker that support Syrian President Bashar Assad's regime. There are plenty more cases but from all the above cases reported by The Express Tribune it can be said that hacker deface a website for various reasons and some can jeopardize the security of the website owner and also the visitors with the threats and warning from the hacker.

2.3.2 Local Website Defacement Cases

The previous news discussed is global news and to narrow down the topic to become nearer, there is also local news in Malaysia regarding website defacement. To make it short, in 2011 a blogger said that 15th of June was a disaster to .gov.my website as

[15] http://tribune.com.pk/story/488464/ptcl-official-website-hacked/
[16] http://www.cbc.ca/news/technology/story/2013/04/16/technology-npr-hackers-sea.html

the mass hacking of Malaysia's government website by international hacker, who called themselves as Anonymous. It happens due to "Government's censorship of the Internet and because Malaysia had blocked 10 file sharing sites"[17]. According to Kun (n.d.), there is also local hacker that called themselves as Dragon Force who deface Malaysia's website to fight to get back their freedom of internet and to remind the website owner to put extra security on their monitored website and among the website in Malaysia hacked by Dragon Force using their interfaces, all of them can be referred in Kun's blogspot[18].

Malaysia Official Government Website
(DoS / Switched off - Up at 3:49am - Down at 4:06am)

Other Malaysian wesites:

SabahTourism.com	Hacked + leaked	
Tour Malaysia (Not Tourism Malaysia)	Hacked	
Tourism Malaysia	Unaffected	
UiTM Penang	Hacked	
JBiotech	Hacked	
Social Welfare Department (Ezi2Care)	Hacked	
CIDB	Hacked but back up	12:20am
Land Public Transport Commision	Hacked but back up	12:15am
1Malaysia	DoS / Switched off	3:45am
Malaysian Communications and Multimedia Commission	Unaffected	
ASEANConnect	DoS / Switched off	
Malaysian Meteorological Service	DoS / Switched off	
Ministry of Education	DoS / Switched off	
Suruhanjaya Pilihanraya Malaysia	DoS / Switched off	
Bomba	DoS / Switched off	
TMNet	Unaffected	
Perbendaharaan Malaysia	DoS / Switched off	
Kementerian Kerja Raya Malaysia	DoS / Switched off	
Parlimen Malaysia	DoS / Switched off	
Malaysian Treasury	DoS / Switched off	
University Kebangsaan Malaysia	DoS / Switched off	
Jobs Malaysia	DoS / Switched off	
Information, Communications and Culture	DoS / Switched off	
Human Resouce Ministry	DoS / Switched off	3:59am
National Sports Council	DoS / Switched off	
Polis Diraja Malaysia (PDRM)	DoS / Switched off	

Figure 2.4: Full list of website defacement events happened caused by Anonymous to Malaysia's government website

[17] http://wanrulez.blogspot.com/2011/06/mass-web-defacement.html
[18] http://ezany-kun.com/senarai-laman-web-malaysia-yang-telah-di-hacked-dragon-force-rilekscrew/

Recent attack in 2013 of web defacement in Malaysia is the cyber war between Philippine and Malaysia's hacker where the Malaysia's hacker decided to take revenge on Philippine's websites on the dead of safety team of Malaysia in Semporna and Lahad Datu. Due to long list of website defaced and the screenshots, further information can be obtained from the link provided in the footnote section[19] [20]. This shows that defacement can happen regardless of demographic locations and governments and the intentions to deface a website are sometimes unclear but some of them sure possess security threats to modern world. Therefore, it is necessary to develop a system to detect website defacement to prevent more severe security threats as supported by Desiderius Erasmus (n.d.)[21] which mentioned, "Prevention is better than cure".

2.4 Website Defacement's Methods

There are many methods in defacing a website, but most commonly used method is through SQL injection that can allow administrative access. Based on Faulkner (2011)[22], SQL injection is "an exploit that takes advantage of poor web development techniques and, typically combined with, faulty database security" and the result is a complete compromised website. Another method is via DDoS (very effective) to jammed the target server and according to Faulkner (2011), DDoS occur when "server receive many requests and server resources are overloaded and the system simply locks up and shuts down". Other method is Port Scan. This is the method used to exploits weak port holes such as File Transfer Protocol (FTP), User Datagram Protocol (UDP) and Internet Control Message Protocol (ICMP) by scanning available ports to pretend as admin/staff to the hacked website and change the content illegally. All these methods can be successful because, according to MyCERT (n.d.)[23], intrusion attack especially website defacement is usually successful because of four factors which is weak password, vulnerable third party plug-in, improper files and directory permission and reuse of old backdoor.

[19] http://www.sararose.my/2013/03/senarai-laman-web-filipina-yang-dihack.html
[20] http://taotauajer.blogspot.com/2013/03/wow-perang-siber-antara-malaysia-dan.html
[21] http://www.brainyquote.com/quotes/quotes/d/desiderius148997.html
[22] http://www.howtogeek.com/97971/
[23] http://www.mycert.org.my/en/services/advisories/mycert/2013/main/detail/919/index.html

2.5 Website Defacement's Statistical Information

Defacement of a website is a very serious cyber-attack. According to the statistic from NationMaster (n.d.), the website defacement of a website that is happening in Malaysia is only 1.7% of all the website defacement that happened globally. And globally, according to Almeida and Mutina (2011)[24], there article in Zone-H reported that in 2010 there are near 1.5 million website defacement cases happening.

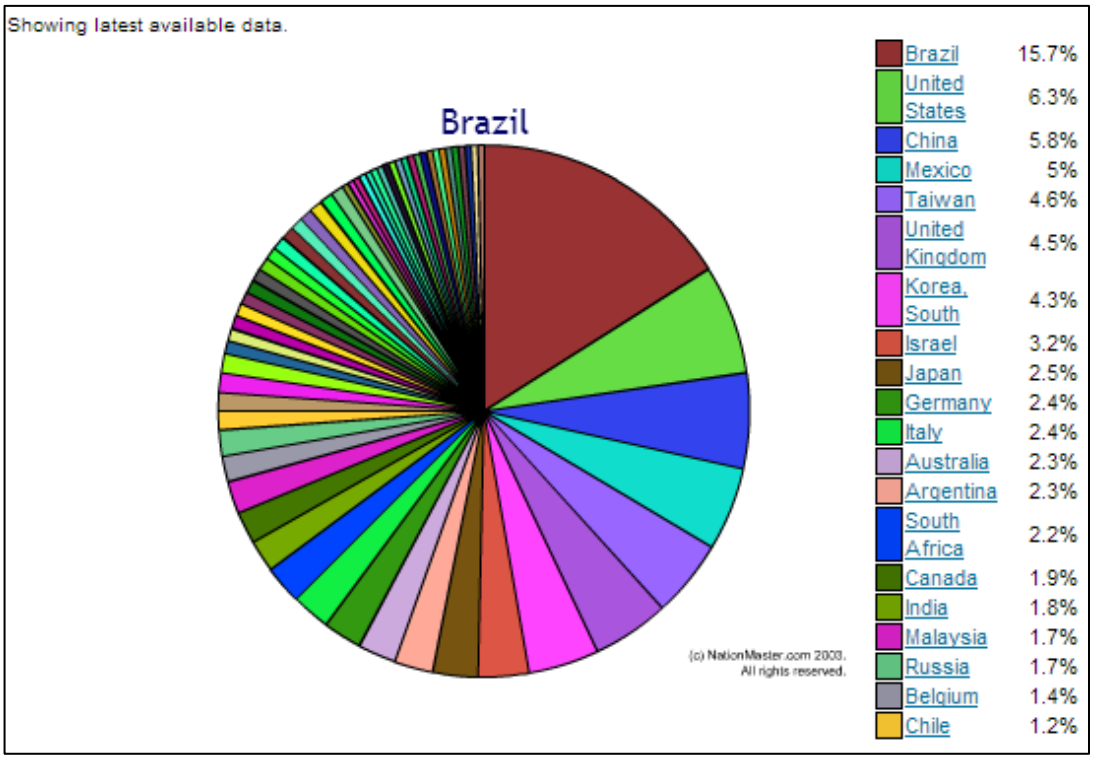


Figure 2.5: Website defacement statistic by countries.

In Malaysia alone website defacement is one of the most common attacks. Based from MyCERT (2012)[25] report, in quarter three of 2012, there are 1099 intrusion incidents reported by MyCERT (increase of 0.36 from last quarter) and most reported intrusion attach is website defacement which is 821 reports out of the 1099 intrusion reports. This means that website defacement is the most cases reported among all of the intrusion cases reported to MyCERT. The percentages of incidents that happened in quarter three of 2012 and the percentage of website defacement happen in Malaysia can be referred in the Figure 6 and Figure 7 as shown below:

[24] http://www.zone-h.org/news/id/4737
[25] Q3 2012 Volume 32 report: http://www.cybersecurity.my/data/content_files/12/1078.pdf

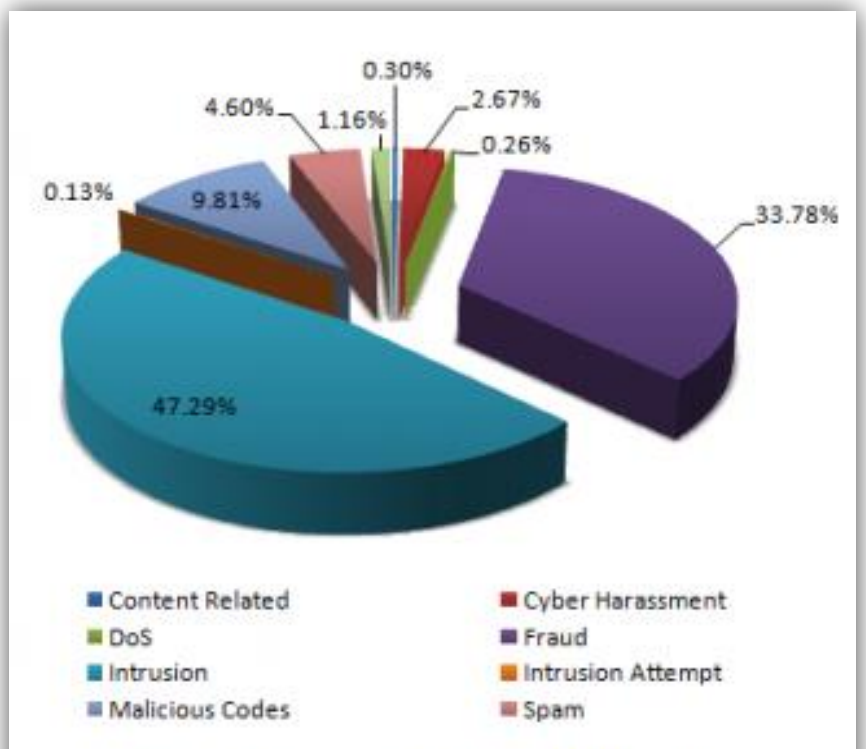


Figure 2.6: Percentage of incidents reported to MyCERT in quarter three 2012

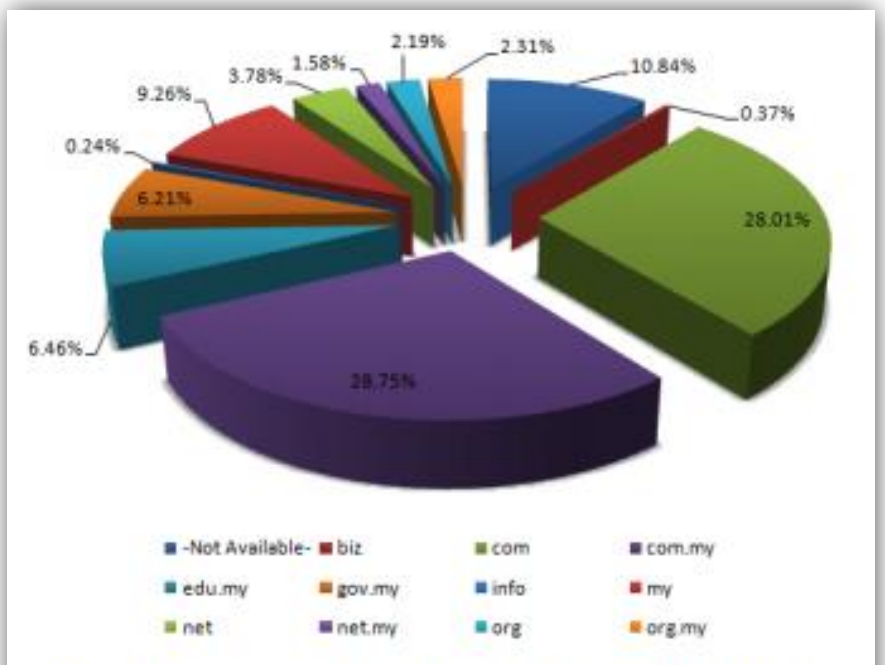


Figure 2.7: Percentage of website defacement by domain in quarter three 2012

2.6 Current Approaches on Website Defacement Detection

This research will focus two approaches to detect website defacement as suggested by two previous studies which is through hash code and anomaly detection. According to Wikipedia (n.d.) "anomaly detection is the search for data items in a dataset which do not conform to an expected pattern". Website defacement, as introduced is a process of illegal modification to a website and to detect such modification is very difficult due to the dynamic nature of a webpage as well as the website content and appearances vary throughout pages (Davanzo et al., n.d.). Based on the study done by Davanzo et al., (n.d.), anomaly detection technique can be feasible and effective solution to cater the dynamic nature of a website because "it does not require any prior knowledge about the page to be monitored". Anomaly detection can be applied to detect intrusion and Davanzo et al. (n.d.) is using the approach based on anomaly detection. There are many detectors that are previously used to detect intrusion being implemented in their study as experimental evaluation such as K-th nearest, Local Outlier Factor, Mahalanobis Distance, Hotelling's T-Square, Parzen Windows and Support Vector Machine (Davanzo et al., n.d.). This research study can implement and apply the result from the study done by them and learn the pros and cons of existing detection algorithm and choose the best approach to be implemented in developing the website defacement detector for this research study.

Another approach suggested by previous study on web defacement detection is hash code approach. The research done by Kanti et al. (2012) proposed algorithm for website defacement detection and also recovery as follow:

1) A web page (pi) is selected for defacement checking
2) Calculate Fresh Hash Code (ci) for chosen web page in step 1 using Secure Hash Algorithm.
3) Compare the Fresh calculated hash code (nci) with its stored hash code in database. If result of comparison is true, it is not defaced, but if otherwise the web page is defaced.
4) Use diff algorithm to compare the two sates of the same web page.

The method that Kanti et al. (2012) suggested to use in their diff algorithm is "DiffText(string TextA, string TextB)" that find difference in two texts without conversion, "DiffText(string TextA, string TextB, bool trimSpace, bool ignoreSpace, bool ignoreCase)" that find difference between two texts with optional conversion and "Diff(int[] ArrayA, int[] ArrayB)" that find difference in two arrays of integers. All three methods will return array of items containing the difference. This study is useful to gain knowledge on what is the efficient web defacement detection techniques as well as spotting exact defacement location and can be implemented in this research study for improvements of the project to be developed. These two approaches will be studied and analyzed by this research study to decide which to be implemented into the project development of this research study.

Existing website defacement detectors are as follow, Site24x7[26] Binary Canary[27] and Nagios[28]. Brief description and their weakness can be referred as follow:

Table 2.1: Description and weaknesses of existing website defacement detector

System	Description	Weakness
Site24x7	• Periodically monitor the content of your webpage • Notified if there is any change in content	• Provide free account but only basic monitoring and 10 min time interval checking
Binary Canary	• Can choose which web pages to monitor. • Checks for web server errors, plus scans website text for a key phrase specified.	• Provide free account but only at 15 minutes time interval and must purchase for 1 minute time interval
Nagios XI	• provides complete monitoring of websites	• Starting price $1995

[26] http://www.site24x7.com/monitor-webpage-defacement.html
[27] http://binarycanary.com/en/default.cfm
[28] http://www.nagios.com/solutions/website-defacement-detection

CHAPTER 3

METHODOLOGY

3.1 Introduction

This chapter will discuss about the research and development methodology that is applied in this research study. The aim and objective of this research study is to automatically detect unintentional or unauthorized changes in the monitored website. The chapter will consist of the research and development methodology used, data collection and data analysis done to achieve the aim and objectives of this research study.

3.2 Research Methodology

This research study is an applied research. According to Mr. Amatya (n.d)[29] in his lecture, applied research "aims at finding a solution for an immediate problem facing a society or an industrial/business organization" and WikiBooks (n.d.)[30] suggest that applied research is "designed to solve practical problem of the modern world". This met with the aim of this research study, to develop a system that can automatically detect unintentional or unauthorized changes in the monitored website. The research methodology approach that will be used in this research study is qualitative approach. In this research, a system will be developed in order to solve the problem statement that is mentioned in the Chapter 1 and to meet the objective of this research project.

[29] http://www.slideshare.net/nagendraamatya/applied-research-methodology-lecture-1
[30] http://en.wikibooks.org/wiki/Research_Methods/Types_of_Research

3.3 Development Methodology

The system development lifecycle or the development methodology that is implemented in this research study is Evolutionary Prototyping in RAD development methodology. This is chosen based on technology used (familiar technology which is Java and HTML), complexity (this research system is a complex system) and time schedule for completion (the time schedule for this project is short, only 28 weeks) of this research study. Figure 8 below shows the Evolutionary Prototyping implemented in this research study:

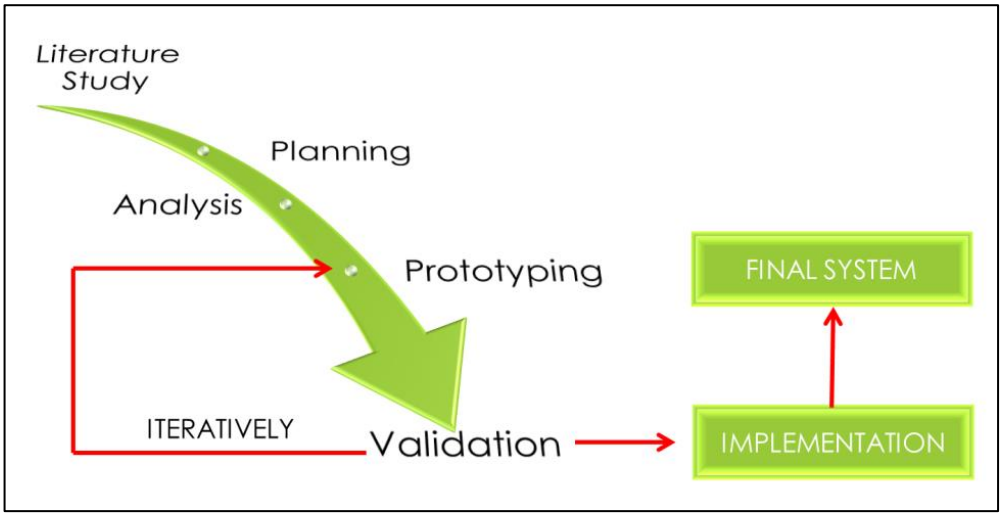


Figure 3.1: The Evolutionary Prototyping in Rapid Application Development (RAD)

3.4 Project Activities and Deliverables

3.4.1 Literature Study Phase

In this phase, this research study is doing literature studies of all previous research related on this research study topic, which is website defacement. In this literature study, the focus is not only on scholarly article, but also news article and reports from related agencies regarding the statistic and recent cases on website defacement be it global or in Malaysia. There are huge amount of references that the author refer. The purpose of the literature study is to gain further understanding and update author's knowledge on website defacement in order to pursue more in this research

study. This phase is important as to make the author aware and understand the works that will be ventured into.

3.4.2 Planning Phase

In this phase, the purpose is to gather relevant data regarding the research study topic and identify the problem that is going to be researched on and prepare the background of study as a foundation to this research study. The crucial element of this research study is to prepare a Gantt chart as a guide to this research study and to monitor the progress of the project. This research study Gantt chart and important milestone can be observed in the Appendices section of this research paper.

3.4.3 Analysis Phase

In this phase, this research study will focus on the data collection of information related to the study. The data collection method that is implemented in this research study is interview, document studies and also observation. Further explanation on the data collection method is elaborated in Section 3.6 (Data Collection) of this research study.

3.4.4 Prototyping Phase

This is the most important phase in this research study that will consume most of the time of the research. The main purpose of this phase is to develop a prototype of a website defacement detector that can automatically detect unauthorized changes to monitored website. As so far, in this research study, there is no prototype being developed yet, but the upcoming prototype is designed to have the following functions, editing tool, monitoring tool and alerting tool.

Further development is the website defacement detector website as the system that are going to be developed is a web based system and also mock website to test the system.

3.4.5 Validation Phase

In validation phase, a completed prototype of the defacement detector system will be tested in artificial environment to see whether the prototype is working as intended. Since the project development lifecycle used is evolutionary prototyping, if the prototype does not pass this phase, it will iteratively go to prototyping phase once again to do improvement on the current prototype and this will iteratively go on until it passes the validation and then will proceed to the implementation phase.

3.4.6 Implementation Phase

In this phase, a prototype that satisfies the research study is deployed and usability testing is done towards the prototype. Further improvement will be done before releasing final complete system.

3.5 Data Collection

3.5.1 Interview

The use of interview as one of data collection method is crucial in this research to develop further understanding in website defacement from professional in term of the technical aspect behind the detection of website defacement which is important for the development of this research study. According to Frechtling and Westat (2002), interview is used when the person to be interviewed has valuable information and knowledge regarding the research study and "that their perspectives affect the success of the project". As for this research study, it is important to interview technical personnel to know and understand more about what is behind a website that can be used to be able to detect unofficial changes in the website. The interview is done in unstructured way. This is because; there is no set of questions prepared before the interview. The person interviewed is individual that has high technical knowledge and skills regarding website and the interview commenced for about one and a half hour. The interview's result will be evaluated and analyzed accordingly to extract valuable information to be used in the development of the system.

3.5.2 Document Studies

Previous studies existed in many document libraries that has been done in website defacement field can give awareness and valuable information to help the development of this research study. According to Frechtling and Westat (2002) as referred to "Lincoln and Guba (1985) defined “a document as “any written or recorded material” not prepared for the purposes of the evaluation or at the request of the inquirer. Documents can be divided into two major categories: public records and personal documents” (Guba and Lincoln, 1981). The internet is the source to gather previous research studies regarding this research topic. Two previous studies found on the internet had implemented two approaches in detecting website defacement which is diff algorithm and anomaly detection approach.

By studying the previous research studies, many valuable information and knowledge is gained in order to help the development of this case study. The result is extracted from previous studies and will be analyzed accordingly further in this research study.

3.5.3 Observations

This research study used observation technique in collecting data. According to Frechtling and Westat (2002), observation technique is a method “by which an individual or individuals gather firsthand data on programs, processes, or behaviors being studied”. The developed system is tested on artificial environment and observed whether it achieve the aim of this research study or not. The result of the observations will be analyzed and further improvement of this research study will be drawn from the observations.

3.6 Data Analysis

The methodology that is being applied to analyze data in this research study is qualitative data analysis and mostly using interpretive technique on all the data collection method as mentioned above. Data gathered is examined and interpreted from the observer's interpretation. The result gathered through the method mentioned are analyzed and discussed in the next chapter of this research study.

3.7 System Architecture

In this section, the framework and flow charts of the project in this research study are as in Figure 3.2, Figure 3.3 and Figure 3.4 respectively as shown below:

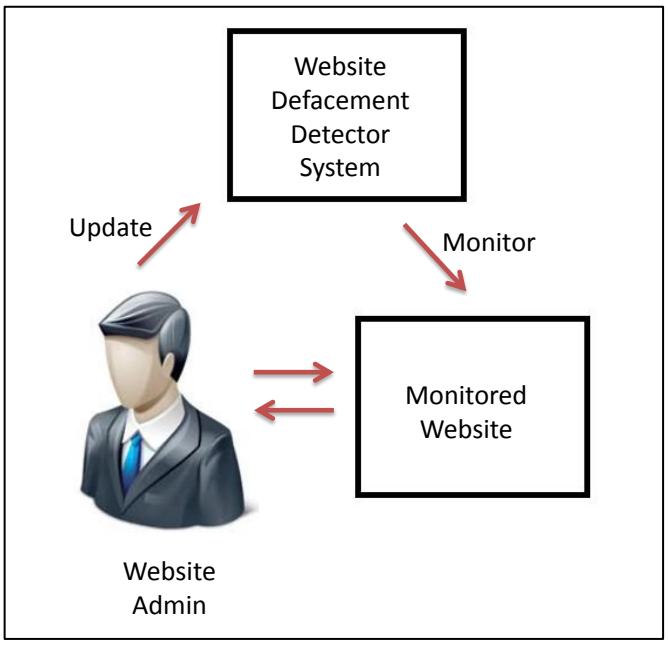


Figure 3.2: System framework of the website defacement detector.

The developed system is a web-based system and website admin must login or register in order to use the monitoring service. Every time the admin update their website, they can just click on the browser extension provided in order to update their website information in this system's database. And website defacement detector will monitor their website based on the updated information that they provide.

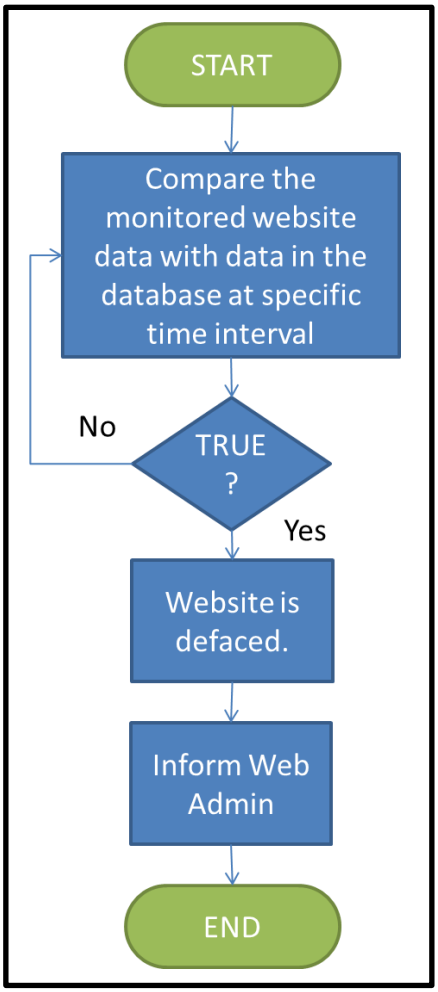


Figure 3.3: Process Flow Chart of the website defacement detector

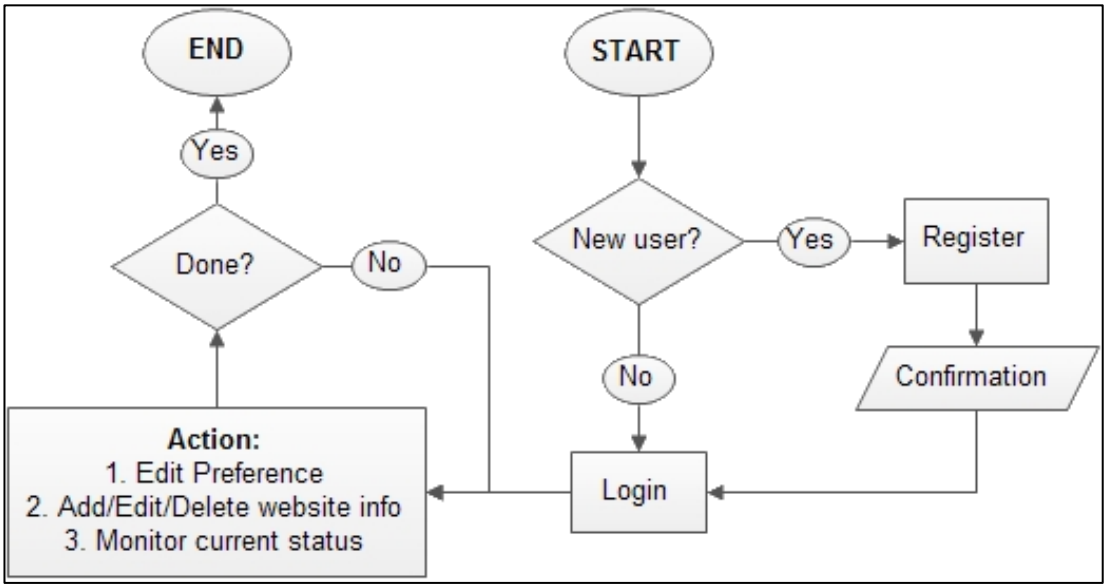


Figure 3.4: General Flow Chart for the system's website

3.8 System Requirement

The project in this research study is targeting the website administrator and also website owner because they are the one that use and administer a website most of the time. This application can help the target user to be aware of the defacement that happen in their website by alerting them as soon as the defacement is detected as to avoid further security threats and to avoid reputation damage.

The system requirement analysis is the hardware and software that the project needed in order to run smoothly in the target users' system. The requirements of the project in this research study are shown below:

Table 3.1: System requirement for the website defacement detector

REQUIREMENT	MINIMUM TOOLS
HARDWARE	
Standard Client	Personal Computer / Laptop / Any standard hardware.
SOFTWARE	
Operating Software	Windows XP
Development Tools	C++ / JAVA Programming language
Database Tools	Microsoft Excel / Microsoft Access
Documentation Tools	Microsoft Word 2003 / Notepad

CHAPTER 4

RESULTS AND DISCUSSION

4.1 Introduction

This chapter of this research study is discussing about the result and findings of the results. This chapter will contain the explanation and discussion about the data that are collected from interview, document studies, and website defacement's pattern observation.

4.2 Interview with Experts

In Chapter 3, it has been mentioned that this research study will collect data via interviewing technical person who have technical knowledge about the website. The information is vital in designing and developing system to detect website defacement in order to achieve the objective of this research study.

4.2.1 Respondent I

The first respondent was Mr. Izzatdin Bin Abdul Aziz, a lecturer in Computer and Information Sciences (CIS) department of Universiti Teknologi PETRONAS (UTP). The interview commenced for about 45 minutes. The objective of the interview was to get the basic idea on how the system can be developed from an expert point of view. Below is the results and discussion about the data gathered from the interview.

- **Proposed Initial Idea**

The initial idea of the project in this research study was to develop the website defacement system as a web-based system or to have the system as a stand-alone system like an antivirus to monitor the websites from defacement. However, after the interview, there were some fruitful comments given on the research study.

Firstly, it is found and noticed that, the system the author are going to develop is a very complex system and the system is possible to be built as a web-based system rather than as stand-alone system because, it is hard and complex for the stand-alone system to monitor websites. Therefore, it is recommended to develop a web-based tool. This research study is also stressed and emphasized to set the scope clearly and focus only on target users which are the website administrator/owners for the system development. Figure 13 below shows the initial framework of the web defacement detector that this research study comes out with:

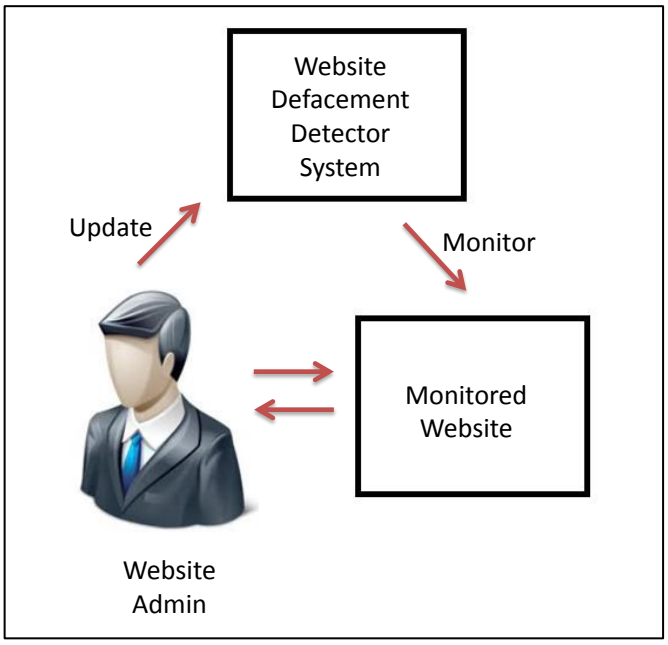


Figure 4.1: Initial framework for website defacement detector

- **Suggested Framework and Recommendations**

After the interview, this research study found that the initial proposed framework in this system will burden the website admin as the website administrator/owner as, they need to update their website as their tasks and they also have to update the database of the website defacement detector so that the system get current and up-to-

date data on the monitored website. This means that the website admin has to do double works updating their website and also the system database and a system should ease no burden. Therefore, through the interview, this research study has developed a new framework for the website defacement detector:

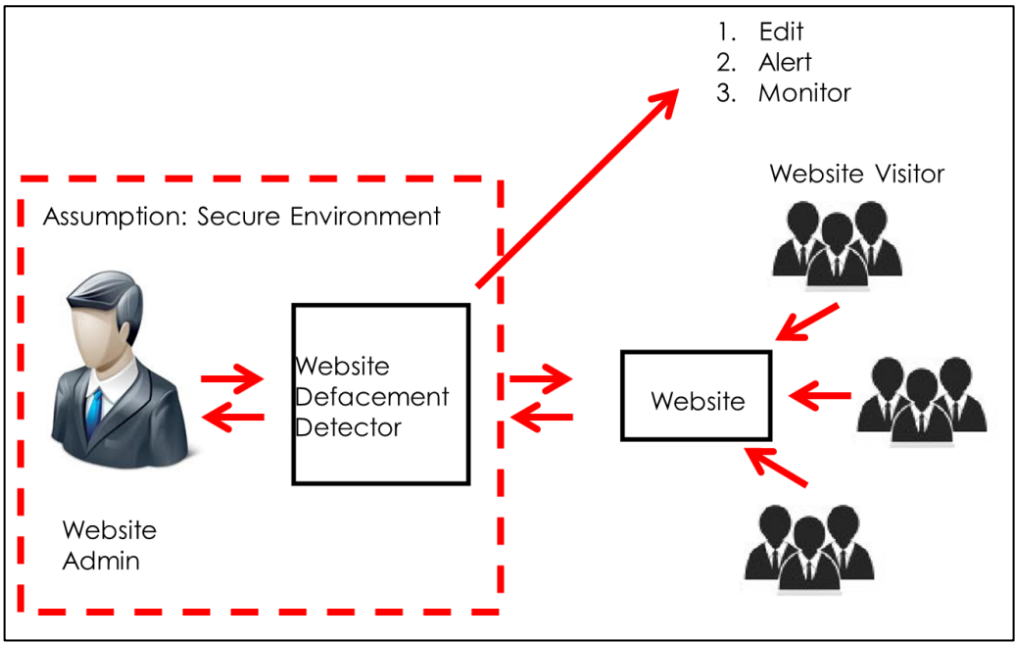


Figure 4.2: Suggested system architecture from Mr. Izzatdin.

In the new system architecture, the website defacement detector system is not an external stand-alone system that monitors the website, but rather, the system is developed to become the middle system for the website admin to update their website. This means that the system acts as a tool for the website admin to update and review their website. This is more efficient as it will indirectly update the database of the website defacement detector when the website admin finished updating the website. This will ensure that the system get the latest genuine data from the website admin on the monitored website with assumption that the admin is in a secure environment protected with firewall or Perimeter Network (DMZ) that add additional security layer. With this framework, the system is able to provide three basic and core functions which are as editing tool to update website, as monitoring tool to monitor the website at a specific time interval and as alerting tool to alert the website admin in case of defacement detection. In short, the system has three functions which are edit, monitor and alert.

4.2.2 Respondent II

Second respondent is Mr. Rizal Bin Yusoff is a student of Universiti Teknologi PETRONAS (UTP) that possesses very high skills in designing and website development. His portfolio[31] is very interesting to view. The interview commenced for 30 minutes through Google chatting services. Below are findings through this interview:

- **Website source code:-**

Most website are developed using Hyper-Text Markup Language (HTML) or PHP. According to Shannon (n.d.), HTML is a computer language that allows the creation of website and to be viewable by anyone on the internet. In other word, HTML is a language to describe to the browser in computer on how to display the website. While according to Rizal (2013), PHP is a scripting language that can be used to create websites. But, PHP is a server-side scripting language which means that the code is executed on the server and only the output is displayed to client's computer in HTML format.

As many know, most browsers allow the user to see the source code of the website that they are interested in. As for example, in Google Chrome browser, web page source code can be viewed by clicking button "Ctrl+U" or as below:-

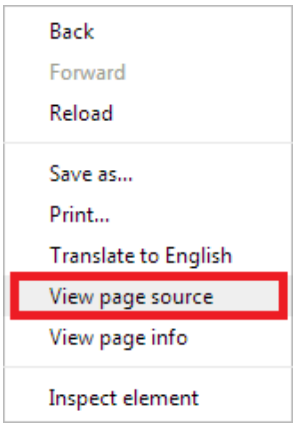


Figure 4.3: Viewing website source code using Chrome.

[31] www.ryzalyusoff.com

This discussion is important to this research study because, the aim of this research study is to develop a system that can automatically detect website defacement. The main focus is to detect and inform website administrator about the defacement.

Previously, this research study is going to use the suggested framework from the first interview, but after the second interview, this research study decided to use the initial framework which means that the system that are going to be develop is not a middle system but it will be developed as a third party system to monitor the websites. The system is going to be developed as a website where user must login and provide the details of the website that they want to be monitored such as its Uniform Resource Locator (URL). The system will provide installation for browser extension for easy update of the website current information and data. This means that, after the website admin has finished editing and updating their website, they can click on the browser extension to update the monitoring system about the new changes.

- **Initial Suggested Interface**

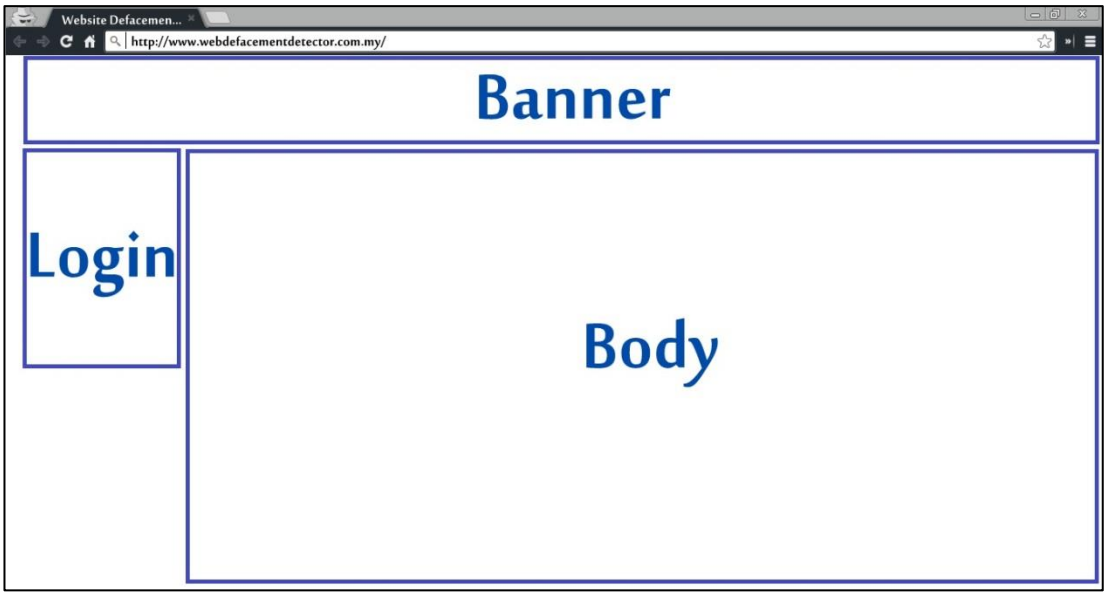


Figure 4.4: Suggested interface (not yet coded)

- **Developed interface**

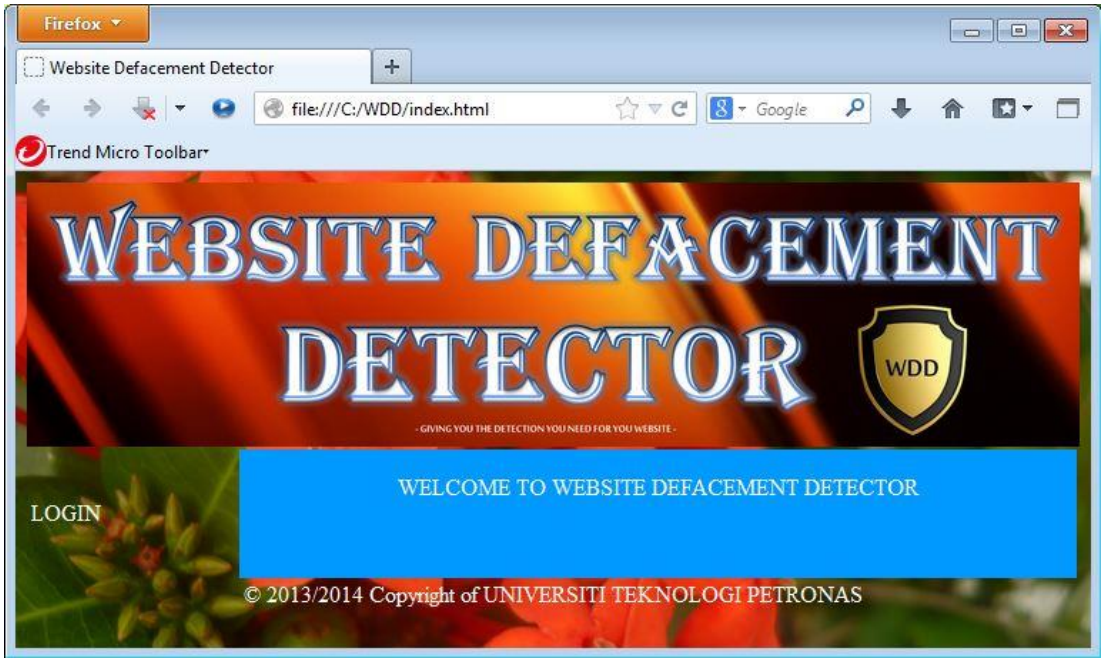


Figure 4.5: The coded interface of the website defacement detector

4.3 Document Studies

This research will explore more into two previous studies on website defacement detection approaches which are done by Davanzo et al. (n.d.) and Kanti et al. (2012) to choose the approaches is the best to be implemented in development of website defacement detector.

Davanzo et al. (n.d.) uses detection approach such as Anomaly Detection Technique in their study and they have experimented on six detectors and they come to conclusion that the detector Support Vector Machine is the most efficient detector to be used in their tested environment and data set. While Kanti et al. (2012) uses Hash Code and Diff Algorithm detection approach in their study. The Hash Code approach is to detect whether or not there is defacement in the monitored website and the Diff Algorithm is to find the location of the defaced website or in other word to alert the website admin where in the website's pane has been defaced. Refer Table 3 as follow for brief description about both researches:

Table 3: Previous studies about website defacement detection approaches

Detection approach	Brief Description	Reference
Anomaly Detection Technique	Experiment with following detector: 1. K-th Nearest 2. Local Outlier Factor 3. Mahalanobis Distance 4. Hotellinng's T-Square 5. Parzen Windows **6. Support Vector Machine**	Davanzo et al. (n.d.)
Hash Code & Diff Algorithm	1. A webpage is selected for checking. 2. Fresh Hash Code for selected webpage is calculated 3. Compare with hash code in database 4. If comparison true, not defaced, if not, defaced	Kanti et al. (2012)

The two studies mentioned above have found to be useful for the continuation of this research study project's development as it provide with existing approaches for the author to further test on the efficiency of the approach and to decide whether or not to implement the approach in this research study or to develop new approach. This research on the efficiency testing of the approaches by the two authors which is Anomaly Detection approach and Hash Code approach will be done further in this research study.

Moreover, this research study has also gained valuable information on how to detect the exact location of the defacement that commenced in the monitored website. This can be done by using the Diff Algorithm as proposed by Kanti et al. (2012). Using the Diff Algorithm, the system can know the location of the defaced website and can alert the website admin to do correction at that location rather than the website admin has to check one by one where the defaced part of the website is. There is no result to be shown in this stage as the system is still not completely developed yet but yet, this is to show the progress that this research study have made.

4.3.1 Hash Function

Progress so far, this research study has decided to use the hash function to detect the defacement done in a website. Data of the website, both from the website's real time

and the data stored in the database will go through hash function that will generate a hash code for both data and then, compared them at specific time interval. The time interval has yet to be decided as the code is not complete yet. This is because, it is necessary to know how long for a particular hash value to be generated and compared to know the optimal time interval for this system.

The real time data of the website is obtained through the source code of the website and the data of the website in the database is updated by website admin. Admin will update their website to this system each time they update their website as to make the system possess the latest data of the website to be compared and monitored. To ease the website admin, a toolbar button will be provided for them to easy update.

4.4 Website Defacement Pattern's Observation

This section provides the information of patterns observed in a collection of defaced websites. There are patterns of website defacement's that is noticeable and can contribute crucial information for this research study. The observations that are done are through Google and Forum and there is a lot of website involves around 50 websites. The demography that this research study found related on the website being defaced is at Pakistan, United Arab Emirate (UAE), Philippine and Malaysia. Normally, website defacement follows certain standards and criteria when they change the visual appearance of a website. The observation is as follow:

4.4.1 Location of the Defaced Webpage

As far as the author has observed, the main focus and target for someone to visually change the appearance of the targeted website is the homepage. They usually will attack the front page or the homepage webpage of the website. This is done because the homepage is where the website visitor is often will come across first before browsing other thing in the website. They want to be seen and they want to be acknowledged for their act of electronic vandalism, which explained why they chose the homepage of a website to deface. In certain isolated case, every webpage of the website is defaced with the same interface. The example is like Jabatan Agama Islam

Wilayah Perseketuan (JAWI)'s website[32] that has been hacked early in 2013 by Sofea Hana. All other webpage in the website is functioning as usual but only the homepage is being visually changed. They have fixed the defacement, but as for reference, the mirror of the defaced interface of JAWI website can be referred in zone-H website[33].

Figure 4.6: The JAWI website hacked (mirror)

As for the pane in the website, as far as the author observed in the source code if the website, usually they removes the entire pane and make it into only one pane and enter their respective images and messages in that pane on the homepage. But there is isolated case like in the Blog Serious case which only the header pane is changed and defaces, but the others remain the same. Therefore it can be concluded that basically a person usually defaced a website on its homepage and they usually remove the entire pane of the homepage and make it into only one pane to display their respective logo, messages and etc. This justification is important as to make the

[32] www.jawi.gov.my
[33] http://zone-h.org/mirror/id/19204586

defacement detection system to produce the best throughput by checking the highly possible webpage to be defaced rather than checking the entire website.

4.4.2 Type of Modification

Usually, as per observed, modification done on a defaced website is similar. Mostly, black background will be used. This is a good indicator for a defaced website especially if the defaced website is not using black background initially. In isolated case, some hacker uses color that they prefer like pink (in the JAWI case) or blue. Furthermore, the hackers that deface the website often put their logo on the website or their name to symbolize their pride to be able to deface that website. The logo and their name usually will be in bright color to be in contrast with the dark background and they often use the color that irritates eyes such as red and yellow. Moreover, they love to convey messages on the defaced website based on their intention on defacing that website. Usually the message is written in hard-to-read font and using bright-irritating color. Good example is as follow:

Figure 4.7: Government website hacked by Dragon Force used bright and irritating color on dark background

Figure 4.8: UiTM Penang Hacked by their ex-students used bright and irritating color on dark background

4.4.3 Website Defacement Intentionality

There are various reasons for a hacker to deface a website. Based on the pattern of messages published on the defaced website, the intention of defacement can be obtained. Some serious case, they deface the website as a benchmark for a more serious security and cyber-attack. But mostly, the intention to deface a website is simply an art of electronic graffiti and as a way to portray and test their skill and for fun only and there are also some that defaced a website based on personal agenda such as did not satisfy with government decision or based on political agenda. Example of intention from various attackers is as follow:

Figure 4.9: Anonymous hacked Sabah Tourism for fun but the information in the website database has been compromised

Figure 4.10: Dragon Forge hacked government website as an act of dissatisfaction on site-blocking on sharing site

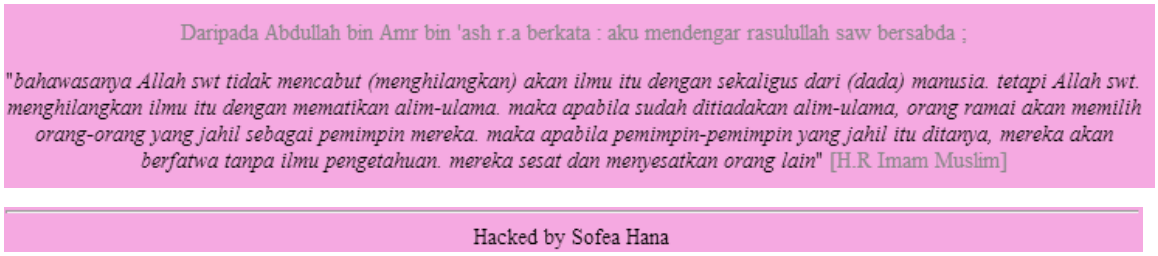


Figure 4.11: JAWI website hacked by Sofea Hana because she consider person in JAWI is not suited for the position

Although it is been looked as for fun, but this is considered as an intrusion case and might lead to information leaking and compromise the integrity of data in the website, further security-related damages and defacement can also ruin the image of the website owner. Therefore defacement detector is a must to conter-measure.\

CHAPTER 5

CONCLUSION

Nowadays, internet has been one of the most important tools to connect people around the globe and website has become the mean that provide the possibility for people to connect among themselves plus sharing information regarding their personal experience (blog) or sharing information about company (company website) and many more such as social networking website, search engine website and etc. According to the statistic of MyCERT (2013), the intrusion that has been reported is increasing each quarter in 2013 and mostly from all the security intrusion, the website defacement is the most intrusion reported. It is reported that website defacement is mostly for fun and skill testing but in this cyber world, as the technology become more sophisticated, likewise the security threats it possesses. Website defacement may be considered as one of electronic graffiti that change visual appearance of a website, but it is not only that, to be able to deface a website, means that the website is vulnerable to further serious security attack which may compromise the integrity of the data in the website and also damage the image of the company that the website portray.

Therefore, a website defacement detector is needed in this scenario as a way to protect website owner from the above-mentioned threats possibility. This is done as to support the Malaysia Computer Emergency Response Team (MyCERT)'s vision to reduce the probability of successful attacks and lower the risk of consequential damage and also as an act to support the CyberSAFE (Cyber Security Awareness For Everyone) campaign implemented by CyberSecurity Malayia.

There are plenty future works that can be done in order to improvise this website defacement detector. The most important one is the algorithm implemented in the

system developed, a study should be done as to obtain the most efficient algorithm and approach to be implemented in the system and more interviews should be done with the website admin to know their exact requirement on this topic. The development of this system will commence soon involving creating a prototype to be tested in an artificial environment, database design, flow chart and pseudo code development. After the prototype done, it will be tested a few round and will be done improvement on related area before completing another prototype for testing. The system is considered final when it passes the entire test and prove that the system can do what it is intended to do and lastly, a complete documentation called project dissertation on this system must be done for future reference to improvise this system.

REFERENCES

Almeida, M., & Mutina, B. (2011, June 1). *Defacements Statistics 2010: Almost 1,5 million websites defaced, what's happening?* Retrieved September 1, 2013, from Zone H: http://www.zone-h.org/news/id/4737

Amatya, N. B. (n.d.). *Applied Research Methodology.* Retrieved July 10, 2013, from SlideShare: http://www.slideshare.net/nagendraamatya/applied-research-methodology-lecture-1

Baloch, F. (2013, March 30). *ECP Website Deface by Indian Hacker.* Retrieved July 8, 2013, from The Express Tribune: http://tribune.com.pk/story/528721/ecp-website-defaced-by-indian-hacker/

Catbird. (n.d.). *What is Web Defacement*. Retrieved July 10, 2013, from Pharming Shield: http://www.pharmingshield.com/pharmingshield/website-defacement.php

CBCNews. (2013, April 16). *NPR Website Defaced By Hackers Supporting Syria.* Retrieved July 8, 2013, from CBCNews: http://www.cbc.ca/news/technology/story/2013/04/16/technology-npr-hackers-sea.html

CERN. (n.d.). *Twenty Years of a Free, Open Web*. Retrieved June 15, 2013, from CERN: http://info.cern.ch/

Davanzo, G., Medvet, E., & Bartoli, A. (n.d.). *A Comparative Study of Anomaly Detection Techniques in Web Site Defacement Detection.* Retrieved July 7, 2013, from IFIP Digital Library: http://dl.ifip.org/index.php/AICT/article/download/43029/3247

Desk, W. (2013, February 26). *HRCP Website Hacked, Counter Hacked.* Retrieved July 8, 2013, from The Express Tribune: http://tribune.com.pk/story/512891/hrcp-website-taken-down-by-hackers/

Desk, W. (2013, January 3). *PTCL Official Website Hacked.* Retrieved July 8, 2013, from The Express Tribune: http://tribune.com.pk/story/488464/ptcl-official-website-hacked/

Dobrev, D. (2004, January 19). *A Definition of Artificial Intelligence.* Retrieved July 1, 2013, from Cornell University Library: http://arxiv.org/pdf/1210.1568.pdf

Faulkner, J. (2011, November 16). *HTG Explains: How Hackers Take Over Web Sites with SQL Injection / DDoS.* Retrieved September 1, 2013, from HowToGeek: http://www.howtogeek.com/97971/

Frechtling, J., & Westat. (2002, January). *The 2002 User Friendly Handbook for Project Evaluation.* Retrieved July 11, 2013, from National Science Foundation: http://www.nsf.gov/pubs/2002/nsf02057/nsf02057.pdf

Han, J., & Kamber, M. (2006). *Data Mining: Concepts and Techniques.* San Francisco: Elsevier Inc.

Hollander, Y. (n.d.). *Prevent Web Site Defacement.* Retrieved July 10, 2013, from Google Scholar: http://202.41.82.144/data/HACKING_INFORMATION/PRINTED%20PAPERS/PREVENT%20WEBSITE%20DEFACEMENT.pdf

Kanti, T., Richariya, V., & Richariya, V. (2012, March 3). *Implementation of an Efficient Web Defacement Detection Technique and Spotting Exact Defacement Location Using Diff Algorithm.* Retrieved July 7, 2013, from IJETAE: http://www.ijetae.com/files/Volume2Issue3/IJETAE_0312_40.pdf

Kroeze, J. H., Matthee, M., & Bothma, T. J. (2004, December). *Differentiating Between Data-Mining and Text-Mining Terminilogy.* Retrieved July 5, 2013, from http://www.sajim.co.za/index.php/SAJIM/article/download/353/344

Kun, E. (n.d.). *Senarai Laman Web Malaysia Yang Telah Di Hacked Dragon Force | Rilekscrew.* Retrieved July 8, 2013, from Blogspot: http://ezany-kun.com/senarai-laman-web-malaysia-yang-telah-di-hacked-dragon-force-rilekscrew/

McCarthy, J. (2007, November 12). *What is Artificial Intelligence*. Retrieved July 1, 2013, from Stanford Formal Reasoning Group: http://www-formal.stanford.edu/jmc/whatisai/whatisai.html

Mitchell, T. M. (1997). *Machine Learning.* McGraw-Hill Science/Engineering/Math.

MyCERT. (n.d.). *What You Should Know About Web Defacement?* Retrieved June 15, 2013, from Malaysia Computer Emergency Response Team (MyCERT): http://www.mycert.org.my/en/resources/incident_handling/main/main/detail/756/index.html

Nilsson, N. J. (2009). *The Quest for Artificial Intelligence: A History of Ideas and Achievements.* Cambridge University Press.

Research Methodology. (n.d.). Retrieved July 12, 2013, from Institute of Hotel Management: http://www.ihmgwalior.net/pdf/research_methodology.pdf

Research Methodology: An Introduction. (n.d.). Retrieved July 11, 2013, from New Age Publishers: http://www.newagepublishers.com/samplechapter/000896.pdf

Russell, S. J., & Norvig, P. (1995). *Artificial Intelligence: A Modern Approach.* Englewood Cliffs, New Jersey: Alan Apt.

Turing, A. M. (1950). Computing Machinery and Intelligence. *Mind,* 433-460.

WanRulez. (2011, June 16). *Mass Web Defacement.* Retrieved July 8, 2013, from Blogspot: http://wanrulez.blogspot.com/2011/06/mass-web-defacement.html

WikiBooks. (n.d.). *Research Methods/Types of Research.* Retrieved July 11, 2013, from WikiBooks: http://en.wikibooks.org/wiki/Research_Methods/Types_of_Research

Wikipedia. (n.d.). *Anomaly Detection.* Retrieved July 9, 2013, from Wikipedia: http://en.wikipedia.org/wiki/Anomaly_detection

Wikipedia. (n.d.). *Artificial intelligence*. Retrieved July 1, 2013, from Wikipedia: http://en.wikipedia.org/wiki/Artificial_intelligence

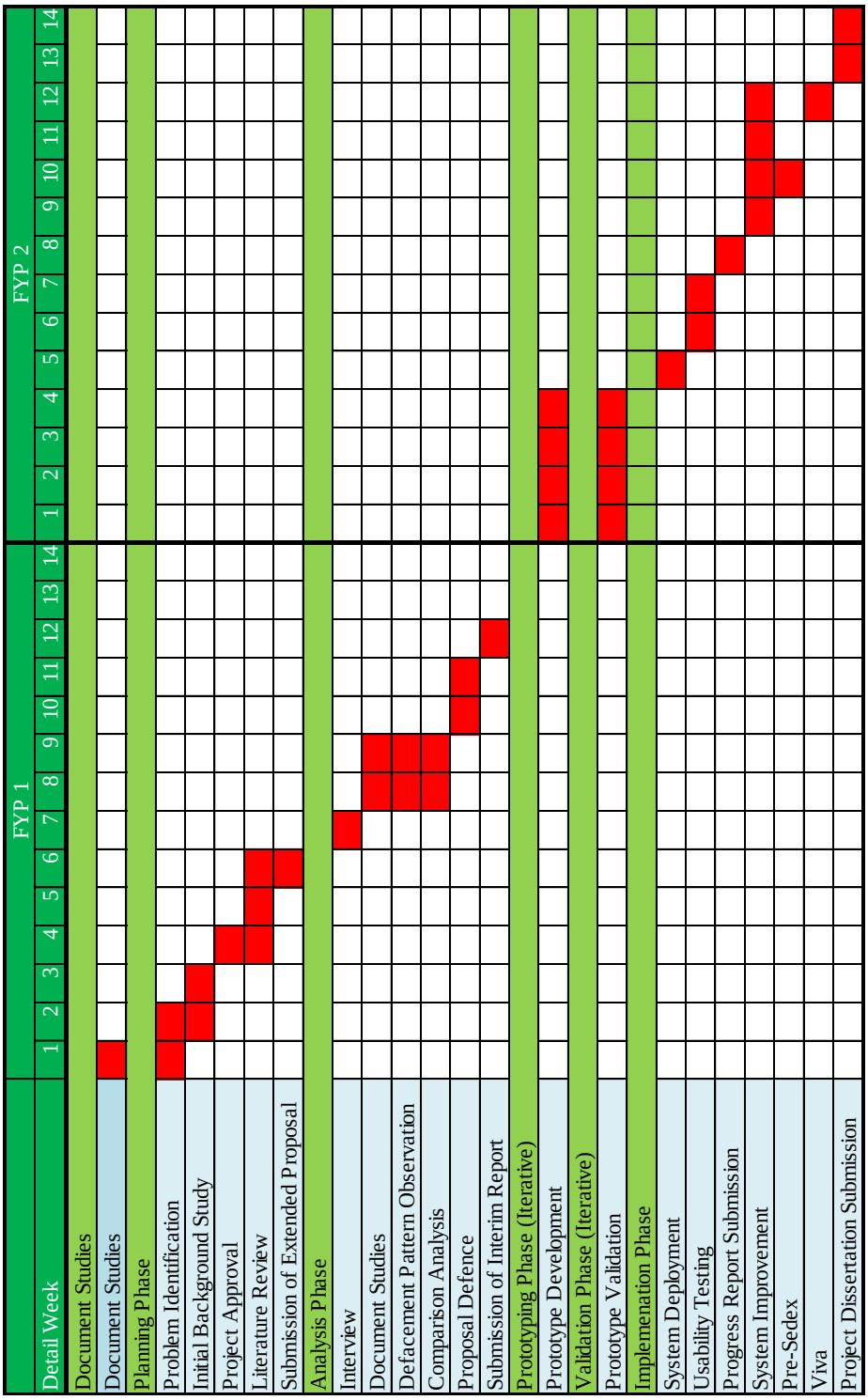
Wikipedia. (n.d.). *Data Mining*. Retrieved July 6, 2013, from Wikipedia: http://en.wikipedia.org/wiki/Data_mining

Wikipedia. (n.d.). *Machine Learning*. Retrieved July 5, 2013, from Wikipedia: http://en.wikipedia.org/wiki/Machine_learning

Wikipedia. (n.d.). *Website*. Retrieved June 15, 2013, from Wikipedia: http://en.wikipedia.org/wiki/Website

APPENDICES

Gantt chart:



Key Milestones: