iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 2 **Issue:** VII **Month of publication:** July 2014

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

Web content filtering for Educational & Business Organization: A Review

Navneet Kumar[1], Barkha Narang[2]

System Administrator, Jagannath International Management School,

New Delhi, Email-navneetvishwas@gmail.com

Assistant Professor, Jagannath International Management School,

New Delhi, Email-barkha.narang@jagannath.org

Abstract – In the recent years, we have witnessed an impressive growth of on-line information and resources. The self-regulating nature of Web publishing, along with the ease of making information available on the Web, has allowed that some publishers make offensive, harmful or even illegal contents present in Web sites across the world. There are many different reasons you would want to block certain content from users. One popular example is having internet access at work place; another is making sure students at schools of all type do not go to inappropriate sites that are prohibited in the school policy. According to Mr. Navneet (Researcher & web expert) and Ms. Barkha, Content filtering is the only suitable solutions to all such problems. It is the process of removing certain (illegal, not suitable contents as per requirement) content from the web before it gets to the user that requested. Actually this content filters blocking access from potentially objectionable, offensive, or irrelevant subject as per their setting.There are lots of sites that you might want to filter out. The most popular is pornography and some others are chat, email, games, personal; guns, bombs, news, advertisements etc. This paper will discuss the problem area which identified absence of web filters, solutions analysis, needs for web filtering, and related to some best tools & technique. It also shows how filtering content can be helpful to raise productivity in school, college, jobs and other business organization.

Keywords - content filtering, techniques for web filtering, browser based filtering, web management in office, content filtering in school, best tools for web filtering.

I. INTRODUCTION

Web filtering or web content filtering is prime requirement of any educational organization. The requirement of content filtering is increases day by day due to innovation in technologies. Technological innovation has brought more computing power into classrooms and business organisation, but with the rise of Chromebooks, iPads, and other devices also comes the need to protect students and employee from inappropriate content across the web, while at the same time allowing students & staff to use rich educational sites to enhance their learning, work and knowledge.

It is becoming an increasingly important topic in K-12 schools, business house and other educational platform. So, it is very necessary to protect these people from obscene or harmful online content through filtering technique. [1]

II. OBJECTIVE

Through this proposed topic "Web content filtering for Educational & Business Organization: A Review." Mr. Navneet try to focus on "importance of web filtering", "ways of Filtering", "its related technique" and best solution for filtering. Some users are unknown from filtering and its requirement. Actually filtering needed in home, business house, schools and other educational institutions after

ISSN: 2321-9653

introduction of the Child Pornography Prevention Act of 1996 (CPPA), The Children's Online Privacy Protection Act of 1998 (COPPA) and other act related to protection from harassment, pornography and other illegal activities related to web medium.

III. PROBLEMS ANALYSIS

The problem: Homes

Most websites that display adult content like pornography require no age verification whatsoever. As soon as they've gotten to grips with the controls, any young child can access online porn and commit other misuses of the internet without detection. This represents something of a growing problem for parents, who may be glad to hear that action is being taken.

After intervention from Prime Minister David Cameron, the UK government is urging internet service providers to actively encourage parents and guardians to switch on parental controls. These are purpose-built filters that analyse each page for inappropriate content before deciding whether it's suitable for the user. If not, the request is blocked and the user is sent back to a safe location.

Introducing these tools in homes would be the simple answer to preventing access to adult content if needed. It allows parents to keep control over their children's web access, without having to forego any websites they may wish to visit.

The problem: Businesses

Web filtering is critical to small and medium-sized enterprises because granting an employee unfettered access to the net spawns three key issues. Firstly, most inappropriate sites are potentially riddled with viruses or malware, which could inflict serious damage on a company network. Data theft is becoming a growing problem among businesses, with a significant chunk of cases occurring due to an unsafe website.

These pages offer mash-ups of online content; often aggregated from a selection of sites. Malware writers set up these pages to host their malicious code and it's in these dangerous corners of the web where people (as well as businesses & educational organisation) are most vulnerable to cyber attacks.

In fact, a 2011 study from Symantec reveals malware - found on unsafe websites, harmful emails and file-sharing portals - accounts for 37 per cent of all data breach cases.[2]

The problem: Educational Organisation

Educational organisation try to facilitate good infrastructure in respect to information technology with wifi enabled campus. Students also able to use social sites and other illicit materials sites at the class or study times. But without web filtering it is difficult to manage the login from improper content to the students and other related member. So web filtering is prime motto to configure filtering technique in education organisation.

IV. SOLUTION ANALYSIS: CONTENT FILTERING

The solution to this issue would be a widespread roll-out of content filtering tools. Though, businesses, educational organisation and families must have proper web content filtering tool to manage IT infrastructure in respective organisation.

Web filtering algorithms examine the page of websites and decide, algorithmically, whether it is appropriate for the setting as required. A simple way of sorting right from wrong would be to categorise results according to their suitability for a certain age, whereby any content deemed to be 18+ would be blocked.

A modern and effective web content filtering solution scans more than the domain name, though. It is able to deconstruct and analyse web traffic, making it able to accurately highlight elements of a page that's unsuitable for browsing.

V. NEEDS FOR WEB FILTERING

A web filter, in the most basic sense, is a program that is capable of blocking certain websites and protects machines from malicious activity. A filter also can track the Internet activity of individual employees or groups, documenting where they surfed and for how long. Web filtering is much, much, more than just blocking Facebook and other popular sites from employee access during work. It's about protecting your network from malicious activity, it's about recouping lost productivity, and it's about maximizing your bandwidth. Implementing a web filter in your business is among the easiest, most cost-effective things you can do to increase productivity and proactively protect your network. After lots of research & survey Mr. Navneet wants to suggest some reasons "why your company /institute /organisation need a web filter":

1. prevention from malicious sites and inappropriate content.
2. avoid data and information leakage.
3. manage your brand and image
4. preventing loss of productivity
5. preventing pornographic or illicit materials in educational or work place.

ISSN: 2321-9653

6. protection from malicious activity.
7. identify "bandwidth hogs"
8. limit online exposures (company or institution liability)
9. manage social networking in the office
10. mental breaks

1. prevention from malicious sites and inappropriate content – web filtering tools and technique allow you to prevent your work and educational environment from malicious sites and inappropriate content. this is managed with the help of softwares. its allow you to prevent access to harmful and malicious content and websites while still providing your student and employees access to good, appropriate and pertinent information. unfettered internet access can lead to inappropriate, malicious or harmful content. this can be in the form of malicious, dangerous or pornographic websites or it can be through the creation of harmful content, through social media, blog, video uploads or other web postings.

2. avoid data and information leakage - crucial data related to company or educational institute is more valuable in anything. in work environment many times it's affect the growth rate of success of the company and institutes. a mix of policy and technology is essential to combat data leakage. monitoring and filtering what your employees share online will help enforce policy and prevent data leakage confidential information; trade secrets, company processes, upcoming product releases, revenue policy, database and other organization information can leak from your organization. this data leakage can be inadvertent or deliberate; however, no matter how it happens, it will cause harm to your company and institutes. so, it must be managed in proper way.

3. manage your brand and image - social media, video sharing and other types of web sites give you the ability to promote your company and brand. these sites give you a quick and easy way to communicate with your customers, announce upcoming products, events and promotions, and promote your company, institutes and brand in innovative and exciting ways. however with these benefits come risks, including damage to your brand and image through employees & students posting negative, inappropriate or confidential content in the company's behalf. to combat this, it is imperative that internet traffic is monitored to ensure that your employees & students are not engaging in harmful practices and your organization is protected from potential threats.

4. preventing loss of productivity – these web filtering tools also helps to prevent productivity losses by preventing employees from accessing websites and applications that violate company policy or interfere with an employee's day to day responsibilities. the top managerial fears with open internet access at work are loss of productivity through cyberloafing. online shopping, gaming, social media, chatting and other personal browsing can sometimes win the work vs. play battle. students and employees more focused on doing these activities become cause of productivity loss of official work vs spending work time on personal applications.

5. preventing pornographic or illicit materials in educational or work place – to control this activity web filtering is most suitable methods for the educational & business organisation. controlling the misuse and abuse of information technology in the workplace is recognised as a vital and increasingly important component of it security. employees & students misuse of organisation computer resources can open up a whole host of problems for organisations from lost productivity, wasted computer resources and e-viral infections to serious business interruption and security breaches which in some cases lead to civil and criminal lawsuits. cyber-skiving is estimated to account for as much as 30-40% of lost worker productivity during working hours. as per world survey [3] following pornography time statistics discovered, this says:

every second - $3,075.64 is being spent on pornography

every second - 28,258 internet users are viewing pornography

every second - 372 internet users are typing adult search terms into search engines

every 39 minutes: a new pornographic video is being created in the united states

a recent survey says that 29.5% of adults who use a computer to access the internet at work visited an 'adult site' in march 2010 alone. [4] this realistic statistic is surely a wake-up call for organisations who mistakenly assume that without web filtering their organisation is safe. firewalls and anti-spam solutions will stop all illicit material entering and being distributed across the corporate network. the reality is that almost all organisations both large and small have illicit image content residing and being distributed over their networks. so what can be done to ensure that your employees & students aren't doing the same?

ISSN: 2321-9653

keeping your organisation porn-free requires a pro-active approach which combines smart human resources policies and effective detection and protection security software solutions.

6. protection from malicious activity - a web filter can help protect your network and your user's desktops against malicious activity such as viruses, malware, phishing, and spyware, by blocking access to sites known to propagate these unwanted internet nuisances. visiting certain sites can increase the possibility of exposure to damaging software including viruses, worms, spyware, malware, and others. by preventing access to troublesome sites, the number of machines infected with viruses or other malicious software drops drastically, really saving you the time and resources needed to fix the infected machine. [5]

7. identify "bandwidth hogs" - many times we get calls saying, "my internet is too slow, we need more bandwidth!" that may be true in some cases, but in most, the slow internet can be blamed on streaming audio or video among other bandwidth hogs. with a web filter, you can identify which users are using the most bandwidth, at what time, and for how long. some bandwidth hogs include: email spam, viruses, malicious intrusion, inefficient network design, social networking, hosting ftp sites, p2p sharing, and regulatory compliance etc.

8. limit online exposures (company or institution liability) – in organisation employees and students download and store copyright materials such as illegally downloaded music, movies, books, images etc. it affects organisation liability. there is some fun fact: about 70% of pornographic sites are visited during the hours of 9 a.m. to 5 p.m. web filtering tools must be needed in organisation. it allows you to block specific sites for specific users.

9. manage social networking in the office – web filtering tools allow you to manage social networking in work place effectively. being on facebook and tweeting during business hours is not really a valid argument for blocking social media sites anymore. as per recent research indicates that employees who are encouraged to tweet, facebook, socialize online are actually more productive. but it must be proper monitored by the higher authority in the organisation. web filtering and monitoring can show you what social media activity of your employees and other web users.

10. Mental Breaks – Web filters doing marvellous job to blocking unwanted sites, malicious activity such as viruses, malware, phishing, and spyware etc. The user are free from these illegal activities so they enjoy using their console with mental peace.

VI. TYPES OF FILTERING

After reading above section it is very easy to understand that "what is web filtering" and "why it is required for organisation". Now we focus on Filtering types which is mention in below. [6] It 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.

1. Browser based filters
2. E-mail filters
3. Client-side filters
4. Content-limited (or filtered) ISPs
5. Network-based filtering
6. Search-engine filters

1. Browser based filters: [7] Browser based content filtering solution is the most lightweight solution to do the content filtering, and is implemented via a third party browser extension.

2. E-mail filters: E-mail filters act on information contained in the mail body, in the mail headers such as sender and subject, and e-mail attachments to classify, accept, or reject messages.

3. Client-side filters:[8] This type of filter is installed as software on each computer where filtering is required.[9] This filter can typically be managed, disabled or uninstalled by anyone who has administrator-level privileges on the system.

4. Content-limited (or filtered) ISPs: Content-limited (or filtered) ISPs are Internet service providers that offer access to only a set portion of Internet content on an opt-in or a mandatory basis. Anyone who subscribes to this type of service is subject to restrictions. The type of filters can be used to implement government, [10] regulatory or parental control over subscribers.

5. Network-based filtering: This type of filter is implemented at the transport layer as a transparent proxy, or at the application layer as a web proxy. [11] Filtering software may include data loss prevention functionality to filter outbound as well as inbound information. All users are subject to the

ISSN: 2321-9653

access policy defined by the institution. The filtering can be customized as per user or group user requirement.

6. Search Engine Filters: Many search engines, such as Google and Alta Vista offer users the option of turning on a safety filter. When this safety filter is activated, it filters out the inappropriate links from all of the search results. If users know the actual URL of a website that features explicit or adult content, they have the ability to access that content without using a search engine. Engines like Lycos, Yahoo, and Bing offer kid-oriented versions of their engines that permit only children friendly websites. [12]

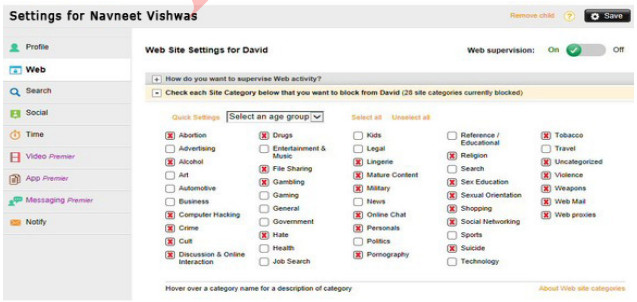
VII. WEB FILTERING TOOLS AND TECHNIQUES

There are number of solutions for schools/colleges/ institutions and other educational and business platform to address their web filtering needs. Following are some tools and techniques suggested by Mr. Navneet after lots of research work on content filtering. Some of them are:

1. Norton Family: Norton Family is a powerful parental control system with plenty of very useful features. You can set the times when your kids are allowed to use the computer, and block access to sites by type ("hate", "pornography", "shopping", "social networks" - there are 40+ categories) or URL.

You get to see which sites your kids are visiting, their web searches and more. And you can configure the program separately for each child, as long as they have their own account on your computer.

This is easy to set up, with a password-protected icon in your system tray giving access to the main settings. Email alerts warn of problems (attempts to reach blocked sites, say), and detailed reports are available online, so you can access them wherever you are. [13] Following is the screen layout of Norton software:



2. Dans Guardian (Cross Platform, Free): Dansguardian runs on Linux, FreeBSD, OpenBSD, NetBSD, Mac OS X, HP-UX, and Solaris. DansGuardian is extremely configurable and allows you to do all sorts of things, like block all images, filter ads out across your entire home network, block files from being downloaded by extension type, and control the effects of the filters, whitelists, and more based on which computer on your network is doing the accessing. You can deploy different filters for different computers based on domain, user, and source IP.

3. K9 (Windows/Mac, Free): K9 is a desktop solution; you install the software and it checks all the internet requests you make against the filters you have specified. In an effort to overcome the limitations of working from a static database, K9 introduced Dynamic Real-Time Rating to actively access the content of websites and ban them if they fall into the filter categories you've selected. It main strong points are the division of filtered content into 60+ categories which is easy to manage.

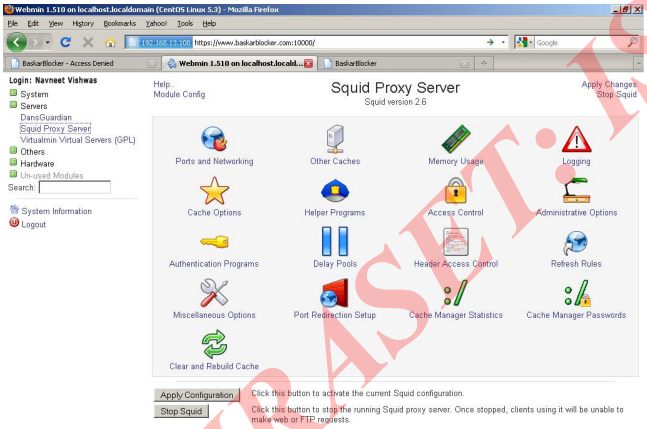
4. OpenDNS (Cross Platform, Free): OpenDNS is a perfect solution for people who either lack the time or expertise to set up and administer a full-out content-filtering server. OpenDNS replaces your current DNS server and allows you to filter every connection coming out of your house if you change the DNS settings at the router level. No matter if someone is on your main desktop or connecting into your wireless via laptop, everything will be filtered by OpenDNS.

ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

You can set custom filters to white list and black list specific sites and customize the range of filters they provide for you.

5. SquidGuard/Squid (Linux, Free): SquidGuard is natively a UNIX-environment only tool, and you can install it onto Linux, FreeBSD, and so forth. It is a standalone filtering tool you have to just connect into with a proxy and you are protected with filtering tools.



6. Some other important tools & technique: There are much software used for web filtering and it's providing a very reliable platform to use it. Some other tools are:

- Securly is a cloud-based solution that integrates with Google Apps for Education and is designed to prevent the problem of "overblocking" in schools and organisation.
- Untangle Internet Content Control provides granular visibility and control with separate controls for students, teachers, classrooms, grade levels, and sites.
- Netbox Blue has a database of over 6 Billion URLs (and growing daily) that enable schools to easily allow or block access to web sites based on pre-defined categories. Teachers, IT staff or other school officials can add to or remove specific URLs if required.
- Lightspeed Systems employs a database of educational URLs that districts can block or allow at their own discretion.
- iBoss Enterprise SWG allows school districts to deliver content based on a specific user, location, or class; it additionally allows for security with integrated APT modules and compliance driven features.

VIII. ONLINE SAFETY TIPS

Online safety is the knowledge of maximizing the user's personal safety and security risks on private information in cyberspace. As the number of internet users continues to grow worldwide, internet safety is a growing concern for both children and adults. Common concerns regarding safety on the internet include: malicious users (spam, phishing, cyberbullying, cyberstalking etc.), websites and software (malware, computer viruses, etc.) and various types of obscene or offensive content. Several crimes can be committed on the Internet such as stalking, identity theft and more. So this is very important to understand the risk cause, security tips as well as proper content filtering technique.[14] Following are the some key points which must to know everyone:

1. Information security :

Sensitive information such as personal information and identity, passwords are often associated with personal property (for example, bank accounts) and privacy and may present security concerns if leaked. Unauthorized access and usage of private information may result in consequence such as identity theft. Common causes of information security breaches include:

a. Phishing

b. Internet scams

c. Malware

2. Personal safety:

The growth of the internet gave rise to many important services accessible to anyone with a connection. One of these important services is digital communication. While this service allowed us to communicate with others through the internet, this also allowed the communication with malicious users. While malicious users often use the internet for personal gain, this may not be limited to financial/material gain. This is especially a concern to parents and children, as children are often targets of these malicious users. Common threats to personal safety include:

a. Cyberstalking

b. Cyberbullying

c. Online predation

d. Obscene/offensive content

3. Prevention/ Securing information:

For securing online medium in best manner you have to follow the below points. Such as

a. Keep shared information at a minimum: Social networks make it simple to inadvertently share details about oneself (address, phone number, birthday, etc.), so as a precaution, it is best not to input this type of information onto these websites or try to update as minimum as required.

b. Passwords: Passwords are often created to keep personal information and property secure. so it is important that passwords should be strong. Creating strong passwords is a way of keeping information secure. A strong password may contain…At least 10 characters, Both upper and lower case letters, Numbers, Symbols (if allowed), Does not contain dictionary words, Avoid using simple passwords such as: "password", "123456", "qwerty", "abc123", names, birthdates, etc.

c. PINs: PINs, like passwords, are means of keeping information secure. A PIN may consist of at least 4 digits. Birthdays, birth-years, consecutive numbers, repeating numbers, and banking PINs should not be used as PINs for your internet accounts. So, don't share pin with anyone.

d. Properly manage your Social networks. Do not accept friend requests from people you don't know.

4. Keep your system updated with Security software /antivirus.

5. Use updated Operating System with Firewalls.

6. Keeping up-to-date your all software in system.

7. Avoid visiting online scams and scams related site.

8. Avoid illegal activity and its related websites.

9. Parental must control their child at the time of using internet, and networked should be filtered by the software.

10. Don't use Public computer for any secure or login purpose.

11. Please check properly when you use Third party programs.

12. Antivirus and anti-malware programs must be updated.

13. Ad and pop-up blockers: Misleading ads and pop ups can contribute to the accidental downloading of malicious software onto your computer. Most web browsers have internal pop-up blockers. This programs/web browser plug-ins removes the ads. So, always try to use this feature.

14. Password managers: These programs help organize passwords for your internet accounts so you won't have trouble remembering them. Password Managers encrypt your password data, and in some cases, automatically fill out your user and password data onto websites.

IX. CONCLUSION

As a conclusion, research scholar & web expert Mr. Navneet want to share (from all parents and business employer) that content filtering must be installed in all education & business organization to filter all unwanted content, so that you can easily enhance the productivity of employees as well as students. You can also able to track and filter websites from the internet and manage the proper tracking record for the respective user. These are great methods and great programs so it must be put into practice. I have found that the best option is to install DansGuardian as the Content Filtering program and you can easily block required content and websites. Content filtering can help businesses keep employees on track at work and not doing non work related things on the internet. These web filtering tools can also help to protect children from offensive material. It can be also used in the homes to protect children from illicit materials on web. Dear parents and business employer be relax, because web

filtering tools make your peoples free from unwanted contents as per your expertise and requirement.

X. REFERENCES

[1] http://en.wikipedia.org/wiki/Web_filtering_for_schools

[2] http://www.thecloud.net/blog/content-filtering-why-is-it-important/

[3] http://familysafemedia.com/pornography_statistics.html#anchor6

[4] http://www.blog.pixalert.com/blogs/preventing-porn-at-work

[5] http://tek2u.com/8-reasons-your-company-needs-a-web-filter/

[6] http://en.wikipedia.org/wiki/Content-control_software

[7] "Search Results for "content filtering"". Firefox Add-Ons. Mozilla. Retrieved 10 June 2014

[8] "Client-side filters". NetSafekids. National Academy of Sciences. 2003. Retrieved 10 June 2014

[9] "Protecting Your Kids with Family Safety". Microsoft

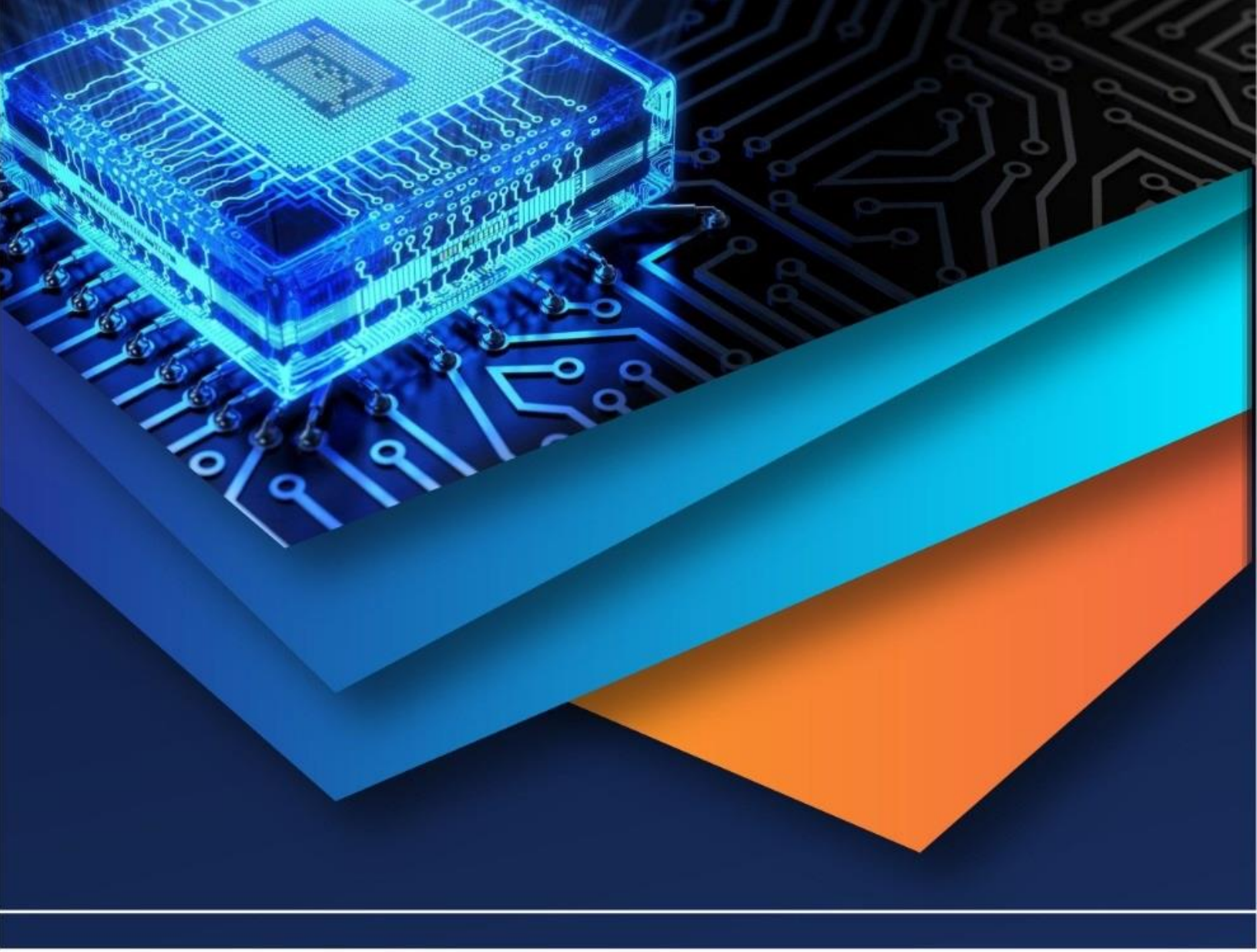
[10] Xu, Xueyang; Mao, Z. Morley; Halderman, J. Alex (5 Jan 2011). "Internet Censorship in China: Where Does the Filtering Occur?" (pdf). University of Michigan.

[11] Explicit and Transparent Proxy Deployments". Websense. 2010

[12] "Filtering". NetSafekids. National Academy of Sciences. 2003

[13] http://www.techradar.com/news/software/applications/best-free-parental-control-software-9-programs-to-keep-your-kids-safe-1140315

[14] http://en.wikipedia.org/wiki/Internet_safety



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY