



IJIRCCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 4, April 2022

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.165



9940 572 462



6381 907 438



ijircce@gmail.com



www.ijircce.com

A Study on the Different Types of Security Attacks

B. Ramesh

Associate Professor, SRS Engineering College, India

ABSTRACT: In order to enforce high protection levels against malicious attack, a number of software tools have been currently developed. Intrusion Detection System has recently become a heated research topic due to its capability of detecting and preventing the attacks from malicious network users. A pattern matching IDS for network security has been proposed in this paper. Many network security applications rely on pattern matching to extract the threat from network traffic. The increase in network speed and traffic may make existing algorithms to become a performance bottleneck.

KEYWORDS: attacks, DOS, security

I. NETWORK SECURITY ATTACKS

To compromise between opening a system and lock it down so that no one can use it, is called security and any action that compromises the security is called a security attack. A system which is providing the services required by the user accurately and preventing the illegal use of system resources is called a secure system.

Attacks can be categorized into following basic categories.

- **Interruption:** For using the data or resources it is necessary that they are available 24/7 for the authorized parties, when and where they need it. Attack on the availability of data is called interruption. Availability can be affected by intentional or un-intentional acts. Examples of un-intentional acts are, accidentally system crash, deletion and overwriting of data and some time due to non human factors like flood, fires and earthquakes. Whereas destruction of infrastructure due to wars, strikes and some attacks by hackers that crashes the system, such as denial of service (DOS) and distributed denial of service (DDOS) attacks are the examples of intentional acts. Protection against availability attacks includes backup and restoration.
- **Interception:** The core concept is that the data should be hiding from unauthorized users. If some one who is unauthorized to see private data, can see or copy the data that can further be used in intensive active attack. Such an attack is known as attack on confidentiality. Data integrity can be accomplished by strong authentication and strict access controls, because some time authorized users may also a threat for confidentiality of data. They can obtain another person's credentials.
- **Modification:** Integrity of data deals with prevention of intentional or unintentional modification of data. Attack on integrity of data called modification. Different algorithms used for validation of data that can resist in alteration of data. Protection of data from modification is foremost concern than detection. Integrity of data could maintain at many layers of OSI system model.
- **Fabrication:** Attack on authenticity called fabrication. Authenticity means that message is coming form the apparent source. It assures that you are who you say you are. User name and password is the most common way to achieve authentication, some other techniques are like smart cards and digital certificates.

Above mentioned attacks are shown in figure 1

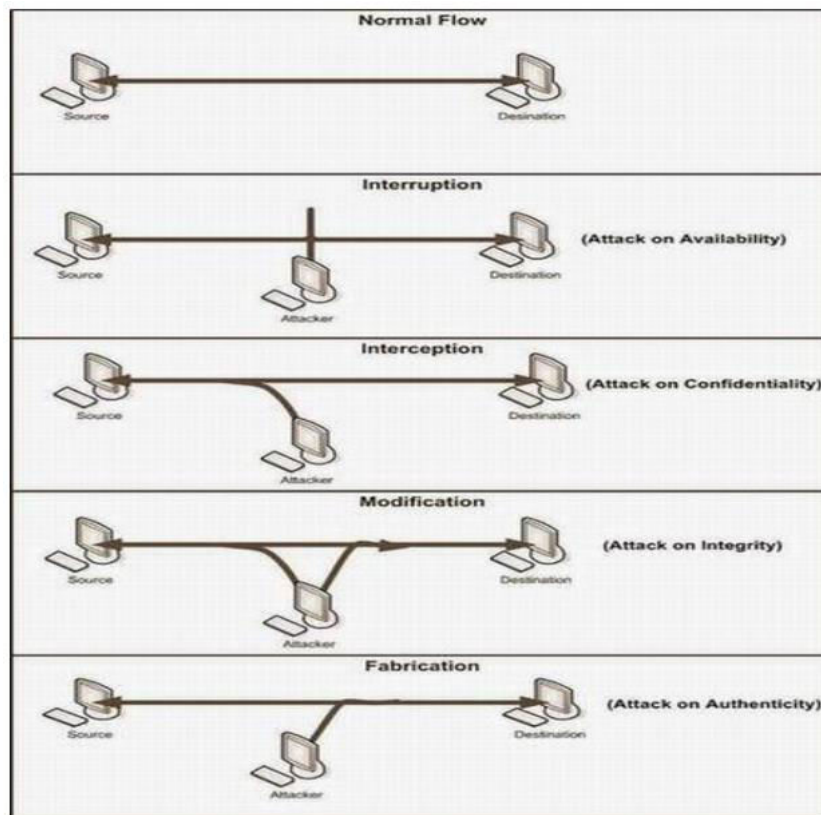


Figure 1. Basic types of Security Attacks

On the basis of these four attacks we can further classify security attacks as passive attacks and active attacks. Passive attacks are only involved in monitoring of the information (interception). The goal of this attack is to obtain transmitted information. Two types of passive attacks are “release of message content” and “traffic analysis”. Passive attacks are hard to detect because they do not involve in any alteration. Different encryption schemes are used to prevent against these attacks.

Active attacks are involved in modification of data (interception, modification, fabrication) or creation of false data. These attacks are further subdivided into four categories, “masquerade”, “replay”, “modification of data” and “denial of service”. When an unauthorized user tries to pretend as an authorized user is called masquerade attack. Replay attacks involved in capturing the message between two communication parties and replay it to one or more parties. Bring the network down to its knees by flooding the useless traffic in network is called denial of service attack.

Figure 2 and 3 are showing passive and active attacks.

Attacks are either active or passive. Information which hackers obtained from a passive attack is used in more aggressive active attack. We will discuss in detail some common types of network attacks.

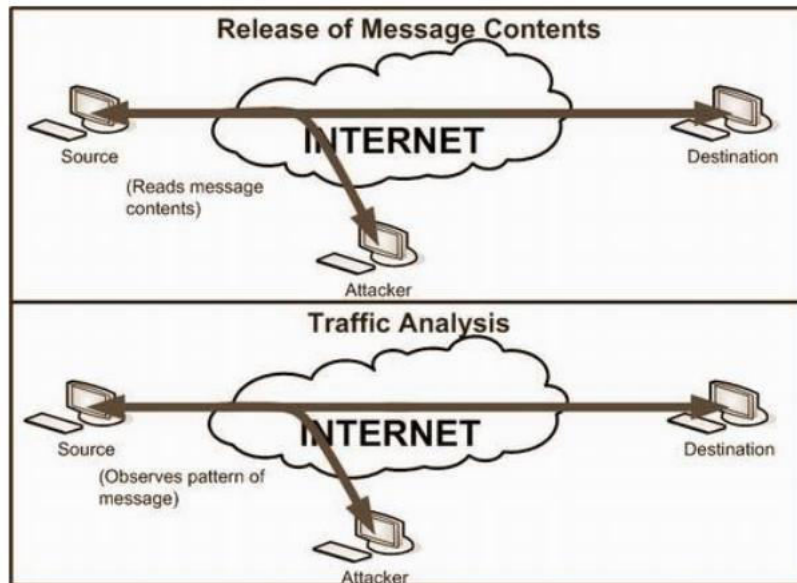


Figure 2: Passive Attacks

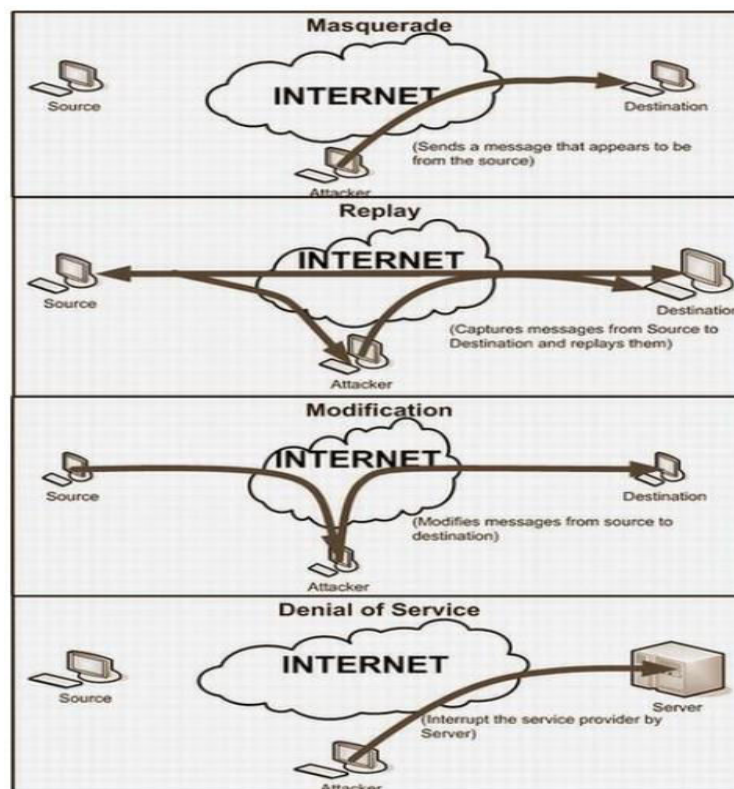


Figure 3: Active Attacks

Reconnaissance Attacks

Gathering information against a targeted host or network is called reconnaissance attack. Attacker analyze the target host and try to discover the details like alive IP addresses, open ports of the network, failour of operating system, and types of services and protocols running on the network. Reconnaissance attacks are common they are not so much

dangerous because they are not involved in any kind of alteration or destruction of data but on the other hand they show the vulnerabilities in the network. They allow hackers to see which ways are open to access the system and provide enough information to them which they can further use in denial of service (DOS) attacks.

Some basic reconnaissance attacks are: Packet Sniffers

Port scan and ping sweep

Internet information queries

Packet Sniffers

As we discussed earlier that data which is traveling across a network is not in a continuous stream of data in fact it is in the form of packets. As we know that we cannot see the atom through naked eye we need a device like electronic microscope same is in the case of analyzing the data packet. Packet sniffer is a tool or device that can be used for capturing the packet at data link layer. Packet sniffer is not only a hacker's tool but it can be used both by the hacker for eavesdropping and by the administrators for network monitoring and troubleshooting. Tcpdump, windump, Wireshark (Ethereal) and Dsniff are examples of different sniffing tools.

Sniffing can be of two types depending on the network.

Passive Sniffing Active Sniffing

Passive Sniffing

Passive sniffing is used in hubbed networks. The drawback of using the hub in network was that, the hub broadcast a packet to each and every machine on the network. There is a filter on each machine which decides whether to accept or discard the packet. If a packet addresses to a specific machine then filter decide to accept it otherwise discard the packet. Sniffer disables this filter so that network traffic can be analyzed. This stage is called "promiscuous mode". Hence if „Bob“ on computer A sends a message to „John“ on computer B, a sniffer on computer C can easily capture the contents of that message even without knowing Bob and John. Passive sniffing is hard to detect because it generates no traffic on network. This type of sniffing worked well when hubs were used. To avoid passive sniffing most of the networks nowadays are using switches instead of hubs.

Figure 4 is showing passive sniffing.

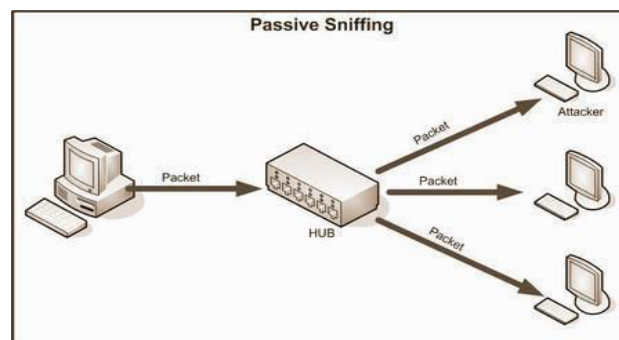


Figure 4: Passive Sniffing

Active Sniffing

Active sniffing is performed on switched network. A switch limits the sniffer to see the broadcast packets. Switch worked as a central entity, rather than broadcasting it simply get message from source machine and send it directly to the addressed machine. So if computer C is in promiscuous mode it cannot see the message from Bob to John.

It does not mean that sniffing is not possible in switched networks. Media Access Control (MAC) flooding and poisoning of the Address Resolution Protocol table (ARP) are the ways to hack a switched network.

MAC Flooding Spoofed ARP Messages

Switches worked on the basis of MAC addresses. They maintain an address resolution protocol (ARP) table in a special type of memory called Content Addressable Memory (CAM). ARP table has all the information that which IP address is mapped to which MAC address.

The act of overloading the CAM is known as MAC flooding. Low memory in older or cheaper switches can cause MAC flooding. Flooding of too many MAC addresses can fill up the memory so that switch cannot hold more entries. At this stage switch goes to a failopen mode and cannot perform IP to MAC mappings, starts behaving like a hub and starts transmitting the data to all machines. In MAC flooding attacker inject large amount of traffic which may draw attention towards hacker. This traffic can be detected by any sniffer detecting software.

The other technique to hack a switch network is called ARP poisoning. A review of ARP is that it is almost similar to Domain Name Server (DNS). DNS resolves domain names to IP addresses while ARP resolves IP addresses to MAC addresses. Hacker fools the switch and tries to pretend the destination machine.

He tries to convince the switch that the IP address of another trusted host belongs to him. A very interesting thing is that it is also up to the attacker that which IP address he wants to redirect to his system, spoofing the system, spoofing the default gateways will redirect all host messages towards the attacker. However for this, attacker has to poison host ARP table. The other way is to poison the ARP cache of a central entity of the network, hacker express that the IP address of switch (or router) is mapped with his MAC address. Through this way all the traffic first goes towards the attacker then the router. Active sniffing is shown below in figure 5

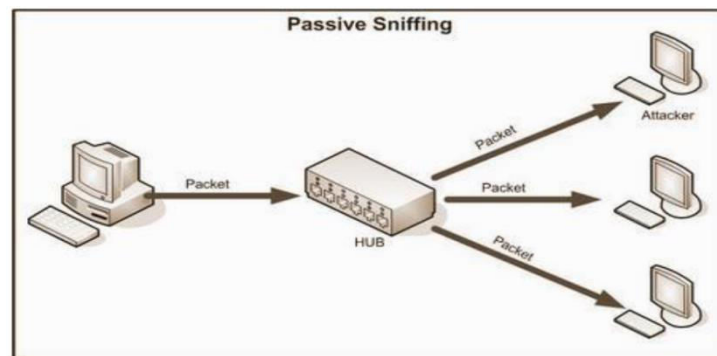


Figure 5: Active Sniffing

II. TYPES OF PASSWORD ATTACK

Strong, long and encrypted passwords does not mean that they are unbreakable; it's just a matter of time. Few years earlier the time to break a password was may be 100 days but now it's just a matter of two or three weeks.

Different types of password cracking attacks are:

- Dictionary Attack
- Brute force attack
- Hybrid Attack

	Dictionary Attack	Brute force Attack	Hybrid Attack
Speed of the Attack	Fast	Slow	Medium
Passwords Cracked	Finds only words	Finds every password(A-Z, 0-9, special characters)	Finds only the password that have a dictionary word as the base

Table 1 Types of password Attacks

Different password cracking programs are available like L0phtcrack, NTSweep, NTCrack, Crack, John he Ripper etc.

Trust Exploitation

When a hacker attacks on a computer which is outside a firewall and that computer has a trust relationship with another computer which is inside the firewall, the hacker can exploit this trust relationship. We can mitigate this type of attack by using private VLANs between switches or by limiting the trust relationship between systems which are inside and outside the firewall. We can also reduce this by eliminating useless trust relations between different servers. For example if our AAA (Authentication, Authorization, and Accounting) server is inside the DMZ (Demilitarized Zone), there is no need to have a relation of AAA server with the file server. Figure 6 explaining trust exploitation phenomena.

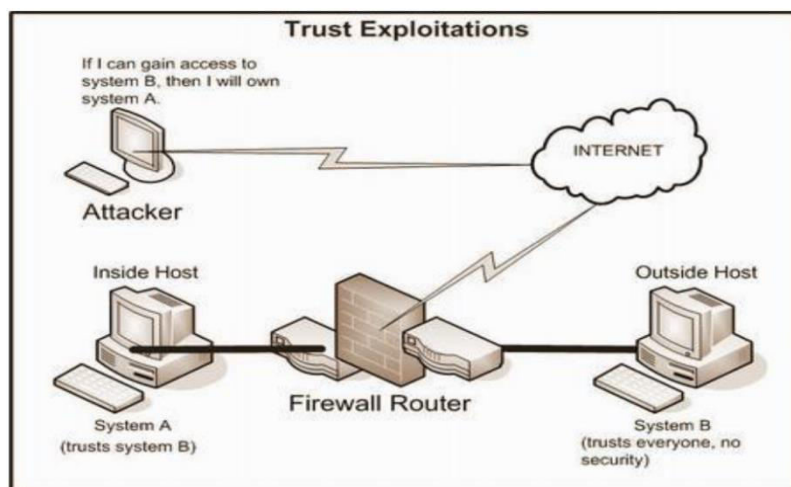


Figure 6: Trust Exploitation Attack

Port Redirection

It is another type of trust exploitation attack in which a hacker bypasses the security mechanism. Consider the below network in which hacker on the outside have the ability to access the public computer but not the computers which are in DMZ or which are inside the firewall. If public computer compromised by the hacker then hacker installs a software that can redirect the traffic towards the hacker, directly to the inside computers. In this way hacker makes a tunnel for communication and bypasses the security firewall. See figure 7 for port redirection attack.

Man-in-the-Middle Attack

When hackers succeed to intrude himself between two communication parties this type of attack is called MITM (Man-in-the-Middle) attack. In this way hacker can intercept data between source and destination host, can modify data and retransmit it to the destination host and can also inject any type of false data. MITM attacks can affect on availability, confidentiality, integrity and authenticity of data. Strong cryptography can mitigate this type of attack. SSL, SSH and use of IPSec also gives end to end security (entire connection is encrypted).

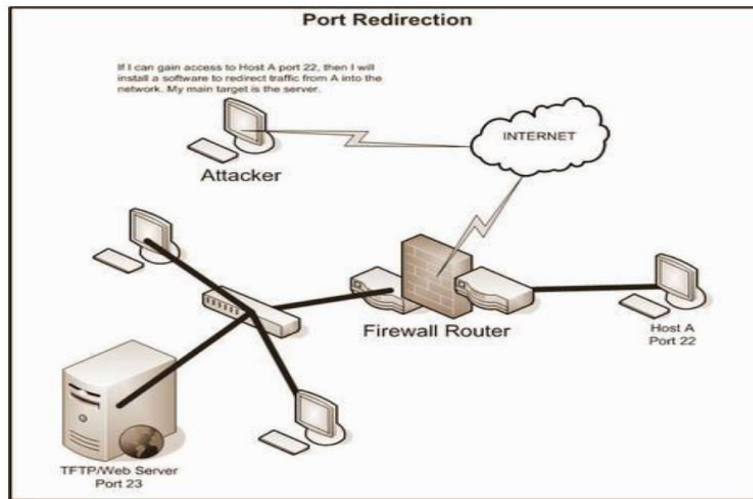


Figure 7: Port Redirection Attack

III. DOS ATTACKS

Types of attack that bring the network down in such a way that resources are not available even for authenticated users are known as DOS attacks. Malicious hacker saturated the target machine with useless traffic so that it cannot respond or too slow to respond and some times unavailable. Attacker may target a single machine to make it impossible for outgoing connections on the network or may attack on the whole network to make it impossible for incoming and outgoing traffic. For example attack on web site of any organization. Ping of death, SSPing, Land, Win Nuke and SYN flood are some of the examples of DOS attacks. In SYN flood attack hacker sends a SYN packet to target host which then respond with SYN acknowledgement, at the end attacker does not send any ACK packet to the target host that causes the connection to remain in half open state. TCP connection does not remove this connection from its table and wait to expire this session, attacker take the advantage of this and continue sending new SYN packets until TCP SYN queue filled and cannot accept new connections. The common method for blocking DOS attack is to place a filter which examines the pattern of data; if same pattern of data came frequently then filter can block that message.

Distributed Denial of Service (DDOS)

In DDOS attacks several compromised systems are used to launch an attack against a targeted host or network. For targeting a host attacker first compromise some other hosts on network and install some software for controlling them usually these compromised hosts are called agents or zombies. Using these agents attacker launch overwhelm attack against the target. Compromised

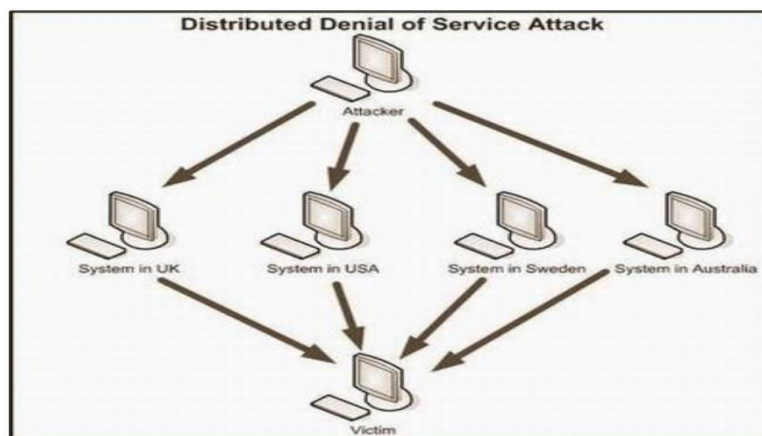


Figure 8: Distributed Denial of Service Attack

systems control with different software like Trino and Shaft. Example of DDOS attacks are SMURF, MYDoom and TFN. DDOS attacks are very hard to defend. To trace out the intruder is also very difficult as they are on back side and using other hosts against the victim. Figure 8 is describing distributed denial of service attack.

Buffer Overflow

We can define buffer overflow as when a hacker tries to store too much data in buffer which it cannot hold. Take an example of glass which can hold 5 ounces of water if we put 8 ounces what will happen? Obviously water overflows from the edges. Buffer overflow is similar to this example;

where glass corresponds to buffer and water corresponds to data. The overall goal of this attack is to weaken the function of victim's program so that hacker can easily take control of that program. Buffer overflow is the best known attack on security which can cause attack against availability, integrity and confidentiality of data. Examples are NetMeeting Buffer overflow, Linux Buffer Overflow, Outlook Buffer Overflow.

Viruses and Other Malicious Program

Viruses and other malicious program have the ability to make duplicate copies of them on an ever increasing number of computers. A "Virus" is just like a computer program that spread by copying itself into other programs. Another malicious program "Worm" is spread through the network. Without the network it cannot spread and can eliminate only when whole network or system is shutdown. Examples of popular worms are Code Red, Slammer, Storm Bot. A malicious program that resides in system and execute on an event like date or time is called "Logic Bomb", "Trojan Horse" is another type of malicious program that hackers use to steal useful information like user name, password and bank account codes.

IV. CONCLUSION

Originally it was assumed that with the importance of the network security field, new approaches to security, both hardware and software, would be actively researched. It was a surprise to see most of the development taking place in the same technologies being currently used. The embedded security of the new internet protocol IPv6 may provide many benefits to internet users. Although some security issues were observed, the IPv6 internet protocol seems to evade many of the current popular attacks.

REFERENCES

1. A White Paper, —Securing the Intelligent Network, powered by Intel corporation.
2. Network Security [Online] available: http://en.wikipedia.org/wiki/Network_security.
3. —Network Security: History, Importance, and Future, University of Florida Department of Electrical and Computer Engineering, Bhavya Daya.
- [4] Vivek Thoutam, "An Overview On The Reference Model And Stages Of IOT Architecture", "Journal of Artificial Intelligence, Machine Learning and Neural Network", Vol 01, No 01, Aug-Sept 2021
- [5] Vivek Thoutam, "A Study On Python Web Application Framework", "Journal of Electronics, Computer Networking and Applied mathematics", Vol 01 , No 01, Aug-Sept 2021
- [6] Vivek Thoutam, "Physical Design, Origins And Applications Of IOT", Journal of Multidisciplinary Cases, Vol 01 , No 01 , Aug-Sept 2021
- [7] Vivek Thoutam, "Models And Algorithms Of Artificial Intelligence", International Journal of Management, Technology And Engineering, Volume X, Issue XI, NOVEMBER 2020
- [8] Vivek Thoutam, "Machine Learning Vs Artificial Intelligence", International Journal of Scientific Research in Science and Technology, Volume 6, Issue 4, July-August-2019
- [9] Vivek Thoutam, "Unique Security Challenges of IoT Devices and Spectrum of Security Considerations", Journal of Artificial Intelligence, Machine Learning and Neural Network, Vol 01, No. 2, Oct-Nov 2021
- [10] Vivek Thoutam, "Artificial Intelligence And Machine Learning In Regulatory Compliance And Supervision", JASC: Journal of Applied Science and Computations, Volume VII, Issue V, May 2020
- [11] Vivek Thoutam, "IoT Cloud Convergence, Emerging Economy and Development Issues", Journal of Environmental Impact and Management Policy, Vol 01, No 02, 2021

- [12] Vivek Thoutam, "A comprehensive review on communication enablers and communication models of IoT", Journal of Community pharmacy practice, Vol 1, No 2, 2021
- [13] Vivek Thoutam, "Pros and Cons of Artificial Intelligence", Journal of Emerging Technologies and Innovative Research, volume 2, Issue 12, December 2015.
- [14] Vivek Thoutam, "Difficulties with Missing Data in Different Applications", Journal of Emerging Technologies and Innovative Research, volume 5, Issue 6, June 2018
- [15] Vivek Thoutam, "Artificial Intelligence And Machine Learning In Regulatory Compliance And Supervision", JASC: Journal of Applied Science and Computations, Volume VII, Issue V, May 2020
- [16] Vivek Thoutam, "Models And Algorithms Of Artificial Intelligence", "International Journal of Management, Technology And Engineering", Volume X, Issue XI, NOVEMBER 2020
- [17] Vivek Thoutam, "Machine Learning Vs Artificial Intelligence", International Journal of Scientific Research in Science and Technology, Volume 6, Issue 4, July-August 2019
- [18] Vivek Thoutam, "Genetic Algorithms and Developments of Intelligent Machines", International Journal of Research and Applications, 7(28), Oct - Dec 2020
- [19] Vivek Thoutam, "SQL Injection Vulnerabilities Prevention through ML IPAAS Architecture", International Journal of Novel Research and Development, Volume 7, Issue 3 March 2022
- [20] Vivek Thoutam, "Future Research Directions And Challenges Towards IoT", International Journal of Creative Research Thoughts, Volume 10, Issue 2 February 2022
- [21] Kola Vasista. (2022). Benefits And Approaches Of Artificial Intelligence. Journal of Artificial Intelligence, Machine Learning and Neural Network (JAIMLNN) ISSN: 2799-1172, 2(02), 52–56. Retrieved from <http://journal.hmjournals.com/index.php/JAIMLNN/article/view/443>
- [22] Kola Vasista. (2022). Practical Approach Of Implementing Artificial Intelligence. Journal of Electronics, Computer Networking and Applied Mathematics (JECNAM) ISSN : 2799-1156, 2(02), 21–24. Retrieved from <http://journal.hmjournals.com/index.php/JECNAM/article/view/445>
- [23] Vasista, K. (2022). Evolution of AI Design Models. Central Asian Journal Of Theoretical & Applied Sciences, 3(3), 1-4. Retrieved from <https://cajotas.centralasianstudies.org/index.php/CAJOTAS/article/view/415>
24. Vasista, K. (2022). Augmented Reality Vs. Virtual Reality. Central Asian Journal Of Mathematical Theory And Computer Sciences, 3(3), 1-4. Retrieved from <https://cajmtcs.centralasianstudies.org/index.php/CAJMTCS/article/view/154>
- [25] Kola Vasista. (2022). Implications for Policy and Practice Towards VR and AR. Journal of Environmental Impact and Management Policy (JEIMP) ISSN:2799-113X, 2(01), 13–17. Retrieved from <http://journal.hmjournals.com/index.php/JEIMP/article/view/452>
- [26] Kola Vasista, "Foreign Capital Issuance and Participants in the Securities Market", International Journal of Research and Analytical Reviews, VOLUME 2, ISSUE 4, OCT. – DEC. 2015
- [27] Kola Vasista, "A Research Study On Major International Stock Market", International Journal of Research and Analytical Reviews, VOLUME 4, ISSUE 3, JULY – SEPT. 2017
- [28] Kola Vasista, "A Review On The Various Options Available For Investment", International Journal Of Creative Research Thoughts - IJCRT (IJCRT.ORG), Volume 7, Issue 2, April 2019, ISSN: 2320-2882
- [29] Kola Vasista, "Types And Risks Involved Towards Investing In Mutual Funds", International Journal of Current Science (IJCSPUB), Volume 12, Issue 1, March 2022 , ISSN: 2250-1770
- [30] Kola Vasista, "Role Of a Stock Exchange In Buying And Selling Shares", International Journal of Current Science (IJCSPUB), Volume 12, Issue 1, March 2022 , ISSN: 2250-1770
- [31] Kola Vasista, "A Detailed Study On The Factors Influencing The Price Of a Stock", International Journal of Novel Research and Development, Volume 2, Issue 8, August 2017, ISSN: 2456-4184
- [32] Kola Vasista, "Objectives And Importance Of Capital Markets And The Role Of Financial Institutions", International Journal of Emerging Technologies and Innovative Research (www.jetir.org), ISSN:2349-5162, Vol.2, Issue 9, page no.475-478, September-2015, Available : <http://www.jetir.org/papers/JETIR1701762.pdf>
- [33] Kola Vasista, "An Overview On Provident Fund, Pension Funds, Pfrda, Insurance Companies And IRDA", International Journal of Emerging Technologies and Innovative Research (www.jetir.org), ISSN:2349-5162, Vol.5, Issue 10, page no.284-287, October-2018, Available : <http://www.jetir.org/papers/JETIR1810A93.pdf>
- [34] Peddyreddy. Swathi, "Approaches And Objectives towards Financial Management", International Journal of Advanced in Management, Technology and Engineering Sciences, Volume IV, Issue I, 2014
- [35] Peddyreddy. Swathi, "An Overview On The Types Of Capitalization", International Journal of Advanced in Management, Technology and Engineering Sciences, Volume VI, Issue I, 2016
- [36] Peddyreddy. Swathi, "Architecture And Editions of Sql Server", International Journal of Scientific Research in Computer Science, Engineering and Information Technology, Volume 2, Issue 4, May-June-2017

- [37] Peddyreddy. Swathi, “Scope of Financial Management and Functions of Finance”, International Journal of Advanced in Management, Technology and Engineering Sciences, Volume III, Issue 1, 2013
- [38] Peddyreddy. Swathi, “A Study On Security Towards Sql Server Database”, JASC: Journal of Applied Science and Computation, Volume V, Issue II, February 2018
- [39] Peddyreddy. Swathi, “A Comprehensive Review on The Sources of Finance”, International Journal of Scientific Research in Science, Engineering and Technology, Volume 1, Issue 4, July-August 2015
- [40] Peddyreddy. Swathi, “A Study on SQL - RDBMS Concepts And Database Normalization”, JASC: Journal of Applied Science and Computations, Volume VII, Issue VIII, August 2020
- [41] Peddyreddy. Swathi, “A Comprehensive Review on SQL - RDBMS Databases”, Journal of Emerging Technologies and Innovative Research, Volume 6, Issue 3, March 2019.
- [42] Peddyreddy. Swathi, “An Overview on the techniques of Financial Statement Analysis”, Journal of Emerging Technologies and Innovative Research, Volume 1, Issue 6, November 2014
- [43] Peddyreddy. Swathi, “COMPLEXITY OF THE DBMS ENVIRONMENT AND REPUTATION OF THE DBMS VENDOR”, Journal of Interdisciplinary Cycle Research, 13 (3), 2054-2058
- [44] Peddyreddy. Swathi, “Implementation of AI-Driven Applications towards Cybersecurity”, JASC: Journal of Applied Science and Computations, 7(8), 127-131
- [45] Peddyreddy. Swathi. (2022). Implications For Research In Artificial Intelligence. Journal of Electronics, Computer Networking and Applied Mathematics (JECNAM) ISSN : 2799-1156, 2(02), 25–28. Retrieved from <http://journal.hmjournals.com/index.php/JECNAM/article/view/447>
- [46] Peddyreddy. Swathi. (2022). A Study On The Restrictions Of Deep Learning. Journal of Artificial Intelligence, Machine Learning and Neural Network (JAIMLNN) ISSN: 2799-1172, 2(02), 57–61. Retrieved from <http://journal.hmjournals.com/index.php/JAIMLNN/article/view/444>
- [47] Peddyreddy. Swathi. (2022). Industry Applications of Augmented Reality and Virtual Reality. Journal of Environmental Impact and Management Policy (JEIMP) ISSN:2799-113X, 2(02), 7–11. Retrieved from <http://journal.hmjournals.com/index.php/JEIMP/article/view/453>



INNO  SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.165

 **doi**[®]
cross **ref**

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

 9940 572 462  6381 907 438  ijircce@gmail.com



www.ijircce.com

Scan to save the contact details