ISSN 2347 - 3983
Volume 8. No. 7, July 2020
International Journal of Emerging Trends in Engineering Research
Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter85872020.pdf
https://doi.org/10.30534/ijeter/2020/85872020

Software Defined Network Evolution: A Quality Viewpoint for Enterprise Management

Sahana D S[1], Dr. Dayanand Lal N[2], Neetha K S [3], Nida kousar G[4] , Deepak S Sakkari[5]
Assistant Professor[1], Assistant Professor[2], Assistant Professor[3],
Assistant Professor[4], Assistant Professor[5]
[1]Department of CSE, GITAM School of Technology, Bengaluru, India, ssanthos@gitam.edu
[2]Department of CSE, GITAM School of Technology, Bengaluru, India, dayanandlal@gmail.com
[3]Department of CSE, GITAM School of Technology, Bengaluru, India, nsrinath@gitam.edu
[4]Department of CSE, GITAM School of Technology, Bengaluru, India, kousar.nida@gitam.edu
[5]Department of CSE, Presidency University, Bengaluru, India, deepaksakkari@presidencyuniversity.in

ABSTRACT

Software Defined Networking (SDN) is an evolving network framework and it is the major exciting innovations for optimizing network services and setup through improved programmability and optimization of the network. In SDN, unlike older system networks, a control plane determines whether to forwarding data is separated from the data plane which transfers data to chosen destinations. It allows the connection to the network more scalable, flexible and coherent (via the SDN controller). System administrators could quickly access network control and optimize flow of traffic without customizing a number of individual network devices with the different levels of abstraction offered by SDN. SDN has great potential .It has led to major investments of data centers, WAN and so on, and is increasing rapidly.

Key words: SDN, Networking Devices, Virtualization, SDN Controller

1. INTRODUCTION

Computer networks are becoming more complicated everywhere now with more and more machines are emerging every day by providing specific set of information. The piece of device used in networks such as IDS(Intrusion Detection Systems, Routers , Switches, Firewalls and other network devices is usually very difficult for the network administrator to handle individually [1]. The Internet and its technology have become immensely powerful due to rapid advances in technology, particularly cloud computing, artificial intelligence, block chain, augmented reality and virtual reality, cognitive cloud computing, IoT, etc. Individuals soon figured that the quickest method to still advertise suspicious goods, and also to collect authentication tokens and transfer computer viruses to utilize the method of wide distribution and simple transmission obtained by researchers who connected computers to each other through the Internet to construct a communication network with some significance[2].

Since the last couple of years Software Defined Networking (SDN) has become a vital phenomenon in the networking platform. Companies and organizations trying to discuss SDN for their organisation and future productivity plans to influence it. Adequately, SDN decreases a network's CAPEX (capital expenditure of network equipment) and OPEX (operational and maintenance expenditure) and that is ultimately what every corporation in the networking sector needs. One of the major explanations for the networking industry to reconsider modern network architecture is the rise of cloud computing, economical demands and even virtualization of server [3**].**

The conventional networks can not match current network requirements such as optimization, central analysis and monitoring, carry changes or tests, least error-prone, functional settings on each network computer, handling of network traffic and virtualization of data center servers. In addition, traditional networks are strongly connected to expensive network components which do not provide any kind of transparency or customizable internals. To address these concerns open source groups have brought up together to inform an approach to networking. So SDN became an evolving approach. Software-defined Networking (SDN) is a

framework that intends to make competitive advantages and control more versatile. By abstracting the control plane from the data transmission function, SDN facilitates control in different networking devices. As the name suggests, SDN is implemented by applications in an effort to learn about implementation. SDN is a layer of software which provides benefits such as reduced manual processing, flexible reliability and centralized network device control[4**].**

Present networking technologies such as SDN do away with the old network's static and decentralized objects. Centralization functionalities of SDN may contribute to an active and stabled network but privacy is a key concern. The groups have assembled with a firewall, antivirus software and an intrusion detection system to prevent unauthorized access to the network. [5**].** SDN has been originated from Open flow. SDN Initially has Control and Data plane separation with Control centralisation and has a OpenFlow to discuss with the Data Plane. But due to the evolution of technologies the definition of SDN has been changed accordingly. SDN is not a method. It is a mechanism for exploring several alternatives to multiple problems [6]. SDN is a framework that enables system administrator to automatically and dynamically track and manage different network devices, different types of networks, topology, traffic and packet handling, using high-language and API policies.

2. LITERATURE SURVEY

Martin et.al [7], explains about Ethane, a new design for networks Business. It enables organizations to characterize, and then directly enforce, a standard network-wide fine grain policy. Ethane combines comparatively straightforward Ethernet flow-based devices with a controller that handles the flow input and routing. Although this structure is possible in reverse with current hosts and switches. Ethane has been launched, supporting wired and wireless users, in both hardware and software. Ethane activities reveal that the network has operated the Stanford University network in 300 hosts, and that implementation process profoundly influenced the design of Ethane.

According to Chen et.al [8] describes the technology which has made convergence on reconfiguring the architecture of the 5 G mobile network. Software-defined architecture was described as an essential direction for 5 G networks to develop. Authors summarized the key research problems in SDMNs in this report. The idea that online world satisfaction typically requires infrastructure-based and resource-less networks, the pioneers are exploring the use of the Software-Defined Networking (SDN) paradigm in these so-called "heterogeneous" structures.

Authors A. Detti et.al [9] illustrates about wireless mesh networks which will work well because of its simplicity and easy management offered by Open Flow applied Software Defined Networking Paradigm. A central server can maximize the use of wireless resources, which can justify and execute processing actions on different levels of the protocol stack. The authors gave overview about the solution for combining functionality of SDN with a Wireless Mesh, where in we are attempting to address the reliability concerns associated with this surroundings. This method for incorporating SDN functionality into a wireless network, attempting to resolve the performance issues associated with this system. The wireless mesh SDN method proposed incorporates ready-to-market technologies.

F.Hu et.al [10] explains about Software-defined network (SDN) is a major critical architecture to work with huge networks that requires from time to time replication or reconfiguration. By shielding the control plane from the data plane, SDN achieves fast replications. Therefore, networking devices simply forward data by adopting the control plane's route table rules. This analysis may help the organization as well as the educated research in the Community and Individuals developing to understand the many popular SDN / Open Flow developments planning. Many crucial unfinished exams Issues were also highlighted in that Field. Authors also compared the advantages and disadvantages of various methods and illustrated about the future developments in this fascinating field of study.

N. Foster et.al [11] describes on presenting the Cisco insight on programming the SDN network. Many Cisco products have been made available with handling Open Flow capable objects. The communication perspective for the network basically consists of the controller and switchable Open Flow switches. The centrally controlled controller can be considered as the network brain that is primarily responsible for determining the incoming packet’s route by alerting the switches in the correct direction to route the packet. This paper showed a complete definition and explanation, and traditionally a literature analysis on the SDN different kinds of studies has already been presented. A description of the simulators used to build such networks was also displayed.

Q.Yan et.al [12] discusses emerging developments and functionality of DDoS attacks on SDN, as well as how to make

proper use of the SDN main elements to break DDoS attacks in high performance computing situations, how to avoid SDN itself from being a target of DDoS attacks and an approach is proposed. Latest patterns and features of cloud-based DDoS attacks, gives a detailed review of SDN-based security measures against DDoS attacks. Authors have investigated the papers on beginning DDoS attacks on SDN, and techniques to combat DDoS in SDN as well. The relationship between SDN and DDoS attacks has not been well explored in previous works, to the best of our knowledge. This task could even help to identify and make full use of the benefits of SDN in solving DDoS attacks in cloud computing interfaces, and to protect SDN itself from being a DDoS attack victim.

3. TRADITIONAL NETWORK AND SOFTWARE DEFINED NETWORKING (SDN)

3.1 Traditional Network

As a combination of data plane and control plane, a network can be described. The data plane will carry out the work of transferring the information in accordance with the routing information while the control plane will determine the network traffic and control decisions needed to achieve user data to the appropriate target [13]. In traditional networking we can see all these in a single device (e.g. routers).There are certain range of hardware devices in traditional networks; mostly routers, switches, and firewalls. All such devices tend to involve hardware interconnection that moves information through them, and software components are customized to control data movement via hardware based on data movement rules and regulations(Example : Huge traffic areas with lots of vehicles moving each day, without any bridges).

The main limitation about traditional network is that the admin has to log into individual system for interaction to configure and control the out-of-box functionality driven by hardware devices that require changes in configuration, making it complicated task and resource-intensive. Nevertheless, the increasing number of innovations that use concepts of virtualization, cloud computing and wireless technologies generates more complex and challenging environments in which the networks need to better support and adapt to these environments, and handle their demanding transactions in real time. Below figure 1 illustrates the architecture of traditional network.

All the devices will be having their own control plane and gives feedback according to the provisioned protocols designed. After the policies have indeed been defined and the flow described, changing the network activities in based on changing traffic demands is very difficult.

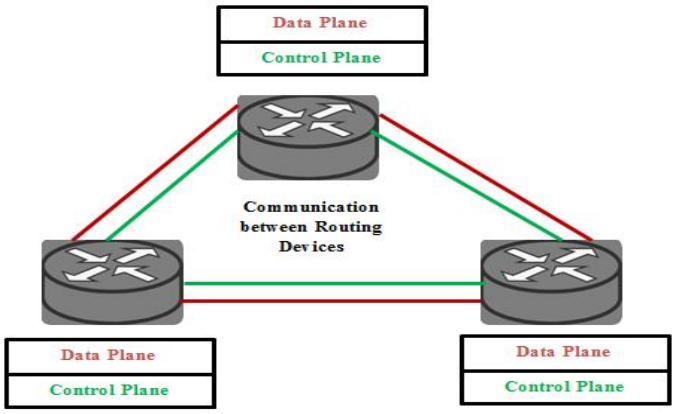

Figure 1: Traditional Network

The way to change the configureuration of all the systems is to make corrections. This leads to a limitation for admins who wish to adapt their network according to the requirements. For traditional networks, security solutions use a complicated mechanism to secure the network. These rules are spread on all computers used for networking. The rules are based on topology of the network; address-based, port-based policies that drop with the changes in the topology of the network . All security policies have been placed on the networking devices and placed at the network entry and exit. If an attacker does this through the networking devices, it can capture all network access, which then affects end-user trust. Traditional network architecture causes constraints on devices that add a lot of difficulty for security policies in those networks.

3.2 Software Defined Network

The purpose of software defined networking was to isolate the Network Devices Control and Data planes. The Control plane makes choices as to how the packets it receives should be sent and the Data plane literally transfers the packets through the system and passes them on via network. SDN suggests that the control plane must be centralized in order to maintain and change the network configureuration in an innovative working and adaptable manner. If a network administrator needs to provide increased capacity or modify existing data movement rules or regulations they don't need to communicate to multiple devices and make manual change. The modification need to be made dynamically enabling them to form and change the network very easily and

quickly. There's an effort with SDN to try to curb this by using certain open principles like OpenFlow.

3.2.1 SDN Architecture

The network is a collection of devices that are connected from one location to another to exchange the information. The internet is one perfect example of a network. Large enterprises and sectors have to dynamically adjust their configuration settings according to their business objectives. In SDN, the network controlling role has been divided from the communication networks into a central entity called controller and these network controllers operated with different roles as transmitting data controllers. The SDN distinguishes the control plane from the networking devices, thus acting as a dynamically controlled unit, like the network operating system or the SDN controller [14].

3.2.2 Architecture

SDN's central functionality involves controller interaction with data plane. Interacting as a system with use of the protocol for open flow. The SDN network with a centralized control plane gives information in this area, so that flows are built on the basis of existing network policies [15].Below figure 2 illustrates the SDN architecture.

In SDN, there are three layers [16]: the application layer; the control layer and the data or infrastructural layer as shown in figure. The first layer is the application layer, which contains systems that delivers the services like switch / network virtualization, firewalls, Routers and load balancers. These are differentiated from the lower layers, which is the data layer. The control layer, or SDN controller, which is located in the middle, is the most important feature of the SDN architecture. Each layer distinguishes the control plane from the data plane and operates as an app as it is associated to the network's digital and physical devices [17][18].To co-ordinate between planes, SDN uses Northbound Interface and Southbound Interface. The application and the control layer employ the Northbound Interface (NBI), while the South Bound Interface (SBI) allows the control layer to interact with the data layer.

The data plane consists of network devices, which gets it through a southbound interface by presenting their features to the control plane. SDN applications reside in the application plane and transmit their machine needs through the northbound interface to the control plane.

(i)Data Plane

The Data Plane describes the physical infrastructure of a network. Devices which are meant for forwarding like Switches and Routers are linked by wired or wireless media. It also perform handling of Traffic forwarding and engine processing , which takes help of some types of protocol like Address Resolution Protocol(ARP), Link Layer Discovery Protocol(LLDP). Helps to provide the interfaces to the control plane for the purpose of communication, controlling functions offered by the network elements or forwarding devices, advertising the capabilities, and also to notify events. It uses the protocol (e.g., Open Flow) for communicating with controller.

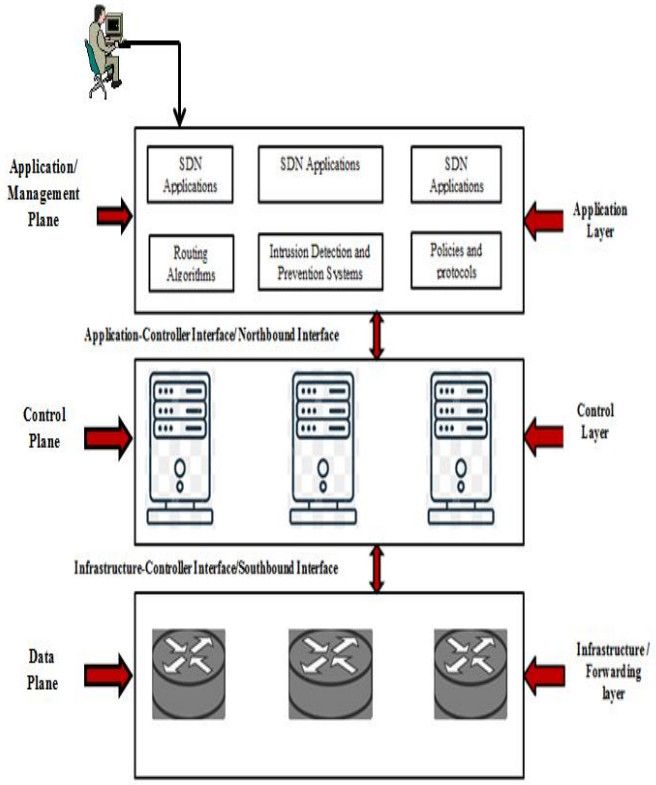

Figure 2: SDN Architecture

A. Open Flow

The open flow protocol will work as a means of synchronization between controller and network devices. This is a flow-based interaction; the data plane has a controller which controls the entry in the flow table [19] [20] for each of the networking devices [21]. An open flow controller implements and removes the forwarding rules within network switches to establish communication across the network. Based on a domain match a forwarding rule includes details about a packet header, sender and receiver port. Sender and receiver IP addresses and similar practices

are performed to alert of the sending or declining of packet information. The controller will modify specific entries to establish a new switch process in the flow tables, and this can also be done in actual environments.

(ii) Control Plane

Basic task is to program the devices for forwarding. So, it serves as the network's brain. The plane contains a centralized controller(s). The controller has absolute global network vision**.** The main objectives of control planes functionalities is to get the network state information by knowing about topology of network, Identifying the device, Computing the path, applying different the security mechanisms, since many controllers, Coordination among different controllers.

(iii) Application plane/ Management Plane

It involves device networking, such as routing, tracking, load balancing, and maintaining firewalls. Main responsibility of management plane is to determine rules and policies. Applications here define the services and behaviors needed by the network, in the business and policy agreement sense.

3.2.3 Benefits of SDN

The below figure 3 illustrates some of the benefits of SDN over Traditional Network. The brief description of those benefits is discussed below.

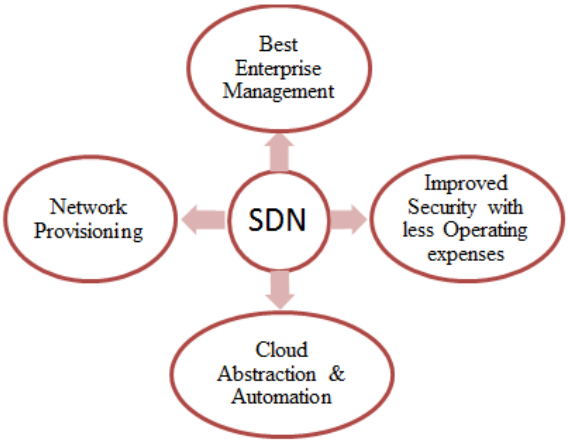

Figure 3: Benefits of SDN

(i) Network Provisioning:

SDN offers a consolidated knowledge of the overall network, enabling the centralization of business management and provisioning.

(ii) Best Enterprise Management

Corporate networks are needed to build on-demand virtual machines and emerging technologies [22] [23] to match the new demands of Big Data Analytics. Using the SDN approach, IT administrators can interact with network configuration without affecting the network

(iii) Improved Security and less Operating expenses

In SDN, both information and protection policies can be regularly controlled and communicated within organization to improve the security. It uses and optimizes commoditized hardware, simplifying the process even further. SDN uses the same infrastructure for various purposes eliminate capital outlays. It is all because of SDN-centric controller, which allows deploying the same hardware with great effect.

(iv) Cloud Abstraction & Automation

The enterprise can also easily unify cloud resources by abstracting cloud resources with the aid of an SDN. Alternating automated responses in the cloud can also be done with SDN. In environments like enterprise-wide SD-WAN networks the process works particularly well.

4. SUMMARY OF METRICS

Table 1 illustrates about various features that are considered to define Traditional Network and SDN.

Table 1: Features considered for defining Traditional network and SDN

Sl no.	Features	Traditional Network	Software Defined Network
1	**Based on**	Hardware	Software
2	**Communication**	Interaction between control plane and data plane happens using protocols such as OSPF, BGP, ARP and STP, which is a limitation both from a technical and management point of view	Having feature of Northbound interface to communicate with APIs, so that application developers can program the network directly
4	Virtualization	The physical location of the control plane impedes the capability of an IT operator to monitor the flow of traffic.	This creates an abstract copy of your physical network when it virtualizes the entire system and enables you to access services from a centralized location.
5	**Network Capacity**	To increase the capacity it requires new hardware	This allows network administrators to have the required services and bandwidths without needing significant physical infrastructure investment.
6	**Configurations**	Manual Configuration	Automated Configuration

Table 2 illustrates about various metrics that are considered to define network capabilities.

Table 2: Metrics Used to Define Network capabilities

Sl no.	Metrics	Traditional Network	Software Defined Network
1	Maintenance Cost		✓
2	Performance		✓
3	Resource Usage	✓	
4	Network management		✓
5	Controller		✓
6	Flexibility		✓

5. ANALYSIS

Among a variety of networking companies that more than fifty percent of businesses are reluctant to invest immediately in an SDN solution. Based on the input collected from various blogs below graph of figure 4, shows the time considered by various organizations to start adapting the SDN. In between some companies lost interest with usage of SDN instead they are willing to utilize the characteristics of both traditional and SDN.

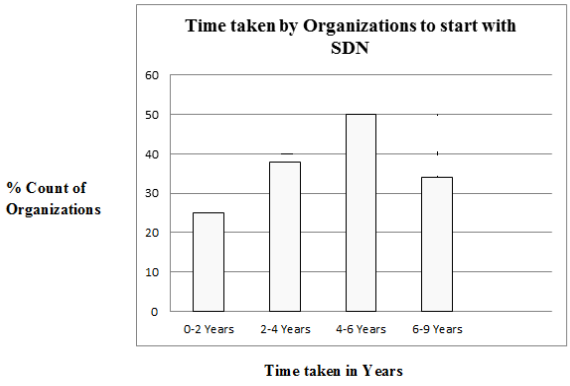

Figure 4: Graph illustrating time taken by organizations to adapt SDN

6. CONCLUSION

SDN helps to provide a standardized information about the network-one can easily customize / track / diagnose problems found in central-level network equipment, removing a great deal of hard work, consequently cost and time saving process. As the software defined networking layer is interactive, it will virtualize the networks that would be built at the high level. This kind of virtual network is built into real physical infrastructure. With numerous northbound APIs for application creation, implementation plan for the SDN methodology is being developed. Progress in software-defined networking and northbound API is now in its initial stages and offers the enormous potential and opportunities which are not previously available for improving SDN-wide security.

REFERENCES

1. Sumit badotra, Japinder Singh . **A Review Paper on Software Defined Networking**.
2. Vinayakumar R, Soman KP, Mamoun Alazab, Sriram S, Simran K. **A Comprehensive Tutorial and Survey of Applications of Deep Learning for Cyber Security.**
3. Hussein , Louma Chadad, Nareg Adalian, Ali Chehab, Imad H. Elhajj and Ayman Kayssi .**Software-Defined Networking (SDN): the security review.**
4. Raphael Horvatha, Dietmar Nedbala,*, Mark Stieninger. **A Literature Review on Challenges and Effects of Software Defined Networking.**
5. Aburomman, A. A., & Reza, M. B. I. (2017). **Survey of Learning Methods in Intrusion Detection Systems.** https://doi.org/10.1109/ICAEES.2016.7888070
6. https://www.opennetworking.org/index.php?option=com_content&view=article&id=686&Itemid=272&lang=en.
7. Martìn Casado, Michael J. Freedman, Justin Pettit, Jianying Luo and Nick McKeown and Scott Shenker . **Ethane: Taking Control of the Enterprise**.
8. Chen, Tao & Matinmikko, Marja & Chen, Xianfu & Zhou, Xuan & Ahokangas, Petri. (2015). **Software defined mobile networks: Concept, survey, and research directions**. IEEE Communications Magazine. 53. 10.1109/MCOM.2015.7321981.
9. A. Detti, C. Pisa, S. Salsano and N. Blefari-Melazzi. **Wireless mesh software defined networks (wmSDN).** IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 2013. “Cisco white paper,” © 2013 Cisco and/or its affiliates. All rights reserved. https://doi.org/10.1109/WiMOB.2013.6673345
10. F. Hu, Q. Hao, and K. Bao. **A Survey on Software-Defined Network and OpenFlow from Concept to Implementation**. IEEE Communication Surveys & Tutorials, vol. 16, no. 4, fourth quarter 2014. https://doi.org/10.1109/COMST.2014.2326417
11. N. Foster, M. J. Freedman, A. Guha, and R. Horrison, **Languages for software-defined networks**. IEEE Commun. Mag. Feature Topic Softw. Defined Netw., vol. 51, no. 2, Feb. 2013.
12.Q. Yan, F. R. Yu, Q. Gong, and J. Li. **Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments A Survey Some Research Issues and Challenges,** IEEE

Communications Surveys & Tutorials, vol. 18, no. 1, first quarter 2016.
https://doi.org/10.1109/COMST.2015.2487361
13. Kreutz, D., Ramos, F., Verissimo, P., Rothenberg, C. E., Azodolmolky, S., & Uhlig, S.**Software-defined networking: A comprehensive survey.**
14.Yogita Hande, Akkalashmi Muddana . **A Survey on Intrusion Detection System for Software Defined Networks (SDN).**
15. Hayward, S. S., Natarajan, S., & Sezer, S. (2015). **A survey of Security in Software Defined Networks**. *IEEE Communications Surveys and Tutorials*, *18*(1), 623–654. doi:10.1109/COMST.2015.2453114.
16. Pradeep Kumar Sharma, S. S. Tyagi . **Improving Security through Software Defined Networking (SDN): AN SDN based Model**.
17.Ashutosh Kumar Singh, Shashank Srivastava, **A survey and classification of controller placement problem in SDN**.
18. Bruno Astuto A. Nunes, Marc Mendonca, Xuan-Nam Nguyen, Katia Obraczka, and Thierry Turletti,. **A Survey of Software-Defined Networking: Past,Present, and Future of Programmable Networks**.
19.Fei Hu, Qi Hao, and Ke Bao, **A Survey on Software-Defined Network and OpenFlow: From Concept to Implementation**.
20.Jean Tourrilhes, Puneet Sharma, Sujata Banerjee, Justin Pettit, **The Evolution of SDN And Open Flow: A Standards Perspective** .
21. Shobharani D, Parikshith Nayaka S K, Swasthika Jain T, Dr. Dayanand Lal , **Effective and Secure Approach for Multi-Keyword Quest Graded over Authenticated Data**, International Journal of Advance Trends in Computer Science and Engineering, 2020, volume 9, number 2, pages 2278-3091.
https://doi.org/10.30534/ijatcse/2020/72922020
22. Mrs. Sahana D S, Mr. Vinay D M, Dr. Dayanand lal N , Mr. Kishore C , **A System to Design and Implement the Solar Sensors.**
23. Mr. Parikshith Nayaka S K, Mrs. Shobha Rani, Dr. Dayanand Lal, Dr. M Anand. (2020). **Convert Channel and Information Hiding in TCP/IP** . International Journal of Control and Automation, 13(02), 582 - 591.