EUROPEAN ACADEMIC RESEARCH
Vol. V, Issue 7/ October 2017

Impact Factor: 3.4546 (UIF)
DRJI Value: 5.9 (B+)

ISSN 2286-4822
www.euacademic.org

Web content filtration (WCF) Techniques across the Globe: A Review

SAURABH PANDEY
Research Fellow/ Producer Studio
Vardhman Mahaveer Open University, Kota (Rajasthan)
Dr. HARISH SHARMA
Associate Professor, Department of Computer Science
Rajasthan Technical University, Kota (Rajasthan)

Abstract:

Owing to the rapid change in technology, access of Internet is being common among all age groups across the globe but the accessed contents are associated with large amount of other unwanted material in different forms. These unwanted materials pose big challenges at personal and social levels. These unwanted materials are also a big challenge in terms of technical, legal and educational aspects. It is need of the hour to make information retrieval from the internet safe and credible (Willard, 2010). With the increase of obnoxious contents viz. violence, pornography, misconduct, mischief, suicide games etc. available on the internet, effective techniques and framework needed to inspect and block/ control unsolicited online content. An attempt has been made in present paper to review existing Web Content Filtration (WCF) techniques which are in practice around the world.

Key words: Filtration Techniques, Obscene Content, Web Content Filtration (WCF), Web Content category

INTRODUCTION

The saying ***"if you open the window for fresh air, you have to expect some flies to blow in"*** is perhaps a truth about

present IT revolution across the world. The media including images, videos including rhymes and educational videos, books, magazines, animations and video games are attracting children towards the internet in early ages. Educational institutions compel kids/ students to complete their project work/ assignment through internet. No one, including school educators, parents, and cyber experts have bothered about the dark side of the unwanted content available over internet, suicide video games for example blue whale game which caused several deaths, unsolicited and obscene contents over the web. On the other hand Internet has become a part of daily routine which is somehow affecting the every aspect of life. This is because it has become the electronic super highway where ones (every age group persons) information needs are satisfied. Internet has become a global communication medium and people of all age groups (kids - adults) to use it for their needs for computing, communication and more importantly reading, learning & teaching (Peddi Karthik, 2013). Unrestricted use of these contents is sufficient to derail kids / students / youths from the right path. The minds of immature children are mainly contaminated by these harmful games, fictitious and edited undesirable contents on internet which can be easily accessed over the web.

Prime Minister of England David Cameron announced a plan to filter online pornography by default for households in U. K., saying the initiative is about protecting children and their innocence (Peterson, 2013).

OBJECTIVES OF THE STUDY

It is well documented that watching the unsolicited content (pornographic content) has very adverse effect over the whole society especially to young mind. A research study led by scientists from the Gregorio Marañón University Hospital in Madrid and the Network of Centres for Biomedical Research in

Mental Health Networks (CIBERSAM) shows that adolescents experiencing a first outbreak of psychosis have lower levels of grey matter in their brains than healthy teenagers. This change was seen in patients suffering from various psychoses, including bipolar illness and schizophrenia. A study done by one of the well-regarded researchers in the field found that "high pornography consumption added significantly to the prediction of sexual aggression." (Kühn & Gallinat, 2014) It is also added that lack of grey matter in brain is linked to schizophrenia and bipolar disorders.

Considering the above, the research was planned with two fold objectives-

1) To review different categories of web content used for web content filtration (WCF)
2) To review different techniques of web content filtration (WCF) in practice

RATIONALE OF WEB CONTENT FILTRATION

It is unfortunate enough that at present there is no full proof mechanism to block/control all these unsolicited/unwanted contents immediately on the network level. In case of any communal anarchy, any rumour reaches to target people very fast which causes the immediate disturbance of peace.

On September 19, 2006, a military-led coup in Thailand overthrew the democratically elected government headed by Prime Minister *Thaksin Shinawatra*. Thailand is not unfamiliar with such upheavals. There have been seventeen coups in the past sixty years. This time, however, internet users noticed a marked increase in the number of web sites that were not accessible, including several sites critical on the military coup. A year earlier in Nepal, the king shut down the internet along with international telephone lines and cellular communication networks when he seized power from the parliament and prime minister. In Behrain, during the run-up

to the fall 2006 election, the government chose to block access to a number of key opposition sites. These events are part of a growing global trend. Claiming control of the internet has been come an essential element in any government strategy to rein in dissent – the twenty-first century parallel to taking over television and radio stations. In contrast to these exceptional events, the constant blocking of a swath of the internet has become part of the everyday political and cultural reality of many states. A growing number of countries are blocking access to pornography, led by a handful of states in the Persian Gulf region. Other countries, including South Korea and Pakistan, block web sites that are perceived as a threat to national security (Faris & Villeneuve, 2008, p.45).Indiscriminate Internet surfing is a major cause of entry for viruses, worms, Trojans, spyware, keyloggers, phishing, pharming and more. Notwithstanding there are essentially three motives or rationales for internet filtering: political filtering, social filtering and security/ conflict filtering.

Therefore, a robust and powerful network architecture plan and different kind of system algorithms (Network Level, Session Level, Application Level etc) is required to detect and control/block/monitor unsolicited/ unwanted contents over the web. Once any kind of network architecture & algorithms will be implemented, it can control/block/monitor any kind of specific content in a particular geographic area as and when needed. Therefore, a much more intelligent system equipped with different level of control is required to avoid the aforesaid shortcoming of present web content filtration (WCF) mechanisms.

The following diagram expresses the motives of present Web Content Filtration practices.

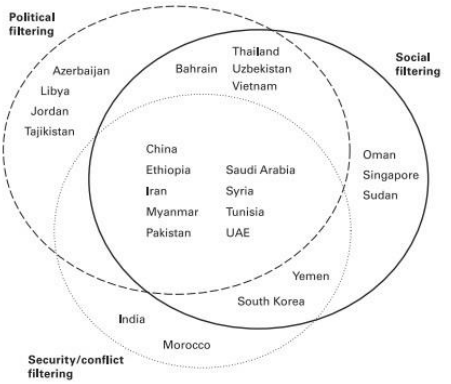

Figure 1 (Motives of Content Filtering)
(Source: Zittrain & Palfrey, 2008 p.26)

EXISTING WEB CONTENT FILTRATION (WCF) CATEGORIES

Web filter categories database are upon the web content viewing suitability of three major groups enterprises, schools, and home/families. The categories are defined to be easily manageable and patterned to industry and home user standards. All the service providers maintain their own content category data base to filter the web content.

Each category contains the list of websites or web pages that have been assigned based on their dominant web content. A website or webpage is categorized into a specific category that is likely to be blocked according to its content. When a website contains elements in different categories, web pages on the site are separately categorized. All the present available solutions regarding the web content have their own database of the websites and their categories. The following best web filtration categories (Fortinet, 2016) are given as below -

ADULT / MATURE CONTENT CATEGORY

Alcohol	Websites which legally promote or sell alcohol products and accessories
Dating	Websites that allow individuals to make contact and communicate with

	each other over the Internet, usually with the objective of developing a personal, romantic, or sexual relationship.
Gambling	Sites that cater to gambling activities such as betting, lotteries, casinos, including gaming information, instruction, and statistics.
And More	Abortion, Advocacy Organizations, Alternative Beliefs, Lingerie and Swimsuit, Marijuana, Nudity and Risqué, Other Adult Materials, Pornography, Sex Education, Sports Hunting and War Games, Tobacco, Weapons (Sales)

BANDWIDTH CONSUMING CATEGORY

File Sharing and Storage	Websites that permit users to utilize Internet servers to store personal files or for sharing, such as with photos.
Freeware and Software Downloads	Sites whose primary function is to provide freeware and software downloads. Cell phone ringtones/images/games, computer software updates for free downloads are all included in this category.
Internet Radio and TV	Websites that broadcast radio or TV communications over the Internet.
And More	Telephony, Peer-to-peer File Sharing, Streaming Media and Download

GENERAL INTEREST – BUSINESS CATEGORY

Armed Forces	Websites related to organized military and armed forces, excluding civil and extreme military organizations.
Charitable Organizations	Sites for organizations that are set up with a mission that serves a public purpose, and are philanthropic in nature. This category excludes advocacy or political organizations.
Finance and Banking	Financial Data and Services -- Sites that offer news and quotations on stocks, bonds, and other investment vehicles, investment advice, but not online trading. Includes banks, credit unions, credit cards, and insurance. Mortgage/insurance brokers apply here as opposed to Brokerage and Trading.
And More	General Organizations, Business, Government and Legal Organizations, Information Technology, Information and Computer Security, Online Meeting, Remote Access, Search Engines and Portals, Secure Websites, Web Analytics, Web Hosting, Web-based Applications

GENERAL INTEREST – PERSONAL CATEGORY

Advertising	Sites that provide advertising graphics or other ad content files, including ad servers (domain name often with 'ad.', such as ad.yahoo.com). If a site is mainly for online transactions, it is

	rated as Shopping and Auctions. Includes pay-to-surf and affiliated advertising programs.
Arts and Culture	Websites that cater to fine arts, cultural behaviours and backgrounds including conventions, artwork and paintings, music, languages, customs, etc. Also includes institutions such as museums, libraries and historic sites. Sites that promote historical, cultural heritage of certain area, but not purposely promoting travel.
Auction	Websites that feature on-line promotion or sale of general goods and services such as electronics, flowers, jewellery, music, etc, excluding real estate. Also includes on-line auction services such as eBay, Amazon, Priceline.
And More	Brokerage and Trading, Child Education, Content Servers, Digital Postcards, Domain Parking, Dynamic Content, Education, Entertainment, Folklore, Games, Global Religion, Health and Wellness, Instant Messaging, Job Search, Meaningless Content, Medicine, News and Media, Newsgroups and Message Boards, Personal Privacy, Personal Vehicles, Personal Websites and Blogs, Political Organizations, Real Estate, Reference, Restaurant and Dining, Shopping, Social Networking, Society and Lifestyles, Sports, Travel, Web Chat, Web Chat, Web-based Email

POTENTIALLY LIABLE CATEGORY

Drug Abuse	Websites that feature information on illegal drug activities including: drug promotion, preparation, cultivation, trafficking, distribution, solicitation, etc.
Child Abuse	Websites that have been verified by the Internet Watch Foundation to contain or distribute images of non-adult children that are depicted in a state of abuse. Information on the Internet Watch Foundation is available at http://www.iwf.org.uk/.
Extremist Groups	Sites that feature radical militia groups or movements with aggressive anti-government convictions or beliefs.
Hacking	Websites that depict illicit activities surrounding the unauthorized modification or access to programs, computers, equipment and websites.
And More	Illegal or Unethical, Plagiarism, Proxy Avoidance, Explicit Violence

SECURITY RISK CATEGORY

Dynamic DNS	Sites that utilize dynamic DNS services to map a Fully Qualified Domain Name (FQDN) to a specific IP address or set of addresses under the control of the site owner; these are often used in cyber attacks and botnet command & control servers.

Phishing	Counterfeit web pages that duplicate legitimate business web pages for the purpose of eliciting financial, personal or other private information from the users.
Spam URLs	Websites or webpages whose URLs are found in spam emails. These webpages often advertise sex sites, fraudulent wares, and other potentially offensive materials.
And More	Malicious Websites, Newly Observed Domain, Newly Registered Domain

COMMONLY USED TECHNIQUES FOR INTERNET FILTRATION

There are many techniques used to filter the internet content. All the techniques are designed to use at certain levels of network architecture. Internet filtering is most commonly implemented at two levels: At the ISP's level – This type of filtration is being implemented by Internet Service Providers (ISPs) at ISP level on the recommendation of the Government and at the international gateway level – This type of filtration is being implemented at the international gateway where the internet traffic of the entire ISP's routed. The uniform and unique filtration achieved at this level across the different ISP's. In the following paragraphs existing techniques for internet filtration have been discussed briefly:

1. **Packet Level Filtering** – TCP/IP Filtering works mainly at network layer to inspect the information packets including source IP address, source port, destination IP address, destination port and the protocol used. Based on the packet and rules the packet may be dropped or granted and may forward the information to network administrator. It is used at the router level as an additional security layer. To start with the network security, the packet level filtering is the way to proceed. This functionality is still the main aim of most of the non-commercial and commercial security tools. Therefore, if anything comes to internal network, it passes through the network security filters. Any type of

outgoing content will also pass through the security filters/security walls before leaving the network completely. Due to this property, the packet level filtering is also called as screening level filtering. The bigger problem with packet level filtering is that it can be hacked easily by a hacker using spoofing process.

2. **Circuit Level Filtering -** Circuit level filtering is another type of security wall which works at the session layer through providing a more general type of security. Circuit level filtering acts as relay for TCP connections. They interrupt TCP links which are being made to a host behind them and complete the handshake on behalf of that host and determine the authenticity of a requested assembly by monitoring the handshake between packets. The circuit level filter is able to hide the outside network. It also restricts the network rules to known computers. Usually, circuit level filter are economical than other protective filters. The main disadvantage of this type of filter is that every packet cannot be detected due to more general things in contemplation of filtering the packets.

3. **Application Level Filtering** – Application level filtering refers to vulnerabilities inherent in the code of a web-application itself (irrespective of the technologies in which it is implemented or the security of the web-server / back-end database on which it is built) (Scott & Sharp, 2003). Application level filtering is demanding and most secure type filtering. But it has lengthy cost of process. Because in this type of filtration, at every filtration layer new session of process starts. This type of filtering works at the application layer and is protocol specific. It is also called as proxy filtering.

4. **IP Blocking** – Internet Protocol blocking is a security filtering that stops transfer of protocols between two or more targets or servers. This type of filtration is applied to block undesirable or unwanted sites and hosts which hack, postpone or harm the network or machine. IP blocking is mainly used by the industries or companies for preventing the invasion of viruses or harmful software or data. It limits the range of websites that are accessed by the persons for official purposes. Educational institutions also use IP blocking type of filtration to protect against unauthorised access of confidential data. Ferguson and Senie (1998) observed that a rebirth of rejection of service attack aimed at various targets in the networking have produced new challenges. While blocking any IP address, all the shared hosted websites associated with that IP gets blocked by default which misleads the main objectives.

5. **DNS Tampering** – The Domain Name System (DNS) is an essential part of the Internet. The primary purpose of DNS is to resolve symbolic domain names to IP addresses (Son & Shmatikov, 2010, p.466). Each DNS resolver or authoritative server stores Resource Records in its cache or its local zone file. A Resource Record (RR) includes a label, class, type and data. The label of an RR is a symbolic domain name used when accessing an internet resource (Khan, 2015). DNS tempering is achieved by purposefully disrupting DNS servers, which resolve domain name into IP addresses. To block access to a particular website, the DNS servers are configured to return the wrong IP address. While this allows the blocking of specific domain names, it also can be easily circumvented by simple means such as accessing an IP address directly or by configuring the computer to use a different DNS server (Deibert, *et. al.*, 2008, p.14).

6. **HTTP Proxy Filtering** – HyperText Transport Protocol (HTTP) is the protocol through which Web pages travel. Another method of filtering involves using *proxy servers* or *Web proxies*, which analyse and possibly modify HTTP content as it travels between computers and the Internet. To implement HTTP filtering, Web traffic must be redirected to travel through the proxy server (Scott & Melgosa, 2013, p.56). It is an alternative way to not allow users to connect directly to website but force or encourage all users to access Web sites via a proxy server. However, as well as improving performance, an HTTP proxy can also block Web sites. The proxy decides whether requests for Web pages should be permitted, and if so, it sends the request to the Web server hosting the requested content (Murdoch & Anderson, 2008, pp.61-62).

7. **Browser Based Filtering** – Content Filtering is new subject in the area of technology. That has to study in deep. This issue appears as consequences for the variety of media and advertisement in the internet web sites that lead to unethical and misuse of World Wide Web users (Karthikeyan, 2014, p.203). In which browser based content filtering solution is the most lightweight solution to do the content filtering, and is implemented via a third party browser extension (Karthikeyan, 2014, p.204). The browser based filtration is performed through add-ons, approving a website with digital certification or enabling custom parental controls individually. Pixel based algorithms to identify the obscene content is highly used in browser based filtering.

DISCUSSION & CONCLUSION

The key feature in a web content filtration (WCF) solution is a high level of "granularity". The term "granularity" refers the degree of best possible database match of the accessed content in right category and criteria. For example, one may want to allow access to Facebook page to branding team but not provide ones employees access to facebook chat. Content filtration system works on the principle of blacklists and white lists category filters. Backlists are lists of websites/ IP/ URL's in database that contain inappropriate materials. White lists are the list of websites/IP/ URL's in database one want to allow to open.

The best filtering results can be achieved by perfect balance between the over breadth and under breadth issues. Because the primary deficiency of any web content filtration (WCF) system is that the censor must choose between two shortcomings: either the system suffers from over breadth (websites that are not meant to be filtered are filtered) or under breadth (not all web sites meant to be filtered are filtered) issues or combination of both (Zittrain & Palfrey, 2008, p.45)

In nut shell Web Content Filtration (WCF) techniques are evolving rapidly. Different countries are opting different techniques as per their need and requirement. It can also be derived that no single technique may be utilized for Web Content Filtration (WCF) of unwanted contents. So, it is recommended that efforts should be made to develop some mechanism which may utilize the hybrid combination of best optimized techniques with a high level of "granularity".

REFERENCES

1. Complete Internet Security. (2015). Retrieved September 03, 2016, from http://www.cyberoam.ca/contentfiltering.html

2. Content Control Filtering Solution. (July 2015). Retrieved July 09, 2015, from https://www.spamtitan.com/content-control-filtering-solution/
3. D. Singh, R. Sharma, and T. Singh, "Enhancement of firewall filtering techniques," *International Journal of Emerging Trends and Technology in Computer Science*, vol. 2, issue 4, pp. 258-261, 2013.
4. Deibert, R., Palfrey, J., Rohozinski, R., Zittrain, J., & Stein, J. G. (2008). *Access denied: the practice and policy of global Internet filtering*. Cambridge, MA: MIT Press.
5. Faris, R. & Villeneuve, N. (2008). Measuring global internet filtering In *Access denied: the practice and policy of global Internet filtering* (p.9). Cambridge, MA: MIT Press.
6. Ferguson, P., & Senie, D. (1998, January). *Network Ingress Filtering*. Herndon.
7. Fortinet (2016). Retrieved April 26, 2016, from https://fortiguard.com/webfilter/categories
8. Karthikeyan, V. K. T. (2014). Web Content Filtering Techniques: A Survey. *International Journal of Computer Science & Engineering Technology , 5*(3), 203-208. Retrieved from http://www.ijcset.com/docs/IJCSET14-05-03-038.pdf
9. Khan, D. (2015). *The Most Indepth Hacker's Guide*. Lulu Press, Inc.
10. Kühn, S., & Gallinat, J. (2014). Brain Structure and Functional Connectivity Associated With Pornography Consumption. JAMA Psychiatry, 71(7), 827. doi:10.1001/jamapsychiatry.2014.93
11. Murdoch, S. J., & Anderson, R. (2008). Tools and Technology of Internet Filtering. In *Access denied: the practice and policy of global Internet filtering* (pp. 57-72). Cambridge, MA: MIT Press.

12. Peddi Karthik*, S. B. (Volume 3, Issue 10, October 2013). A Face Body Detection Method for Filtering X-Rated Content . International Journal of Advanced Research in Computer Science and Software Engineering , 242-246.
13. Peterson, A. (2013, July 23). The UK Wants to Filter Porn. Heres How It Might Hurt the Internet. The Washington Post. Retrieved September 14, 2015, from http://www.highbeam.com/doc/1P234947521.html?refid=easy_hf
14. Scott, D., & Sharp, R. (2003). Specifying and enforcing application-level web security policies. *IEEE Transactions on Knowledge and Data Engineering, 15*(4), 771-783. doi:10.1109/tkde.2003.1208998
15. Scott, R., & Melgosa, A. (Feb./March 2013). Using Blocking / Filtering Technologies. *The Journal of Adventist Education,* 55-67. Retrieved from http://circle.adventist.org/files/jae/en/jae201375035513.pdf
16. Son S., Shmatikov V. (2010) The Hitchhiker's Guide to DNS Cache Poisoning. In: Jajodia S., Zhou J. (eds) Security and Privacy in Communication Networks. SecureComm 2010. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 50. Springer, Berlin, Heidelberg.
17. Web Filter Categories. (2016). Retrieved January 12, 2017, from https://fortiguard.com/webfilter/categories
18. Willard, N. (2010). Teach them to swim. *Knowledge Quest*, 39(1), 54-61.
19. Zittrain, J. & Palfrey, J. (2008). Internet Filtering: The politics and mechanism of control In *Access denied: the practice and policy of global Internet filtering* (p.45). Cambridge, MA: MIT Press.