iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** IX **Month of publication:** September 2022

DOI: https://doi.org/10.22214/ijraset.2022.46637

www.ijraset.com

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

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue IX Sep 2022- Available at www.ijraset.com

A Review of Modern Computer Networks

Tanmya Vishvakarma
[1]*Department of Information Technology, U.I.E.T, Panjab University, Punjab, India*

Abstract: ***A computer network's principal role is to facilitate the transfer of digital information between computers. An interconnected network of computer equipment is all that constitutes a computer network. Distributing tasks among different machines is frequent in a computer network. Most networks confront substantial threats from attacks on their resources. This research focuses on computer networks. It is only through the establishment of a computer network that this is made possible at all. Nodes include things like computers, cell phones, servers, and other networking gear. Computer networks enable the Internet, as well as the shared use of application and storage servers, printers, and fax machines. Through the use of computer networks, many jobs can be completed. Systems can be classified as open or closed. If you want to connect to the network, the open system is ready to go. Closed systems, on the other hand, require further authentication to connect to other networks.***
Keywords: ***Computer networks, Protocols, Types of networks, Topology, Nodes, Data transfer etc.***

I. INTRODUCTION

As computer hardware, software, and networking have improved over the last few decades, so has the amount of time people spend online. The proliferation of both computer networks and Internet communication has resulted in a rise in the number of potential security breaches within them. Today's internet is continually being attacked by new attack vectors that are being discovered on a regular basis. As a result, computer networks are becoming increasingly vulnerable to attack. Personal, societal, government, and business functioning can be disrupted and influenced by threats and vulnerabilities. Modern computer systems are increasingly reliant on network security, making it a top priority. Network security can be jeopardized by erroneous conduct and misuse by both outsiders and insiders (Anderson, 1980). Secure network communication is the ultimate goal of any network security strategy. Intruders such as Denial of Service (DoS) attacks, tampering with or deletion of data, or data loss are prevented. Authentication and access controls can be used to prevent external intrusions, but they don't help with internal ones.. Additional protection against network invasions is provided by network intrusion detection and prevention systems (NIDPS). Even if the traffic appears legitimate, it could be the result of an intrusion into your network. In Addition to the security system, NIDPS aims to identify abnormal behavior or misuse. Increasing numbers of Internet and network attacks have necessitated the need for computer network security. As the Internet becomes more susceptible to both internal and external threats, NIDPS has become an increasingly important component. Its goal is to keep computer network resources safe from abuse, misuse, and illegal access. It is a word that describes an unlawful attempt to risk a computer system's security, integrity, or availability, or to disobey its rules or policies. A network intrusion detection system (NID) keeps an eye out for suspicious activity and notifies system administrators if it detects anything that could signal a breach in security. A Network Intrusion Detection System (NIDS) is a software or hardware device that can automate NID (NIDS). As part of its intrusion detection function, the Intrusion Detection System (IDS) can stop or block potentially intrusive behavior (IDPS). In 1987, it proposed the first ID model, the Intrusion detection expert system. In order to build the ID system, this was the foundation. NIDPS has been studied extensively since then, and there are several approaches to do so. The detection and defense of network breaches has advanced tremendously, but there is still a long way to go. (Amrita, 2019)

II. NETWORK CONNECTION TYPES

A. Peer-to-peer Networks

When there are less than 10 computers engaged and no need for heightened security, peer-to-peer networks are more often used. The word peer refers to the fact that all computers are treated equally and may freely exchange information with one another. The networked computers may freely exchange data and use any common peripherals, such as printers and scanners, that are attached to any one machine. In Fig. 2, we see an illustration of how nodes in a P2P network are linked to one another.

B. Client/Server Networks

Larger networks function well as client/server systems. Files and programs used by several users on a network are often stored on a single computer, known as a server.

The server often has better specs than a typical desktop PC. The other computers, known as client PCs, have their network access managed by the server. If you're not the network administrator, you won't be able to log in to the server. The server computers are reserved for staff usage only. It's a visual representation of a client/server network's computer connections.

III. NETWORK COMPONENTS

A computer network comprises the following components

1) At least two machines are required.
2) Traditionally, computers have been linked by cables, but wireless networks are quickly gaining popularity.
3) Each computer has its own NIC, or network interface (this is called a network interface card or NIC).
4) A switch is a device used to redirect data flow from one location to another. They no longer use hubs.
5) System software for managing a network.

A. Types of Network

These are the broad classes into which the network may be partitioned.

- Local Area Network (LANS)
- Wide Area Network (WANs)
- Metropolitan Area Network (MANs)
- Wireless Networks

1) Local Area Networks

A common restriction on LANs is that they may only operate inside a certain building, floor, or other location. You're probably only allowed to use one kind of communication due to constraints (cabling). Since the infrastructure for this system only needs to be set up in a relatively limited area, the related expenses are far lower than those of a WAN. They are often used in offices and factories to connect computers and share information and hardware. In standard LANs running at 10 to 100 mbps, lag time and errors are negligible. Until recently, LANs could only reach speeds of 10–100 mbps.

2) Wide Area Network

A wide area network may cover hundreds of miles, an entire country, or even an entire continent. The number of LANs that might exist, each at a distinct place, increases. The backbone of most WANs is a dense web of cables or phone lines, each of which links a pair of routers in a far-flung location. In order for two routers to communicate without using a common cable, they will need to use a circuitous path. Modems on personal computers enable such intermediary connections. Connection between two networks represented by a wide area network (WAN).

3) Metropolitan Area Network

A Metropolitan Area Network (MAN) is similar to a LAN, but on a larger scale. It may be private and cover a cluster of adjacent corporations, or it could be public and cover a whole city. In contrast, metropolitan area networks (MANs) serve as the backbone for telecommunications providers throughout many cities. There are just one or two wires in a MAN and no switching components.

4) Wireless network

The market for portable computers like laptops and notebooks is expanding at a rapid rate. Since a connected connection to a user's workplace LAN is not an option, we must rely on wireless networks to allow users to access their data when away from the office. For example, a single router on board an airplane would keep a radio connection with another router on the ground, switching between routers as the plane moved. This setup is identical to a standard LAN, except that the connection to the outside world is a radio link rather than a cable one. (M. B. D. K. and B. D. Et.al, 2015)

IV. REVIEW OF LITERATURE

(Balasubramaniam, 2015) Computer networks are becoming more and more commonplace. In today's world, a computer network is much more than just a collection of linked gadgets. For the aim of exchanging digital information, a network of computers is created.

(Chou, 2006) According to this article, computer networks can be used to perform communication survey research. Network surveys are compared to traditional survey methods such as mail, phone, and fax, and their benefits and drawbacks are examined.
(He, 2017) Increased interest in computer network security is a direct result of the rise in popularity of these software applications. There are many aspects to take into account when it comes to network security. On the basis of real-world experience, this article provides recommendations and steps for the system design principle to help network users become more aware of network security dangers and better comprehend some network security technology.
(RANA, 2021) It's possible to communicate and share resources between two or more computers that are linked together in a network (e.g. information) It is a telecommunications network that enables computers to communicate with each other. Computer networks use network links to transfer data between connected computing devices (data connections). Packets are used to transport data. Cable or wireless media can be used to establish connections between nodes.
(Sunkari, 2021) In a computer network, or data network, computers are able to connect with one another via a telecommunications network. Computer networks use data links to transfer data from one networked device to another. Using cable or wireless media, network links can be established between nodes. One of the most well-known networks in computer technology is the Internet Computers that serve as nodes in a network are known as network nodes.
(Thota, 2013) Security and privacy concerns have increased significantly in the previous decade as the internet has advanced. Computer science students' perceptions of network security are the focus of this study. Using a questionnaire, we were able to collect data from a total of 33 pupils. Using the phenomenographic technique, we give an analysis here.
(Mali, 2018) For academic platforms that deal with computer networking-related topics, the preparation of computer networking labs is a must. An investigation on the characteristics and potential advancements of several laboratory strategies typically employed in educational institutions is presented in the following paper.
(L. Y. N. M. Et.al, 2017) Engineers and scientists in network research and industry need to be able to think critically and rigorously about their work. Student participation in the networking community and the dissemination of actual research can go hand in hand when repeating research, as we have shown.
(Kushwaha, 2014) The primary goal of computer network R&D is to develop a new protocol or algorithm, which must then be tested to ensure its efficacy and verified for practical deployment.
Deepak Gupta, 2016) Technology and services can be integrated into the house through networking in order to improve the quality of life. The term Digital Home Network refers to a type of home networking. As a result, a network of computers, televisions, appliances, wiring, security, and lighting systems was established in the home, which was connected to the Internet via a home gateway.

V. NETWORK SECURITY

Network security typically employs multiple layers of defense, including authentication and data encryption, firewall and IDS technologies, antivirus and VPN implementations, and others.

A. Routing Protocol Defects

Options for sending traffic from a certain source. When an IP packet is routed, the source routing option in the IP header is taken into account, allowing the packet's expected path to the destination host to be defined. However, this might leave a host vulnerable to attacks from other hosts if the intruders have prior knowledge of which hosts are trusted and can use this information to impersonate these hosts while attacking the system.

B. Windows Operating System Security Flaw

Overflowing ISAPI buffer Microsoft Internet Information Server (IIS) is the most popular piece of server software for Windows NT and Windows 2000. Multiple ISAPI (Internet Services Application Programming Interface) are installed at the time of IIS installation. With ISAPI, developers may employ a wide range of DLLs to improve the functionality of the IIS server. Some DLLs, including idq.dll, include a programming fault and do not perform a proper boundary check. Most notably, they let the lengthy string through unimpeded. The vulnerability allows an attacker to submit data to the DLL, trigger a buffer overflow, and seize control of the IIS server. If it is determined that the system is affected by the aforementioned flaw, the issue may be fixed by applying the most recent Microsoft updates. Concurrently, you shouldn't use the ISAPI add-on and you should verify and cancel any that do. Inspect the status of this restoration on a regular basis. The rule of least privilege states that just the smallest set of services must be actively running for the system to function correctly.

C. *Safety Defects Existing in the Internet*

The Internet relies on the TCP/IP protocol, which has security holes that contributed to the birth of the insecure Internet. TCP/IP has many advantages, including powerful capabilities, Support for a wide variety of decentralized application protocols, network connectivity technology, etc., but many security issues have arisen because of the agreement's lack of attention to safety at its inception. TCP/IP data flows that rely on clear text transmission, such as those that employ HTTP, FTP, Telnet, or user accounts and passwords, are particularly vulnerable to online hacking, manipulation, and forging because of the exposed nature of the sent data. TCP/IP uses an IP address to identify each network node, but an attacker may fake off the system by changing their own IP address to seem like a legitimate one within a limited area. This technique is known as Source Address Spoofing.

Source Routing Spoofing is a kind of spoofing in which an attacker forges a connection by forging the IP packet's source address.

Attacks on the routing information protocol (RIP). Because the node that receives the information does not verify the authenticity of the information, an attacker could issue incorrect routing information online, take advantage of a router or host ICMG redirection information, and execute a network attack. The Routing Information Protocol (RIP) is used to publish dynamic routing information in local area networks. Current firewall systems are only able to effectively detect the login user identity through the IP address and protocol port.

VI. NETWORK SECURITY STRATEGIES

A safe network is essential to survival, and only a safe network can reach its full potential. Network security technologies, such as authentication, encryption, a firewall, and intrusion detection, are always developing to keep up with people's growing use of networks.

A. *VPN Technology*

A virtual private network (VPN) is a technology that uses the internet's underlying network to establish a private network, enabling users to send and receive data securely across a public network (thus the term virtual private network). Routing filtering technology and tunnel technology are two typical approaches to building a Virtual Private Network (VPN). At present, a virtual private network's security relies on four basic technologies: tunnelling, encryption, key management, and user identity authentication tools and infrastructure. Popular VPN tunneling protocols like Stage Networking Standard (PPTP), Layer 2 Tunneling Proper procedure (L2TP), and Internet Backbone Security (IPsec) should accommodate a variety of security service levels of intensity, including those for identifying and authenticating their sources, intercepting their data, and so on. There are a few different ways to categorize VPNs based on how users access them (dial-up vs. shuttle VPN, for example), based on the tunnel protocol used, and based on who is paying for the service (client vs. server sponsorship).

B. *Intrusion Detection Technology*

Intrusion detection technology is a hot topic in network security studies because it is an active safety measure that can spot and stop both internal and external network invasions as they happen. As time goes on, the field of intrusion detection is developing in three distinct directions: distributed intrusion detection, intelligent intrusion detection, and all-in-one security defense solutions. An Intrusion Detection System (IDS) is a collection of software and hardware used for this purpose, and while it serves numerous purposes, chief among them is detection. In addition, it can assess and recover from network intrusion events according to the level of harm they posed, discover intrusion archives that can be used as a legal basis, and block, close, or otherwise deal with potential intrusions.

Technically, there are two kinds of invasive monitoring detection model

1) If it is feasible to specify what constitutes normal behavior in an anomaly detection model, then any variation from that behavior is an intrusion. Despite a low non-response rate, the test model had a large false positive rate.
2) The feature detection model will be helpful if it is possible to list all potentially harmful actions and if each action that matches the list triggers an alarm. The purpose of this model is to capture packets using a mode matching technique and the features of the library for comprehensive comparison, to determine if an attack or hostile invasion has happened, with a low rate of false positives but larger non-response rates. The shortcomings of this testing method become more clear as network technology advances. The high threshold for data matching limits our ability to detect even the most basic forms of attack..

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue IX Sep 2022- Available at www.ijraset.com

C. Data Encryption Technology

Encryption may be used to protect data in transit over the Internet, as well as login credentials and other private data. Link encryption, endpoint encryption, and node encryption are the three most common kinds of encryption; the first protects data as it travels from one network node to another, the second encrypts data as it travels from one user's device to another's, and the third encrypts data as it travels from one node to another's.

Multiple encryption algorithms are actually used in the process of encrypting data, all with the intention of delivering the highest level of security and protection at the lowest feasible cost in terms of processing time. Only encryption offers sufficient security for safeguarding private information. How are public-key cipher algorithms distinct from its typical cryptographic algorithm counterparts, since both need a classification and key? With a regular password, the sender and the receiver have access to the same encryption key. In public-key cryptography, both the sender's key and the receiver's key are the same, and it is very difficult, if not impossible, to determine which is which. Common practices include encrypting data using DES or IDEA and then passing the session key along with an RSA public key, for example.

D. Authentication Technology

Aside from being crucial to the security of any and all open-source information systems, certification also serves two other vital functions The purpose of sender authentication is twofold (1) to guarantee the sender is legitimate, and (2) to check the data's integrity and make sure it hasn't been changed with during transmission, replay, delay, etc. Message authentication, identity authentication, and digital signature are the primary certification methods that are relevant to this discussion. The communication parties concerned with avoiding third-party harm and hiding their tracks have found a solution in message and identity authentication. It is impossible for someone else to transmit or receive information using my identity, and it is also impossible for me to deny having sent or received information using my identity afterwards.

Whereas the router has its own power cord, the dish only needs the one connecting cable. Starlink's Wi-Fi router is the hub of your home network, where your lightning-fast internet connection originates and throughout which all other devices on your network connect.

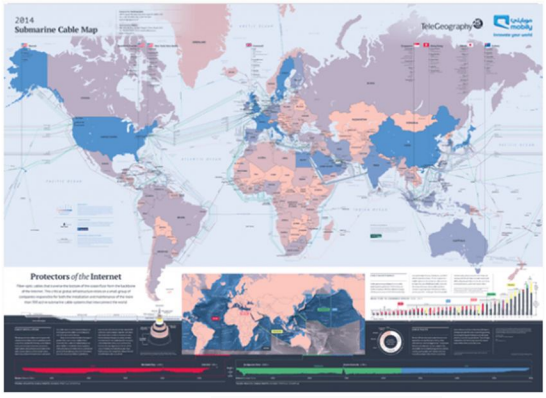


Figure-1: Submarine cable map

Submarine cables are decidedly uncool. In spite of the fact that they are not as eye-catching as satellites, the massive network of fiber optic cables that spans the globe is the one responsible for the majority of the laborious work that is required to keep our information moving from one location to another. There are approximately 420 active submarine cables that collectively reach more than 1.1 million kilometers (over 700,000 miles) around the planet at this time. The network is heavily concentrated in major cities with thriving information economies, such as Singapore and New York, but cables can link to virtually any location.

VII. STAR LINK

India is one of the world's most promising consumer marketplaces because of the rising demand for high-speed internet caused by the ongoing pandemic scenario [COVID-19]. In light of the current situation, in which all education and businesses are going online for their day-to-day operations, and there is a pressing need for high speed internet connectivity, Starlink has made an introductory offer to customers all over the world, including those in India, to provide them with high speed internet from the sky via satellite. The timing of Starlink's offer couldn't be better, as high-speed internet is in extremely high demand right now.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue IX Sep 2022- Available at www.ijraset.com

There is already widespread internet usage, but improvements in connection speed could prove pivotal. The need has arisen, and the answer has fallen from the sky. In the meantime, other ISPs exist, including Reliance JIO, Vodafone-Idea, Airtel, and others that focus on FTTH, mobile Internet, and satellite Internet.

A. Elon Musk

Elon Musk's initial offer for his satellite internet service may appeal to people who need high speed internet and users who are not accessing the internet services adequately. Those who are having trouble connecting to the internet could also benefit from this deal. SpaceX, owned by tech tycoon Elon Musk, recently announced that it will be developing a comparable service named Starlink. Using satellite technology, this service would provide Internet connectivity wherever on Earth. The current research is limited to the geographical limitation of India; but, the results thus far have been encouraging, and people will soon have access to the information they require to take their businesses forward effectively despite the pandemic and lockdown. In the midst of a pandemic and lockdown, people will be able to obtain the resources they need to advance their businesses. In light of India's enormous consumer market, it's possible that Elon Musk may find a lot of success there.

B. How Does it Work ?

When Starlink is fully operational, everyone on Earth will be able to access the web from anywhere on the globe. Starlink is Elon Musk's idea to deploy thousands of miniature satellites into geostationary orbit. All of these satellites will be placed in the exact same orbit. To send information to Earth at the speed of light.

With passing years, Earth's orbit becomes more and more congested. This can be attributed in part to Starlink's quick growth; the company has launched hundreds of satellites into low Earth orbit (LEO) since 2019.

Satellite owner/ Operator	No. of Satellites	Country of Operator/owner
SpaceX	358	USA
Planet Labs, Inc.	246	USA
Iridium communications, Inc.	89	USA
Civil	78	USA
OneWeb satellites	74	United Kingdom
SES S.A.	51	Luxembourg
Intelsat S.A.	36	USA
ORBCOMM Inc.	35	USA
DoD/US Air Force	33	USA
EUTELSAT Americas	33	Multinational

Table-1: Operational satellites for different countries

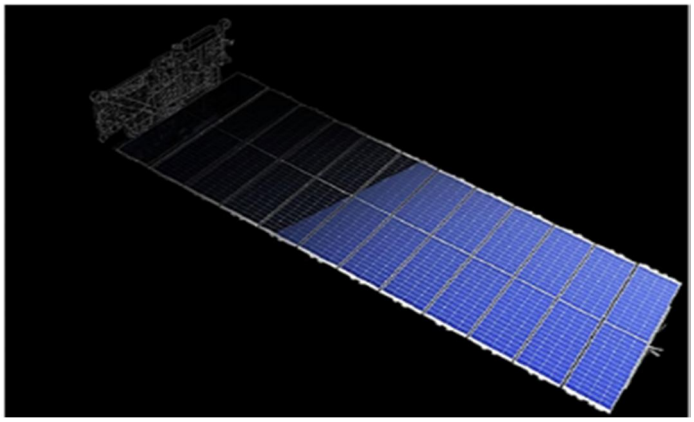


Figure 2- Showing an Image of Starlink Satellite in space

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue IX Sep 2022- Available at www.ijraset.com

Figure -3:Showing launching of Starlink Satellite in space

Figure-4: Showing the Image of Tracker Antenna to track the signals from Starlink Satellite

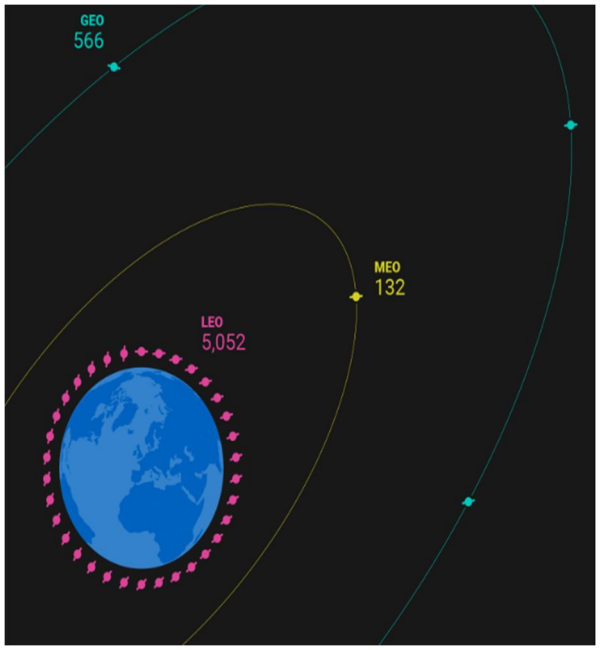


Figure-4: Satellites are shown larger than their actual proportions

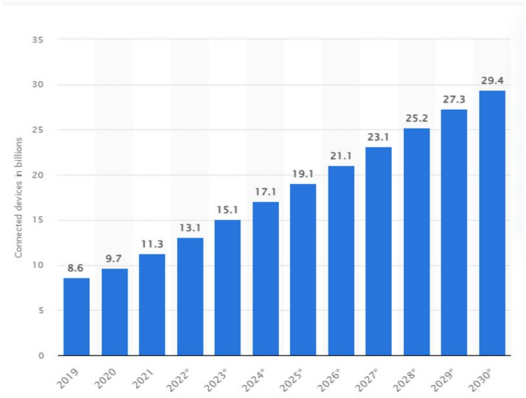


Chart-1:Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2030

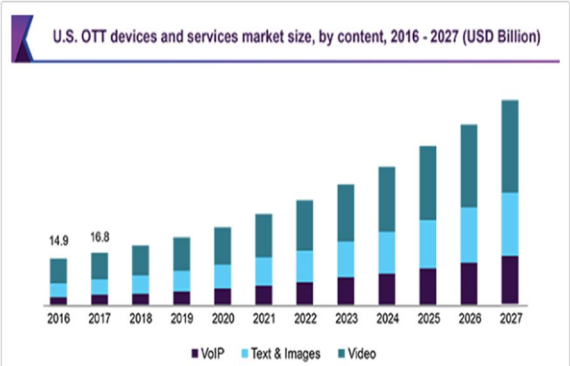


Chart-2 :OTT devices and services by market size

Satellite owner/ Operator	No. of Satellites	percentage of Operational Satellites
Commercial	1440	54%
Government	436	16%
Military	339	13%
Civil	133	5%
Combination (other)	112	4%
Combination (commercial)	206	8%
Defunct Satellites	3200	

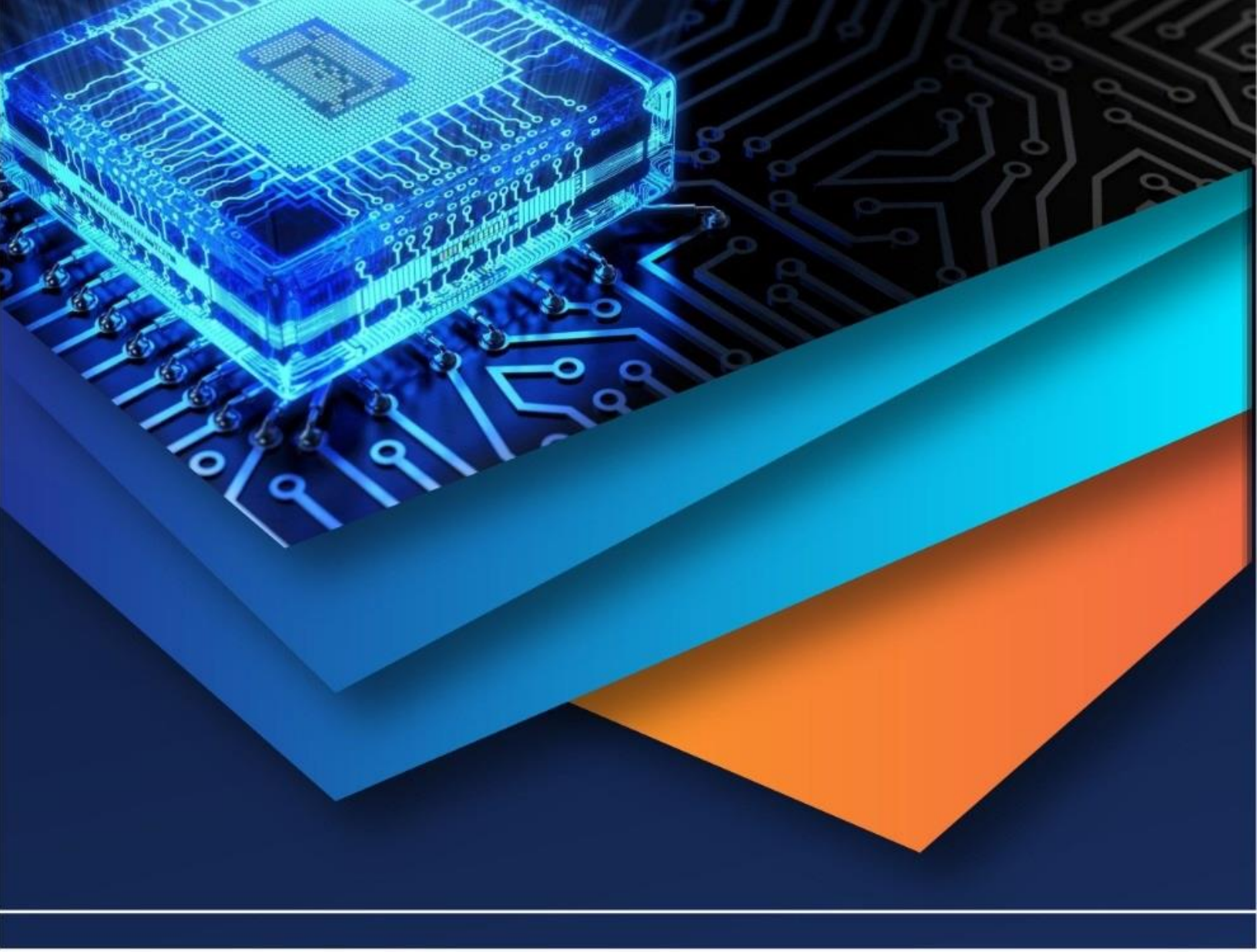
Table-2: 54% of operational satellites are for commercial use

VIII. CONCLUSIONS

When it comes to keeping up with the ever-evolving threat landscape, those responsible for network security must always be learning and evolving. To keep sensitive information safe, we cannot rely on a single line of defense; instead, we must use many levels of defense, each with its own advantages and synergies. The author has researched in the field of network security and produced an account of the most common threats to network security, a rundown of the ways in which network security strategy has been applied, and an outline of the basic principles underlying the creation of network security defenses. In the approaching years, this issue should be lessening as technology breakthroughs spread across society.

REFERENCES

[1] Amrita. (2019). An intelligent ensemble based system for detecting and combating intrusion in computer network. *SHODHGANGA*. https//shodhganga.inflibnet.ac.in/handle/10603/339209
[2] Balasubramaniam, D. (2015). Computer Networking A Survey. *Research Gate*. https//www.researchgate.net/publication/317101504_Computer_Networking_A_Survey
[3] Chou, C. (2006). Computer networks in communication survey research. *IEEE Xplore*. https//ieeexplore.ieee.org/document/649555
[4] Deepak Gupta, S. M. (2016). SMART HOME NETWORKING. *INTERNATIONAL JOURNAL OF CONVERGING TECHNOLOGIES & MANAGEMENT*, *02*(02). https//www.gyanvihar.org/journals/index.php/2018/12/05/smart-home-networking/
[5] Et.al, L. Y. N. M. (2017). Learning Networking by Reproducing Research Results. *ACM SIGCOMM Computer Communication Review*, *47*(02). https//ccronline.sigcomm.org/wp-content/uploads/2017/05/acmdl17-97.pdf
[6] Et.al, M. B. D. K. and B. D. (2015). Computer Networking A Survey. *Research Gate*, *02*(05). https//www.researchgate.net/publication/317101504_Computer_Networking_A_Survey
[7] He, J. (2017). The Research of Computer Network Security and Protection Strategy. *AIP Conference Proceedings 1*. https//aip.scitation.org/doi/pdf/10.1063/1.4982538
[8] Kushwaha, V. (2014). A Study of Research Tools and Techniques in Network Congestion Control. *International Journal of Engineering Research & Technology (IJERT)*. https//www.ijert.org/research/a-study-of-research-tools-and-techniques-in-network-congestion-control-IJERTV3IS20049.pdf
[9] Mali, M. S. R. (2018). Methodologies to the Strategy of Computer Networking Research laboratory. *IJIRT*, *05*(03). https//www.irjet.net/archives/V5/i3/IRJET-V5I3313.pdf
[10] RANA, S. (2021). Computer Network. *IJIRT*. https//www.ijirt.org/Article?manuscript=142642
[11] Sunkari, S. (2021). A Brief Study on Data Communication and Computer Networks. *SSRN*. https//papers.ssrn.com/sol3/papers.cfm?abstract_id=3904826
[12] Thota, V. C. (2013). Computer Science Students' Perception of Computer Network Security. *DIVA*. https//www.diva-portal.org/smash/get/diva2614625/FULLTEXT01.pdf



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY