iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 1 **Issue:** II **Month of publication:** September 2013

DOI:

www.ijraset.com

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

Vol. 1 Issue II, September 2013
ISSN: 2321-9653

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

A Review Paper On Firewall

Dr. Ajit singh[1], Madhu Pahal[2], Neeraj Goyat[3]

Bpsmv.ajit@gmail.com[1] , madhupahal@gmail.com[2] , sbit.cse08426@gmail.com[3]

School Of Engineering And Sciences, Bhagat Phool Singh Mahila Vishwavidyalaya Sonipat (Haryana) 131001 India

Abstract : *A firewall is a software that establishes a security perimeter whose main task is to block or restrict both incoming and outgoing information over a network. These firewalls are basically not effective and appropriate for corporate environments to maintain security of information while it supports the free exchange of views. In this paper, we study network firewall that helps the corporate environment as well as the other networks that want to exchange information over the network. A firewall protects the flow of traffic over internet and is less restrictive of outward and inward information and also provide internal user the illusion of anonymous FTP and www connectivity to internet.*

Keywords: *Firewalls, gateways, packet filter, firewall configuration, working of application gateways*

1. Introduction :

Computer networks are designed to connect two or more computers located at same or different corners in world. They are free to exchange information with any other computer. This kind of sharing is a great advantage for both individuals as well as for corporate world but as we know in today's era, most important and confidential information is also exchanged on internet so attacker can do easily attack and can find out the important information and can harm the company in any manner.

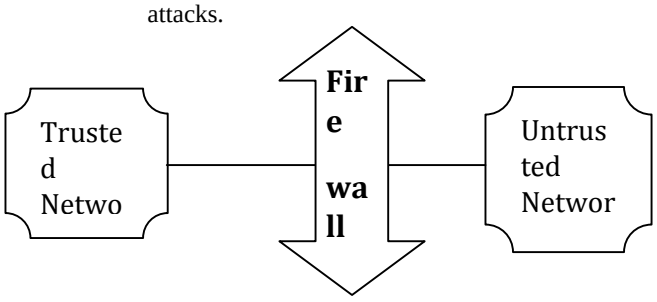
Most common type of attacks are :

- As corporation may have large amount of valuable data, leaking of which to competitors can do a great loss.
- There is also a danger from outside world such as viruses and worms, they can enter into corporate network.

To prevent our data from these dangers we must ensure some security mechanisms such that inside information remain inside and outside information remain outside and prevent outside attackers from entering in corporate network. One solution of this problem is the firewall. The main task of firewall is to regulate flow of information between computer network. It protects network by standing between network and the outside world. The data transfer in any direction must pass through the firewall.

2. Characteristics of Good Firewall :

(a) Transfer of information either from inside to outside or from outside to inside must pass through the firewall.
(b) The authorized traffic should be allowed to pass.
(c) The firewall must be strong enough to prevent from attacks.



3. Types of Firewalls :

There are different kinds of technique which may be implemented by a firewall. Some of them are as follows :

(a) Packet filter
(b) Application gateway
(c) Circuit level gateway
(d) Proxy server

3.1 Packet Filter :

- It looks at one packet at a time and then apply some set of rules to each packet and then decides to either forward the packet or discard the packet.
- The rules are based on a number of fields in the IP and TCP/UDP headers i.e. Source and

destination address, IP protocol field, TCP/UDP port number.

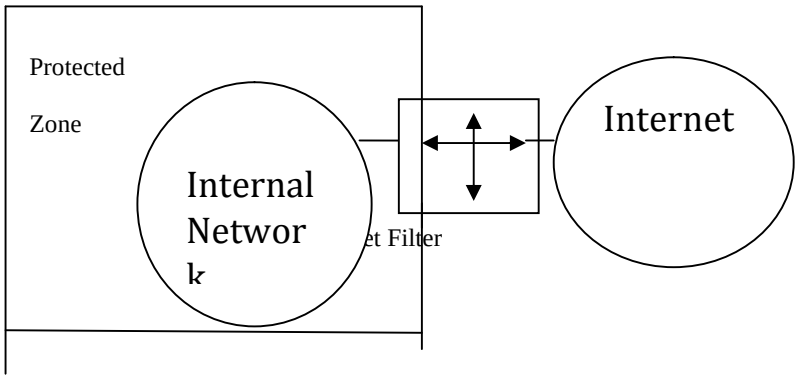


Fig. packet Filte

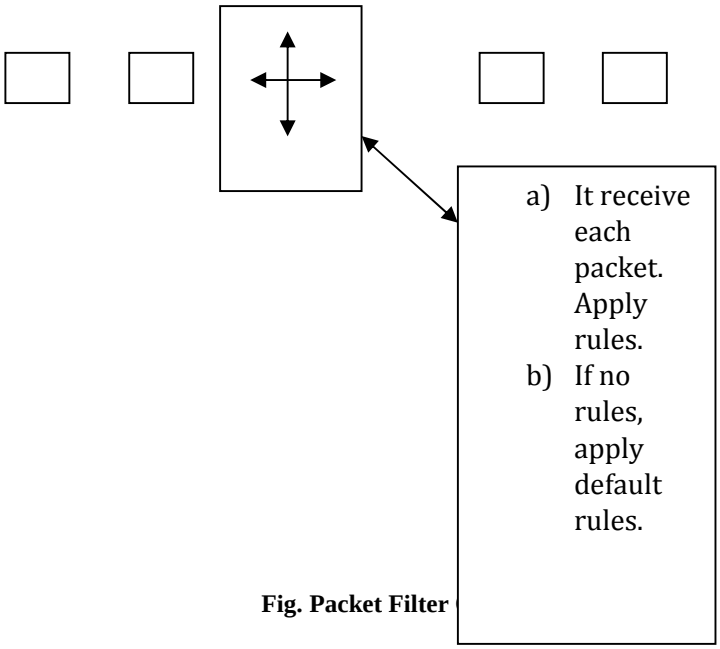


Fig. Packet Filter

Attackers can break the security with the help of following techniques:

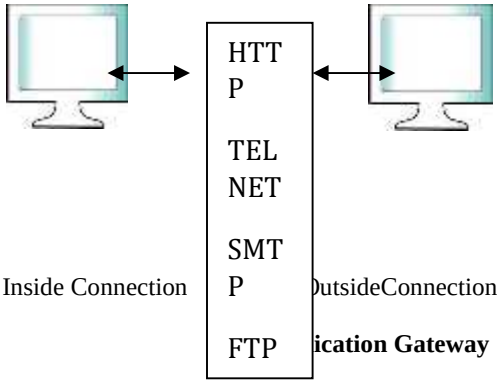
(a) **IP ADDRESS SPOOFING :** In this type of attack, attacker send a packet to internal network, by setting source
(b) Ip address equal to IP address of inside user.

Solution: we can defeat the attacker by discarding all packets which has the same source address equal to internal address.

(c) **SOURCE ROUTING ATTACKS:** Here attacker specify the route that is followed by the packet to move along the internet so that packet filter can be fooled to bypass its normal checks.
Solution: the solution of this attack is discard all packets that use this option.

Advantages:
(a) It is Simple to implement.
(b) Low hardware cost, cheap boxes can do packet filtering.
(c) Rules set are less complex.

3.2 APPLICATION GATEWAYS : In order to control risks when internal server allow connections from internet we use a technique called application gateway, also known as proxy server because it acts like a substitute and decides about flow o f information.



ication Gateway

Working of application gateways:

(1) An internal user make connection with application gateways i.e. HTTP, FTP.
(2) An application gateway ask the internal user with which it want to communicate.
(3) User then provide its id and password which is required to access services.
(4) Now on behalf of user application gateway accesses the remote host.
(5) After this application gateway acts like a proxy of actual user and delivers packet either from user to remote host or from host to end user.

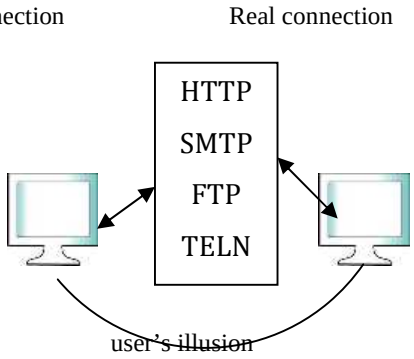


Fig. Application gateway creates an illusion

4. Firewall configuration :

A firewall is a combination of packet filters and application gateways. Depending on this, following are the configurations of firewalls.

Firewall configurations

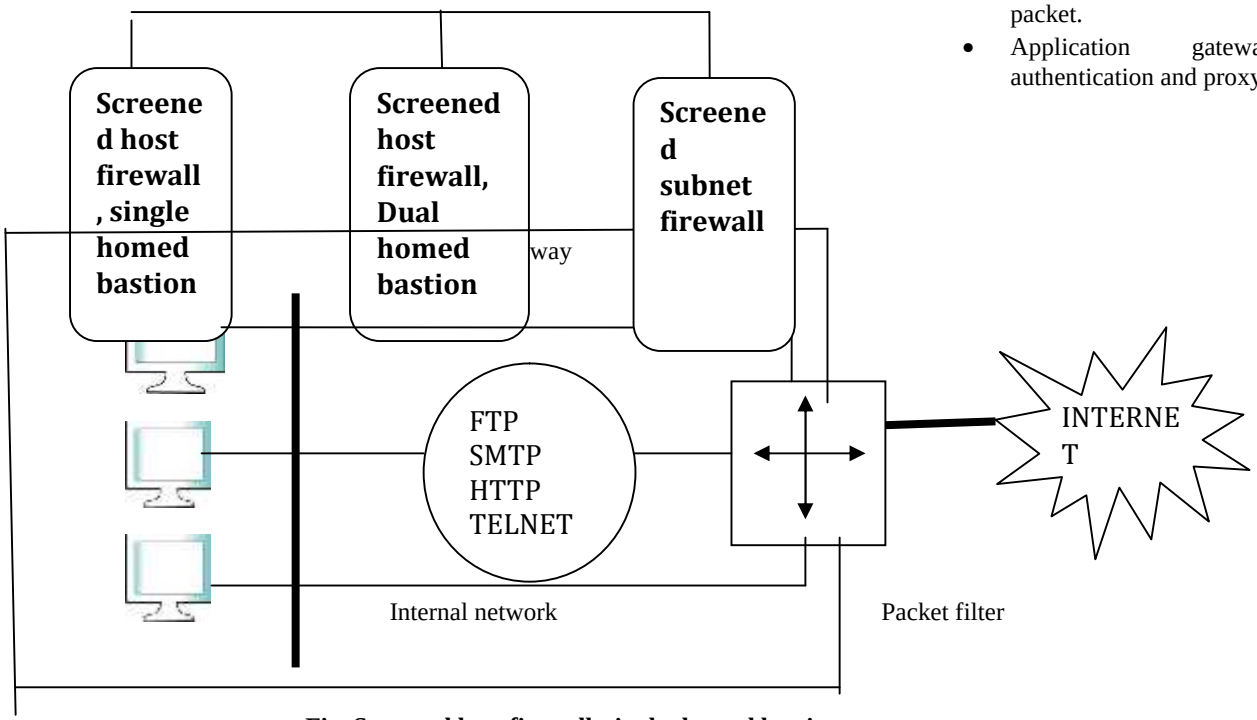


Fig. Screened host firewall, single- homed bastion

Disadvantage :

Here Internal users are connected to both application gateway as well as to packet filters therefore if packet filter is

Real connection

4.1 SCREENED HOST FIREWALL, SINGLE HOMED BASTION :

In this type of configuration a firewall consists of following parts :

(i) A packet filtering router
(ii) An application gateway

The main purpose of this type is as follows:

- Packet filter is used to ensure that incoming data is allowed only if it is destined for application gateway, by verifying the destination address field of incoming IP packet. It also perform the same task on outing data by checking the source address field of outgoing IP packet.
- Application gateway is used to perform authentication and proxy functions.

successfully attacked then the whole Internal Network is opened to the attacker.

4.2 SCREENED HOST FIREWALL, DUAL HOMED BASTION :

To overcome the disadvantage of a screened host firewall, single homed bastion configuration , another configuration is available known as screened host firewall, Dual homed bastion.

In this, direct connections between internal hosts and packet filter are avoided.

As it provide connection between packet filter and application gateway, which has separate connection with the internal hosts.

Now if the packet filter is successfully attacked. Only application gateway is visible to attacker. It will provide security to internal hosts.

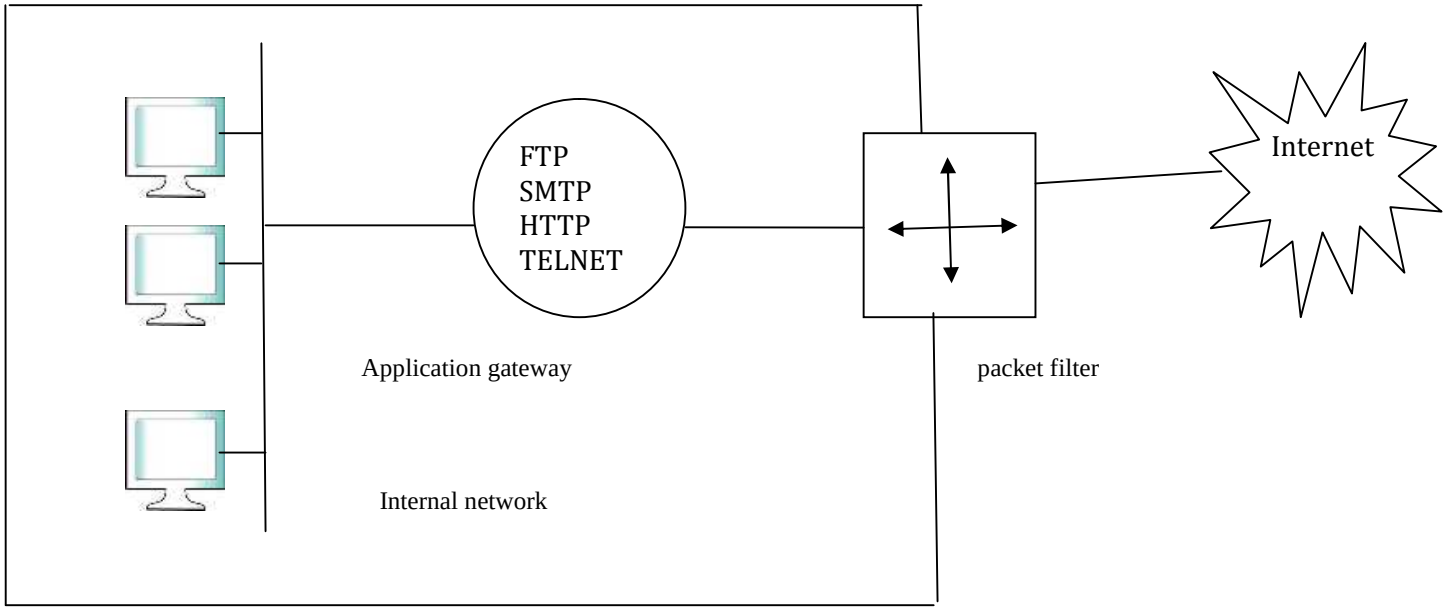


Fig. screened host firewall, dual homed bastion

4.3 SCREENED SUBNET FIREWALL:

It provides the highest security among all firewall configurations. It is improved version over all the available scheme of firewall configuration. It uses two packet filters, one between the internet and application gateway and another between the application gateway and the internal network.

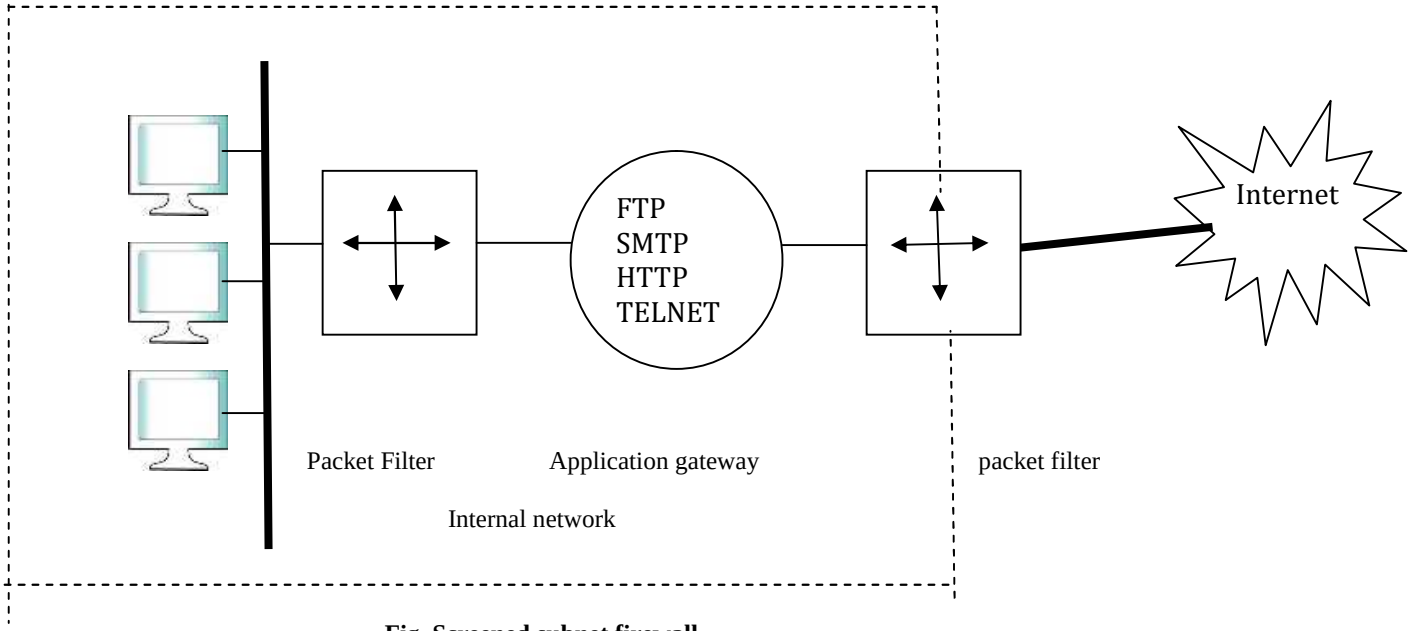


Fig. Screened subnet firewall

5. Limitations of firewall :

Till now as we discussed about all the security it provides to us and also a firewall is an extremely usefull security measure for any organization but at the same time it does not solve all the practical security problems. Its main limitations are as follows :

(i) **Virus attacks:** A firewall can not completely protect the internal network from virus threats because it can not scan every incoming packet for virus contents.

(ii) **Insider's intrusion:** A firewall is designed to protect insider from outside attacks but if an inside user attacks the internal network, the firewall cannot prevent from such type of attack.

(iii) **Direct internet traffic :** a firewall is only effective if it is the only entry exit point of a network but if there exist more than one entry exit point from where attacker can exchange information firewall can not handle such type of situations carefully.

6. Conclusion :

As we have discussed so far that firewall is very important part of computer defense against viruses, spyware, Trojans and other malwares and also between direct malicious attacks from outside and outside of network. A good firewall is the one that provide full protection of network without effecting the speed of our computer and our network access. In order to provide security, one should keep following things in mind :

- We should never install any software from suspicious sources. Always download from the respected sites available on internet.
- Use a firewall to monitor all data or information that we want to exchange over the internet.
- On every computer a firewall software must be installed else it will only take one PC to become infected and very fast it will effect the all computers available on that network.

REFERNCES:

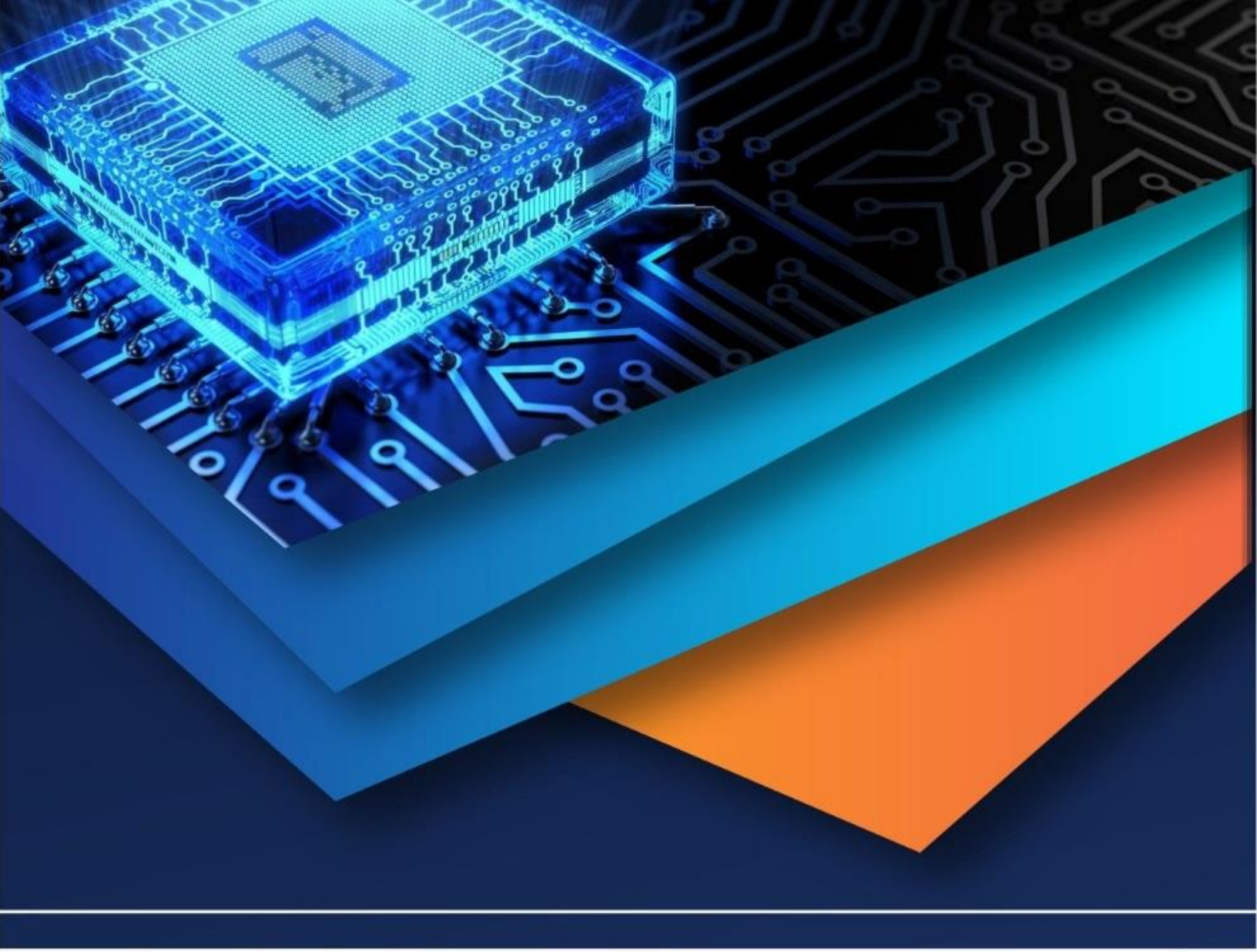
http://books.google.co.in/books

www.cs.ucdavis.edu/research

http://gregorio.stanford.edu

http://www.google.co.in/imgres?imgurl=http://computerclipartsnet

http://www.milincorporated.com/a3-firewall-internet-security.html



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY