Virtual Dispersive Network in the Prevention of Third Party Interception: A Way of Dealing with Cyber Threat

Apoorva Ganapathy

Senior Developer, Adobe Systems, San Jose, California, USA

*Corresponding Contact:
Email: apganapa@adobe.com

Manuscript Received: 12 Sep 2020 - Revised: 12 Nov 2020 - Accepted: 18 Nov 2020

ABSTRACT

Virtual Dispersive Network (VDN) in preventing third party interception - a way of dealing with cyber threats. VDN is a unique approach to cybersecurity, wherein a signal is transmitted in short bursts or quantum packets, which can't be covertly read without disrupting their content. No one can intercept data sent to you without introducing some noise in it. In this study, we have explored the use of Virtual Dispersive Network in cybersecurity which is still an innovation in the fight against cyberattacks however is still shows considerable potential in reducing cyberattacks on wireless networks drastically.

Keywords: Virtual Dispersive Network (VDN), Cybersecurity, Computer Network System, Encryption, Malware Threats, Ransomware, Phishing Attacks, Hijacking

INTRODUCTION

Cybersecurity refers to the security and protection of software, hardware, and data, interconnected systems from cyber threats. Companies and individuals use cybersecurity practices in protecting computer systems and data centers from unauthorized access. An efficient cybersecurity protocol can effectively enhance the security system against vicious threats which can destroy, delete, alter, access, and collect sensitive data from an individual's or company's systems (Ganapathy, 2019b). Also, cybersecurity strategies can effectively prevent threats that are capable of disabling and disrupting the normal functions of a system or device. The increase in devices, programs, and users in current business and the increase in confidential and sensitive data have also brought about cybersecurity's increased significance for data protection (Neogy & Paruchuri, 2014). In addition, the volume of cyber threats and attacks is rising and the attackers and techniques used have become even more sophisticated, adding to the problem.

Cybersecurity and its elements

The field of cybersecurity may be divided into numerous sections. The efficiency of a cybersecurity system is dependent mainly on processes used in the coordination of the different sections. All organizations face cybersecurity maintenance challenges from the constantly changing attack environment. Resources are collected in the traditional reactive techniques to protect and secure computing systems and data sources from the most prominent attacks leaving the less prominent ones undefended. Unfortunately, this traditional reactive tactic is no more efficient (Paruchuri, 2019). To be updated with the constantly changing security threats, there is a need to adopt an advanced adaptive and proactive method. There are numerous CAO (Cybersecurity Advisory Organizations) that assist; for instance, and the NIST (National Institute of Standards and Technology) has recommended the adoption of constant real-time assessments and monitoring as a system for assessment of risk to fight both new and recurrent threats (Vadlamudi, 2015).

The advantages of the maintenance and utilization of cybersecurity processes are;

- Cybersecurity protects business data from attacks and breaches.
- Cybersecurity protects network systems and data.
- Cybersecurity prevents unauthorized users from accessing.
- An efficient cybersecurity system improves recovery time after a breach.
- Cybersecurity systems protect computer endpoints and end-users.
- Complies with regulations.
- It improves the continuity of business.
- An efficient cybersecurity system increases customers', partners,' stakeholders, and developers' trust and reputation.

TYPES OF CYBERSECURITY THREATS

Maintaining cybersecurity to keep it up to date with the current technologies, threat intelligence, and trends in security can be a challenging process. Cyber-attacks can come in numerous forms, and it essential to protect data and other assets from all forms.

The following are types of cyber threats:

- **Malware**: malware includes viruses, spyware, Trojans, worms, and so on. They are used to attack a computer system by inserting malicious software into programs or files.
- **Ransomware**: This is a different kind of malware. An attacker locks up files on a user's computer, usually using an encryption code. After the lock-up, the attacker demands a ransom payment to unlock and decrypt the files.
- **Social engineering**: this cyber-attack uses human interaction to fool users and break security protocols, and access usually protected sensitive data.
- **Phishing**: this is also a form of social engineering whereby attackers rely on sending fraudulent text messages and emails that look like prominent and reputable sources. This is usually random texting to steal confidential information through data such as login data and credit card information.
- **Spear phishing**: this attack targets a specific business, user, or organization.
- **Insider threats**: these are threats from negligent employees, customers, or contractors that lead to security breaches and losses. They can also be malicious when they are intentional.

- **Distributed Denial of Service**: shortened as DDoS. The traffic of a particular system (website, server, or another network resource) is disrupted using numerous systems. This is done by overrunning the targeted system with packets, connection requests, or messages. This can cause a system crash, slow system speed, and prevent the legitimate network from utilizing the system.
- **Advanced Persistent threats**: shortened as APTs. This type of cyber-attack whereby the attacker infiltrates a system and stays within the network undetected for a prolonged time to steal data.
- **Man in the Middle attacks**: shortened as (MitM). This is just like APTs. The attacker infiltrates the network and listens in on correspondence, intercepts, and relays conversations and communications between parties without their knowledge. Here the parties or users may think the connection is only within themselves.

There are other widespread attacks such as cross-site scripting (XSS), malvertising, botnets, SQL injection attacks, zero-day exploits, and so on. Malware forms are numerous and come in different forms like viruses, worms, and ransomware.

CYBERSECURITY CHALLENGES

Data loss, hackers, evolving cybersecurity methods, risk management, and privacy are part of the constant challenges faced by cybersecurity. The volume and numbers of cybersecurity threats and attacks may likely not reduce in times to come. The increase in application, devices, and entry points for attacks like the invention of the IoT (Internet of Things) brings about a greater need for network and device security. The constantly changing nature of security threats is one of the most challenging problems faced in cybersecurity. New methods of cyber threats and attacks emerge from the development of new technologies or advancements of current technology. Being up to date with the constantly evolving and advances in threats while remodeling policies and systems to prevent recent attacks can be complicated (Vadlamudi, 2016).

Challenges such as making sure all the cybersecurity elements are constantly up to date to prevent possible weaknesses. This may be even more challenging for small enterprises which are do not have the workforce or needed resources. Also, companies collect numerous data from users who have plans to use one or more of their services. This would increase the possibility of a cyber-attack by attackers who may want to steal Personally Identifiable Information (PII) as more user data are collected, resulting in a new concern. For instance, enterprises that collect PII on cloud storage are likely targets for ransomware attacks. Therefore, there must be efforts by such organizations to prevent data breaches on the cloud. Cybersecurity policies must also address End-user education. Insider threats from employees can occur accidentally when they unknowingly carry malware or viruses to the office through personal computers or mobile phones. Security insight and awareness training held frequently will enable staff to know cyber threats better and know how to play their part against cyber-attacks. Also, the scarcity of qualified cybersecurity crew is an issue faced in cybersecurity. The significance of cybersecurity personnel in managing, analyzing data, and responding grows as the volume of the gathered data used by enterprises increases (Paruchuri, 2018).

Use of automation in cybersecurity

The use of an automated machine in cybersecurity to protect an organization's data is increasing in importance. Automation machines now play crucial roles in protecting

company data from the increasing amount of sophisticated cyber threats. Artificial Intelligence and machine learning are used in places with a large amount of data sources to enhance three primary cybersecurity categories, which include:

- **Detection of cyberthreats**: Artificial Intelligence systems can carry out data analysis and detect threats that are already known and new threats.
- **Responding to threats**: Artificial Intelligence can also automatically generate security protocols.
- **Human Assistance:** security personnel is often overworked with reoccurring and repetitive tasks which can be automated. These tasks could be alerts, emails, and so on. The use of Artificial Intelligence can reduce work fatigue by automating significant data analysis and automatically handling low-risk alerts and several other reoccurring tasks, giving staff more time to handle more complicated jobs.

There are several other benefits of using AI in cybersecurity, and they include classification malware and attacks, analysis of traffic, compliance analysis, and so on.

There several cybersecurity products and services offered by cybersecurity vendors which cover a variety of fields (Ganapathy, 2019a). Antimalware, identity and access management, intrusion prevention systems, endpoint protection, intrusion detection systems, data loss prevention, encryption tools, security information and event management, virtual private networks, virtual dispersive Networking, endpoints detection, and response, and so on. Some of the most prominent cybersecurity service providers IBM, Microsoft, Splunk, Cisco, Fortinet, CrowdStrike, KnowBe4, etc.

MAN IN THE MIDDLE (MITM) ATTACKS

MiTM attacks are a popular kind of cybersecurity threaten whereby hackers listen in on the interactions between two endpoints. These attacks happen in the middle of two host communication legitimately, enabling the attacker access to 'eavesdrop' on the communication they ordinarily are not supposed to be a to list to. This is also where the name "man in the middle."

MiTM attacks are cyberattacks in which confidential and significant data are intercepted by attackers who utilize numerous methods of interjecting themselves into the process of communication. The hacker may then begin to listen to the communications passively and stealing confidential data and secrets (Vadlamudi, 2018). The attacker may also participate actively by modifying the contents of the messages or by a person or system impersonation where the other party may believe he is communicating with someone else.

This is similar to landlines and telephones, where a person can listen to calls with a third connected telephone. The parties conversing may not know that there is a third-party listener. This is a perfect man-in-the-middle attack scenario.

MitM attackers use several techniques, they include:

- **Address Resolution Protocol (ARP) poisoning**: ARP refers to a low-level system on the local networks that deciphers the MAC (Machine Address) to the Internet protocol address (IP address). Hackers infiltrate the system by inserting untrue data into the system to deceive the computer into thinking that the hacker's system is the network's gateway. As soon you the victim connects to the network, the hackers receive all the victims' network traffic which ought to be ordinarily collected by the actual network

gateway. The attacker receives the traffic and then sends it to the actual destination. By doing this, the attack gets access to all your packets.

Scenario

Greg (the hacker) enters a network using network sniffing tools

Greg then examines the victim's network packets to anticipate a series of packets between the gateway and the victim.

Greg then transmits a packet to the victim's system using a false source address of the gateway and the actual Address Resolution Protocol sequence to trick the victim's computer into thinking that the hacker's system is the network.

Greg also simultaneously bombards the victim's network gateway with a DoS attack (Denial of Service attack). This is to make the victim receive the false ARP packets before the network gateway can react.

In summary, Greg tricks the victim's computer into reasoning that the hackers' computer is the actual gateway making the man in the middle attack a success.

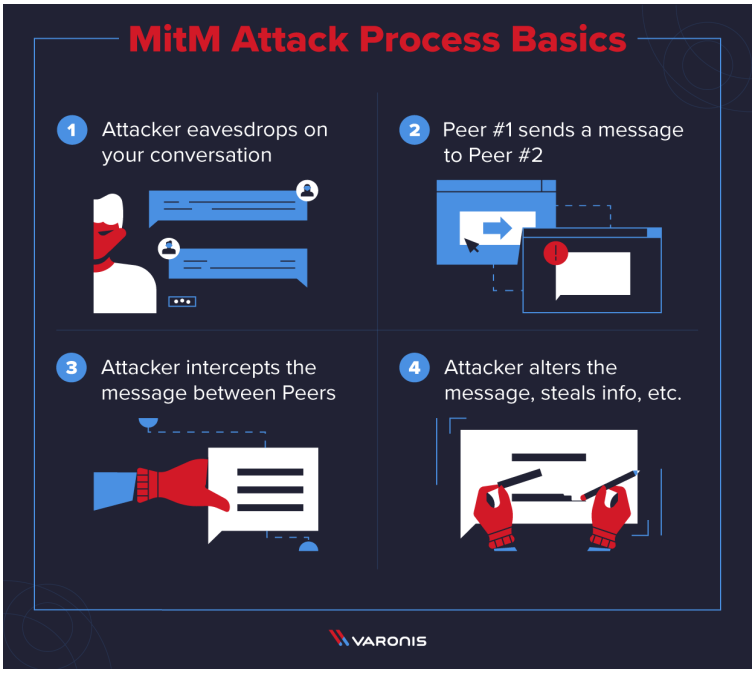

Figure 1: MiTM Processes (Source: varonis.com)

- **Domain Name System (DNS) cache poisoning** happens when a hacker gives his victim a false DNS entry that takes him to a new website. The site may look like an original and well prominent site, but it is not. By doing this, the attackers can capture information and data like passwords, pins, usernames, and so on when the victim enters the phony site. For instance, Greg finds out that his victim uses a specific Domain Name System revolver, and Greg knows that just like older versions of BIND, the victim's resolver is highly susceptible to attacks. Greg utilizes the vulnerability to manipulate the DNS resolver that the site is located in his IP address. When the victim

tries to visit the site, the DNS resolver will redirect him to the hacker's system as it believes that the site's IP address is stored there. Greg then finishes the connection with the actual site to prevent the victim from realizing that there is a man in the middle listening. Thus, the attacker (Greg) can access and see all the victims (or any using the DNS resolver to connect to the site) packets that he sends.

- **Hypertext Transfer Protocol Secure (HTTPS) Spoofing:** For most users, HTTPS is one of the many ways to get to know whether or not their data are safe. 'S' in HTTPS, means secure and that is precisely what attackers want victims to assume. HTTPS spoofing involves hackers developing HTTPS websites that look just like legitimate ones with authentication certificates that are valid. However, the URL will be slightly different from the legitimate ones. For instance, a Unicode which looks like an alphabet may be used in place of an actual alphabet to confuse victims.
- **Eavesdropping on Wi-Fi**: Hackers can eavesdrop on traffic and communications on unsecured or public Wi-Fi networks with general names to deceive victims into connecting to steal confidential data and information such as credit card details, credit, or some other data that may be sent on that network. Numerous videos are showing how simple it is for hackers to do this.
- **Session Hijacking**: Session hijacking involves an attacking style whereby the attacker allows the victim to access a webpage, for instance, an email account for banking operations. After the victim logs in, the attacker then steals his session cookie and records it into his account using his browser. This is possible as most web browsers utilize a machine that creates a momentary session token used for possible requests in the future so that users did have to input passwords and usernames repeatedly. A hacker can get essential traffic and discover the session login token of a user and utilize it in making requests just like the user would. There is no need for spoofing by the attacker after getting the session token (Ganapathy, 2016a). With a victim's active session token, the hacker can the victim has the ability to do. For example, Greg, the hacker, can transfer all the victim's saving to another account offshore or even use it to buy cryptocurrencies or any other goods or services. It can also be used to get into your workplace and access files or business networks.
- **Rogue Access Point:** Wireless card-equipped devices usually try to connect to the access point transmitting the most powerful signals automatically. However, hackers can create their wireless access point then deceive devices at close ranges into connecting to its domain. The hacker can then manipulate all the traffic generated from the victim's network. The fact that the hacker does not need to be on a trusted network to carry out this attack makes it even more dangerous (Vadlamudi, 2017). The attack needs to be nearby physically.

MAN IN THE MIDDLE DETECTION

Discovering man-in-the-middle attacks can be pretty tricky, especially without adequate security measures. A MiTM attack can last a long time undetected if no intentional and active steps are taken to examine your system and network. Exploring pages for proper authentication and installing infringement detection systems are some of the critical techniques used in detecting potential attacks (Paruchuri, 2017). However, these processes may need extra detailed examination afterward.

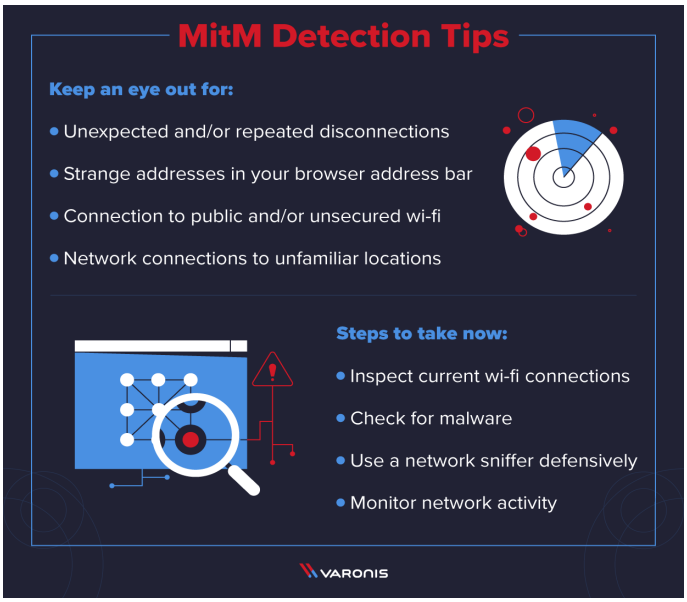

Figure 2: MiTM Detection (Source: varonis.com)

It is pretty essential to adopt preventive methods to avoid the attack of MiTM before occurrence. This technique would prevent possible damage and makes it more beneficial than detecting them as they occur actively. Users must pay more attention to their browsing practices and see possible harmful areas as it is essential for maintaining high network security. Below are some of the ways we can prevent man-in-the-middle attacks.

- **Encrypting powerful WAP/WEP on Access Points**: This method prevents third parties without permission from accessing a user's wireless access point network by just being close by. A hacker can force his way into a network encrypted with a weak encryption mechanism and operate as a man-in-the-middle attacker—the better the encryption implementation, the safer the network. Login credentials with a more powerful router: changing your router login from the default settings to a stronger one is quite essential. Changing both the router login credentials and the Wi-Fi login is quite crucial. A hacker may change a user's DNS servers to their false servers using their login credentials. They can even go as far as infecting the user's router with vicious software.
- **Virtual Private Network (VPN):** Within a local area network (LAN), a secure environment for confidential data may be created using VPNs. VPNs create several subnets for securing communications through the use of encryption-based keys. This method prevents a hacker from deciphering the traffic in the VPN even if he can connect to the network.
- **Force HTTPS**: By using HTTPS, communications over HTTP can be made secure through the public-private key exchange. This makes the sniffed data useless to the hacker (Ganapathy, 2018). Websites must try to make provisions for just HTTPS and disregard the counter HTTP.
- **Public Key Pair Based Authentication**: MiTM attacks are usually based on different spoofing of one thing or the other. There are several stack layers in which the Pubic Key pair-based authentication can be utilized to ensure that communications remain original and the intended communication holds.

Figure 3: MiTM Prevention (Source: varonis.com)

VIRTUAL DISPERSIVE NETWORKING (VDN) AND CYBERSECURITY.

Virtual Dispersive Networking takes an approach similar to that of the time-honored military Radio spread spectrum security. Radios randomly swivel through frequencies and break down communications into numerous parts. Similarly, virtual dispersive networks break down the original communications into several data streams and separately encrypt every single part, then transmit them through several servers, systems, and computers (Paruchuri & Asadullah, 2018). This moves the data dynamically and also to an enhanced route. The streams and routes are randomized while at the same time it takes in the network issues. The communication gets to the attackers, and it would be not easy to discover several pieces of data as they go on like cloud, hubs, IoT, etc.

Messages are from one device to another device through a spawning machine for connection on a network which comes first and virtualizes the abilities of the internet device. This is a method VDN. The VDN transmits multiple packets for communication to a different selected network address and connects the message to the second device.

Virtual dispersive Networking presents a highly advanced and innovative development in cybersecurity unmatched by any other network security technique. Virtual Dispersive Networking secures wireless networks to a level comparable to the wired network. The question of cybersecurity is now within the domain and control of the users. Other cybersecurity frameworks handle data transmission based on a firewall, within and through to the NOC (Network Operations Center). VDP protects the data transmission network at the most vulnerable point, which is the Internet. It is a software solution that functions on the current network system and devices. VDN installation is quite simple because it is downloadable, just like other software downloaded to several devices.

Currently, devices on a standard network transmit an entire data (which may be files, documents, videos, images, and so on) using just one stream from the first device to the second. The use of a single data stream in sending and receiving data makes the network vulnerable and highly susceptible to attacks, especially MiTM attacks.

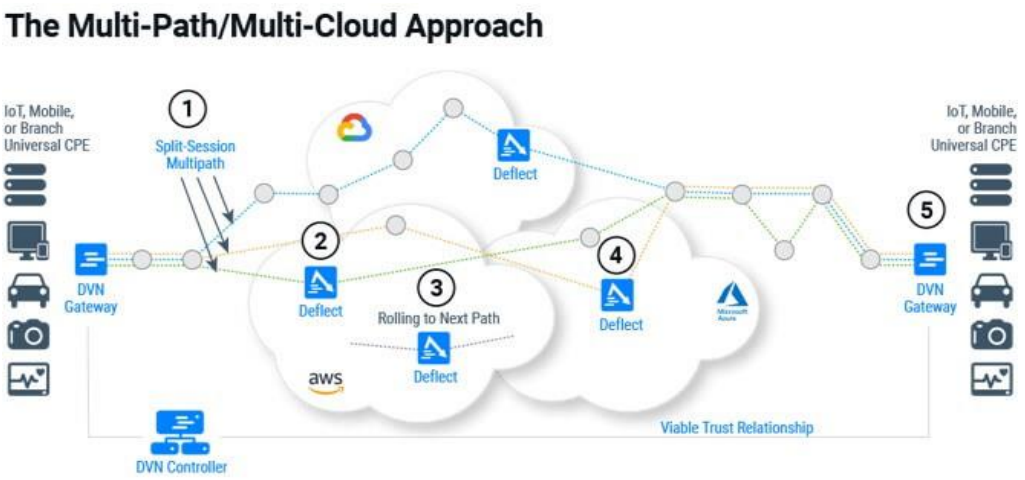

Figure 4: VDN (Source: arridae.com)

Virtual Dispersive Networking prevents a network system from Man in The Middle attacks by separating data into several parts and making the several parts use separate streams to their destination. VDN also provides additional security by encrypting the numerous paths distinctly. After the separate and individual parts get to the receiver, authentication and reassembling take place to make it ready for use (Ganapathy, 2016b). This makes it difficult for the attacker, as a man-in-the-middle attack on a single separate path only gives the hacker a small part of a possibly big file. This makes the hack useless as a piece of a larger file may not be used except with the other parts that have all been transmitted using differently encrypted streams or routes. The paths for each stream of data are randomly selected simultaneously and constantly change in a similar manner to a "spread spectrum frequency hopping" radio for Internet Protocol networks. Virtual Dispersive Networking makes it very difficult for hackers to discover the other paths on which the remaining parts are being transmitted through. Also, VDN does not ensure secure data transmission, and it additionally provides more enhanced network throughput speeds, capacity to firewall devices in the 'cloud', and improve service quality (Paruchuri, 2015). It also protects users from network operations interruption through the automatic and instant detection of attacks on any part of a network and separating the compromised device from the other network (Vadlamudi, 2019). This makes attacks on the impossible.

Benefits of Virtual Dispersive Networking

- **Advanced cybersecurity**: man in the middle attacks are avoided by scattering the numerous data over several encrypted streams. Pieces of data obtained by hackers remain useless as they are encrypted and nearly impossible to decrypt.
- **Tough network**: packets of data are rerouted to current paths whenever connections are lost on the numerous streams as a result of network collapse. Also, new paths may be added to which can run network failure downtime.
- **Performance and speed**: network bandwidth is increased since data transmission is carried out using several separate streams. This enhances the speed of data flow on the separate.

CONCLUSION

Today's disruptive technological innovations are more government-based, with their first penetration into financial markets and other industrial sectors such as banks and insurance companies. In addition, several networks like the cloud can use virtual dispersion networking tools in keeping their communications or environment secure from MiTM and other cyberattacks. The wide adoption of this technology may be hampered by fear of change, and an organization can, however, discover the potentials of the technology in data and communication security.

REFERENCES

Ganapathy, A. (2016a). Blockchain Technology Use on Transactions of Crypto Currency with Machinery & Electronic Goods. *American Journal of Trade and Policy*, *3*(3), 115-120. https://doi.org/10.18034/ajtp.v3i3.552

Ganapathy, A. (2016b). Virtual Reality and Augmented Reality Driven Real Estate World to Buy Properties. *Asian Journal of Humanity, Art and Literature*, *3*(2), 137-146. https://doi.org/10.18034/ajhal.v3i2.567

Ganapathy, A. (2018). UI/UX Automated Designs in the World of Content Management Systems. *Asian Journal of Applied Science and Engineering*, *7*(1), 43-52.

Ganapathy, A. (2019a). Cyber Security for the Cloud Infrastructure. *Asian Journal of Applied Science and Engineering*, *8*(1), 15-24.

Ganapathy, A. (2019b). Mobile Remote Content Feed Editing in Content Management System. *Engineering International*, *7*(2), 85-94. https://doi.org/10.18034/ei.v7i2.545

Neogy, T. K., & Paruchuri, H. (2014). Machine Learning as a New Search Engine Interface: An Overview. *Engineering International*, *2*(2), 103-112. https://doi.org/10.18034/ei.v2i2.539

Paruchuri, H. (2015). Application of Artificial Neural Network to ANPR: An Overview. *ABC Journal of Advanced Research*, *4*(2), 143-152. https://doi.org/10.18034/abcjar.v4i2.549

Paruchuri, H. (2017). Credit Card Fraud Detection using Machine Learning: A Systematic Literature Review. *ABC Journal of Advanced Research*, *6*(2), 113-120. https://doi.org/10.18034/abcjar.v6i2.547

Paruchuri, H. (2018). AI Health Check Monitoring and Managing Content Up and Data in CMS World. *Malaysian Journal of Medical and Biological Research*, *5*(2), 141-146. https://doi.org/10.18034/mjmbr.v5i2.554

Paruchuri, H. (2019). Market Segmentation, Targeting, and Positioning Using Machine Learning. *Asian Journal of Applied Science and Engineering*, *8*(1), 7-14.

Paruchuri, H., & Asadullah, A. (2018). The Effect of Emotional Intelligence on the Diversity Climate and Innovation Capabilities. *Asia Pacific Journal of Energy and Environment*, *5*(2), 91-96. https://doi.org/10.18034/apjee.v5i2.561

Vadlamudi, S. (2015). Enabling Trustworthiness in Artificial Intelligence - A Detailed Discussion. *Engineering International*, *3*(2), 105-114. https://doi.org/10.18034/ei.v3i2.519

Vadlamudi, S. (2016). What Impact does Internet of Things have on Project Management in Project based Firms? *Asian Business Review*, *6*(3), 179-186. https://doi.org/10.18034/abr.v6i3.520

Vadlamudi, S. (2017). Stock Market Prediction using Machine Learning: A Systematic Literature Review. *American Journal of Trade and Policy*, *4*(3), 123-128. https://doi.org/10.18034/ajtp.v4i3.521

Vadlamudi, S. (2018). Agri-Food System and Artificial Intelligence: Reconsidering Imperishability. *Asian Journal of Applied Science and Engineering*, *7*(1), 33-42.

Vadlamudi, S. (2019). How Artificial Intelligence Improves Agricultural Productivity and Sustainability: A Global Thematic Analysis. *Asia Pacific Journal of Energy and Environment*, *6*(2), 91-100. https://doi.org/10.18034/apjee.v6i2.542

--0--